STUDY

Requested by the LIBE committee

European Parliament

The future EU-UK relationship: options in the field of the protection of personal data for general processing activities and for processing for law enforcement purposes

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate General for Internal Policies of the Union
PE 604.976 - August 2018

EN

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

The future EU-UK relationship: options in the field of the protection of personal data for general processing activities and for processing for law enforcement purposes

STUDY

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, examines the available mechanisms for personal data transfers between the EU and the UK after Brexit. The study shows that an adequacy finding for the UK would be beneficial, but insufficient. Notably, and to the extent that there is a consensus on these points, there is a need for a bespoke instrument that establishes a standstill period, and which allows the UK to participate in (i) the development of EU data protection policy, (ii) internal market data transfers, and (iii) security and law enforcement initiatives.

PE 604.976 EN

ABOUT THE PUBLICATION

This research paper was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and was commissioned, overseen and published by the Policy Department for Citizen's Rights and Constitutional Affairs.

Policy Departments provide independent expertise, both in-house and externally, to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU external and internal policies.

To contact the Policy Department for Citizens' Rights and Constitutional Affairs or to subscribe to its newsletter please write to: poldep-citizens@europarl.europa.eu

RESPONSIBLE RESEARCH ADMINISTRATOR

Kristiina MILT
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

AUTHORS

Hans GRAUX, Time.lex
Alessandra INNESTI, Spark Legal Network
Inês DE MATOS PINTO, Spark Legal Network
Peter MCNALLY, Spark Legal Network
Patricia YPMA, Spark Legal Network
Rianne SIEBENGA, PwC
Wim WENSINK, PwC

With the support of Professor Emeritus Jos DUMORTIER acting as legal supervisor, and George ALDERS (PwC) and Sandra MOCHÈL (PwC).

LINGUISTIC VERSION

Original: EN

Manuscript completed in August 2018
© European Union, 2018

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

CONTENTS

LIST OF ABBREVIATIONS

ACAs	Administrative Cooperation Arrangements
ADR	Alternative dispute resolution
AEO	Authorised Economic Operator
AFIS	Anti-Fraud Information System
AQSIQ	General Administration of Quality Supervision, Inspection and Quarantine of China
B2B	Business to Business
BASA	Bilateral Aviation Safety Agreement
BCRs	Binding Corporate Rules
CETA	Comprehensive Economic and Trade Agreement
CFR-net	European contract law network
CHAFEA	Consumers, Health, Agriculture and Food Executive Agency
CIS	Customs Information System
CIWIN	Critical Infrastructure Warning Information Network
CJEU	Court of Justice of the European Union
CPCS	Consumer Protection Cooperation System
CPVO	Community Plant Variety Office
DG FISMA	Directorate-General for Financial Stability, Financial Services and Capital Markets Union
DG HOME	Directorate-General Migration and Home Affairs
DG JUST	Directorate-General for Justice and Consumers
DG MOVE	Directorate-General for Mobility and Transport
DG SANTE	Directorate-General for Health and Food Safety
DG TAXUD	Directorate General Taxation and Customs Union
DG TRADE	Directorate-General for Trade
DPA	Data Protection Authority
DRIPA	Data Retention and Investigatory Powers Act
EASA	European Aviation Safety Agency
EASO	European Asylum Support Office
EBA	European Banking Authority
ECCs	European Consumer Centres
ECDC	European Centre for Disease Prevention and Control

ECHA	European Chemicals Agency
ECHR	European Court of Human Rights
ECRIS	European Criminal Records Information System
EDES	Early Detection and Exclusion System
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFSA	European Food Safety Authority
EFTA	European Free Trade Association
EIOPA	European Insurance and Occupational Pensions Authority
EMA	European Medicines Agency
EORI	Economic Operators Identification and Registration
EPCIP	European Programme for Critical Infrastructure Protection
ESMA	European Securities and Markets Authority
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
EUROSUR	European Border Surveillance System
FEDMA	Federation of European Direct and Interactive Marketing
FVO	Food and Veterinary Office
GDPR	General Data Protection Regulation
GSP	Generalized System of Preferences
IBM	Integrated Border Management
IPA	Investigative Powers Act
JRC	Joint Research Centre
MENA	Middle East and North Africa
ODR	Online Dispute Resolution
OLAF	European Anti-Fraud Office
PICS	Programme Information and Collaboration Space
PNR	Passenger Name Record
PPPAMS	Plant Protection Products Application Management System
RAPEX	European rapid alert system for non-food dangerous products
RASFF	Rapid Alert System for Food and Feed
REX	Registered Exporters
SCCs	Standard Contractual Clauses
SESAR	Single European Sky ATM Research
SIS	Schengen Information System

SMEs	Small and Medium Enterprises
TDI	Trade Defence Instrument
TEU	Treaty on European Union
UK	United Kingdom
USA	United States of America
VIS	Visa Information System

LIST OF TABLES

EXECUTIVE SUMMARY

Background

This study has been commissioned against the backdrop of the UK's Brexit referendum of 23 June 2016, and the subsequent official notification by the UK government of its intention to withdraw from the European Union (EU). Since that notification, negotiations have been ongoing between the UK and the EU on the form and content of their future relationship. One of the key policy areas that raises concerns in these negotiations is data protection. The protection of personal data is recognised as a fundamental right for European citizens, enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. This implies essentially that no collection, exchange, use or other form of processing of personal data may occur unless certain measures have been taken to ensure that such processing will be done in full compliance with the EU's legal and policy framework for data protection.

Brexit poses clear challenges with respect to data protection. As a Member State of the EU, the UK is required to comply with, and align to, the EU's regulatory and policy framework. As a corollary of membership, exchanges of personal data meet no additional legal hurdles. This affects both private companies, public sector bodies and institutions that can exchange personal data with their EU peers in relative freedom. After Brexit, this freedom of exchange is no longer ensured in the same manner, and entities in the UK that depend on information exchanges may face significant additional hurdles, or may simply be unable to continue these exchanges. This creates challenges for both private enterprise and for the public sector, including such issues as law enforcement cooperation.

Aim of this Study

The aim of this study is to summarily examine possibilities and legal and institutional prerequisites for continuing the exchange and processing of personal data between the UK and the EU following Brexit, also in view of a future relationship agreement. This is done by examining existing legal mechanisms and policy measures that can support the exchange of personal data, but also by looking at current information flows between the EU and UK, and between the EU and third countries. In this manner, the study may support Brexit negotiations and contribute to a correct appreciation of the main options for organising information flows between the UK and the EU post-Brexit.

Main findings

The study shows that the existing legal mechanisms and policy measures which are presently used to support the exchange of personal data between the EU and third countries can alleviate some of the concerns surrounding Brexit, but that none of these, in isolation or collectively, would be sufficient to permit a continuation of personal data flows and cooperation in relation to data protection on the same basis as today. Notably, an affirmative adequacy finding for the UK (both in relation to data protection in general under the General Data Protection Regulation (GDPR) and in relation to law enforcement under the Law Enforcement Directive) would be highly beneficial, but insufficient to allow a continuation of current information flows. While adequacy findings would be appropriate for private sector exchanges, in the public sector – both for internal market exchanges and law enforcement exchanges – a multitude of legal instruments exist beyond general data protection law, that determine which countries may participate in information exchanges, and on which basis.

An adequacy finding would be a beneficial step in ensuring the continued integration of the UK in such information exchanges – assuming that there is a mutual understanding that this should be the outcome of negotiations – but it would not be sufficient without a broader legal basis in the form of a bespoke legal agreement that would authorise the UK and EU to continue to participate in information exchanges. Furthermore, it should be noted that an adequacy finding is generally a lengthy process, the initiation of which could only begin after the UK has left the EU. Therefore, an adequacy finding is insufficient to avoid a temporary standstill in information exchanges, which would be mutually detrimental.

Other common legal instruments used in data protection law to organise personal data exchanges – such as standard contractual clauses, binding corporate rules, certification, codes of conduct and approved ad hoc contractual terms – are equally available to the UK after Brexit, but the use of such instruments is generally resource intensive and unsuitable to set up a broad framework for data exchanges that can be used to organise compliance transfers of personal data on a large scale, including particularly regarding SMEs.

Globally, and to the extent that there is a consensus on the political desirability of each of these points, there is a need for a bespoke instrument that establishes an initial standstill period that allows the EU and the UK to continue personal data exchanges on a provisional basis, taking into account that the UK's data protection law is already substantially aligned to EU data protection law and policies. Furthermore, the bespoke agreement can allow the UK to participate in (i) the development of common EU data protection policy (i.e. by contributing to positions of the European Data Protection Board, by participating in the one-stop-shop mechanism, and by ensuring a homogeneous application of EU case law in relation to data protection, including in the UK), (ii) internal market data transfers, and (ii) security and law enforcement initiatives. Assuming that the EU and UK mutually agree on the desirability of these priorities, this would seem to be the only approach that can avoid a temporary halt in personal data exchanges, and that can ensure continuous alignment of data protection policy between the UK and EU, even after Brexit.

1. INTRODUCTION

1.1. Objective and research question

This study has been commissioned against the backdrop of the UK's Brexit referendum of 23 June 2016, and the subsequent official notification by the UK government of its intention to withdraw from the EU. Since that notification, negotiations have been ongoing between the UK and the EU on the form and content of their future relationship. As of December 2017, the European Council conclusions decided that there has been sufficient progress "to move to the second phase related to [...] the framework for the future relationship"[1].

One of the key policy areas that raises particular concerns in these negotiations is data protection. The protection of personal data is recognised as a fundamental right for European citizens, which is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. This implies essentially that no collection, exchange, use or other form of processing of personal data may occur unless certain measures have been taken to ensure that such processing will be done in full compliance with the EU's legal and policy framework for data protection.

Brexit poses clear challenges with respect to data protection. As a Member State of the UK, the UK is required to comply with, and align to, the EU's regulatory and policy framework. However, the outcome of this requirement is that information exchanges containing personal data meet no additional legal hurdles. This affects both private companies, public sector bodies and institutions that can exchange person data with their EU peers in relative freedom. After Brexit, this freedom of exchange is no longer ensured in the same manner, and entities in the UK that depend on information exchanges may face significant additional hurdles, or may simply be unable to continue these exchanges.

The UK government is keenly aware of this issue, and has made some proposals to ensure continuity in personal data exchange options.[2] It has stressed that "Data flows between the UK and the EU are crucial for our shared economic prosperity and for wider cooperation, including on law enforcement. It is therefore essential that as part of the UK's future partnership with the EU, we agree arrangements that allow for free flows of data to continue, based on mutual trust in each other's high data protection standards".[3] In the same document, the UK government also noted its intention for the UK to be compliant with EU data protection law and wider global data protection standards on exit, and expressed its preference for a specific UK-EU model for exchanging and protecting personal data, building on the existing adequacy model, and mutual recognition of each other's data protection frameworks as a basis for the continued free flows of data.

Furthermore, on the 26th of June 2018, the UK Parliament adopted the European Union (Withdrawal) Act 2018[4] (hereafter the "Withdrawal Act"), which repeals the European Communities Act 1972 through which the UK acceded to the European Union. However, the Withdrawal Act does not abrogate all law originating from the EU: so-called "EU-derived domestic legislation" (such as the transposition of EU Directives) is retained. Similarly, any direct EU legislation which has effect in EU law immediately before exit day, is ruled to form "part of domestic law on and after exit day" (so-called "retained law"). The Withdrawal Act of course does not obviate the need for a withdrawal agreement between the UK and EU,

[1] European Council. Guidelines European Council (Art. 50) meeting. 15 December 2017. EUCO XT 20011/17, para. 1. See: https://www.consilium.europa.eu/media/32236/15-euco-art50-guidelines-en.pdf.

[2] See notably the UK government paper on "The exchange and protection of personal data – A future partnership paper", https://assets.publishing.service.gov.uk/ government/u ploads/system/uploads /attachment data /file /639853/The exchange and protection of personal data.pdf.

[3] Ibid, para 43.

[4] See http://www.legislation.gov.uk/ukpga/2018/16/contents/enacted/data.htm.

and specifies that such an agreement must be approved through a separate act of Parliament. Thus, a certain degree of continuity is ensured. However, the UK would retain the power to modify any such EU-derived domestic legislation or retained law, so that continued compliance is not assured. Furthermore, while the Withdrawal Act specifies that case law from the European Court of Justice preceding Brexit is in principle retained, future case law from the Court is not applied, and UK courts will have the power to overturn case law from the European Court in the same manner as national case law. Thus, the Withdrawal Act offers no assurance of continuity in data protection law in the longer term.

More recently, on 12 July 2018 the UK Government published its White Paper on The Future Relationship between the United Kingdom and the European Union[5]. The White Paper states the UK's objective of leaving the Single Market and the Customs Union; while nonetheless aiming to "preserve the UK's and the EU's frictionless access to each other's markets for goods, protecting jobs and livelihoods on both sides, and propose new arrangements for services" and to "maintain the shared security capabilities that keep citizens in the UK and the EU safe". A specific chapter in the Paper sets out how this should be done, emphasising two pillars of activity: on the one hand ensuring continued exchange of personal data between the UK and the EU with strong privacy protections for citizens; and on the other focusing on ongoing cooperation between data protection authorities in the EU and in the UK.

Regarding the former point, the White paper indicates the UK government's preference for obtaining an adequacy assessment, but also stresses its desire to go further, namely by creating a framework to facilitate dialogue between the EU and the UK in order to minimise the risk of disruption to data flows, and by setting up close cooperation and joined enforcement action between the UK and the EU in order to ensure continued regulatory alignment. On the latter point – i.e. the role of data protection authorities – the UK Government similarly stresses its desire to ensure continued cooperation between the UK's Information Commissioner (ICO) and the Member States' data protection authorities. This cooperation would extend to enforcement, redress, and participation in the One Stop Shop mechanism which facilitates data protection compliance for undertakings which process personal data across multiple Member States. In summary, the proposal aims to ensure that the effects of Brexit on businesses in particular would be minimal by minimising interruptions in data flows and facilitating the application and enforcement of data protection rights.

The objective of this study is therefore to summarily examine possibilities and legal and institutional prerequisites for the continuation of exchanging and processing of personal data between the UK and the EU following Brexit and in view of a future relationship agreement. In this manner, the study may support Brexit negotiations and contribute to a correct appreciation of the main options for organising information flows between the UK and the EU post-Brexit.

1.2. Outline of the study

Given the study's objective as described above, this document is structured to facilitate a quick but accurate understanding of the legal and policy complexities related to personal data exchanges between the UK and EU in a post-Brexit environment. Chapter 2 of this study provides a first overview of the precise problem, by explaining how and why membership of the EU has such a profound impact on the ability to exchange personal data, including the role of recent legislative overhauls in the EU. Chapter 3 then examines the impact of Brexit, explaining summarily what the implications of a Brexit would be in the absence of mitigating measures.

[5] Future Relationship between the United Kingdom and the European Union, White Paper from the UK Government, published 12 July 2018, see https://www.gov.uk/government/publications/the-future-relationship-between-the-united-kingdom-and-the-european-union.

Chapter 4 describes adequacy assessment mechanisms for third countries (to be understood for the purposes of this study as any country which is not a Member State or European Economic Area (EEA) country) and their legal bases, explaining how and to what extent personal data can be exchanged with third countries in general, i.e. without considering the specific circumstances of the UK. Finally, chapter 5 looks at personal data transfers between the EU and the UK and does so by discerning between private sector transfers and public sector transfers. All desk research reports of the 15 selected European Commission Directorates General (DGs) and Agencies can be found in Annex III. The main findings of the desk research on these entities are summarized in section 3.3, while the insights are employed throughout the study.

2. THEORETICAL FRAMEWORK AND SCOPE OF THE STUDY

2.1. Theoretical framework

The EU's legal and policy framework is very extensive, comprising both general legislative and normative texts and sector specific rules. The latter group is comprised of a broad range of legislation and norms that regulate how specific exchanges occur or how specific EU or national public sector bodies are required to exchange personal data. These sector specific rules will be examined in more detail in Chapter 4, where we will examine current data flows between the UK and the EU.

The former group (general legislative and normative texts) is comprised principally of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR); and of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (also known as the Police and Criminal Justice Directive, or the Law Enforcement Directive).

The GDPR, which became applicable as of 25 May 2018, provides for the general legal framework that applies to the processing of personal data, both in the public and private sector. It repealed the earlier Data Protection Directive 95/46/EC as of that date. As a Regulation, the GDPR applies directly in all Member States without requiring any transposing legislation at the national level on issues which are addressed by the Regulation, although there are certain topics for which the GDPR allows for national law-making. Similarly, as a text with EEA relevance, the GDPR applies additional to the non-Member State EEA countries Iceland, Liechtenstein and Norway.

The GDPR explicitly carves out a few policy areas from its scope of application. Article 2.2 of the GDPR states that the "Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;
(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
(c) by a natural person in the course of a purely personal or household activity;
(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

Point (d) in this list thus refers generally to data processing in the context of law enforcement, the application of criminal law and public security, which is regulated instead by the aforementioned Law Enforcement Directive that replaced the earlier Council Framework Decision 2008/977/JHA. As a Directive, contrary to a Regulation, the Law Enforcement Directive requires transposition into national law, for which a deadline was set of 6 May 2018.

Finally, personal data processing by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data still applies. This Regulation is presently undergoing revision in order to bring its substance in better alignment with the GDPR.

Similarly, within the context of electronic communications, a more specific legal framework exists in the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications or e-Privacy Directive). The e-Privacy Directive was amended substantially in 2009 through Directive 2009/136/EC, especially in relation to the use of cookies and similar technologies. This Directive too is presently undergoing revision to improve alignment with the GDPR, and a proposal for a Regulation on Privacy and Electronic Communications (e-Privacy Regulation) was published in January 2017. If adopted, this ePrivacy Regulation would repeal and replace the e-Privacy Directive as amended.

Most exchanges of personal data between the UK and the EU will therefore be regulated by the GDPR or by the Law Enforcement Directive, although processing activities undertaken by EU bodies (before or after any such transfer) will generally fall within the scope of Regulation (EC) No 45/2001. This approach ensures a relatively homogeneous legal framework within all Member States and EEA countries, allowing them to exchange personal data with the same freedom as within their own national borders.

Transfers of personal data outside of the EU and EEA countries however are subject to more stringent legal requirements, in order to ensure that personal data of EU citizens cannot trivially be exported to a destination where the EU's high standards of data protection may not apply. The GDPR, Law Enforcement Directive and Regulation (EC) No 45/2001 therefore all contain similar rules which only permit the transfer of personal data to recipients that are not subject to EU data protection law under specific legal requirements.

These shall be discussed in greater detail in the following chapter, but the implications are clear: after the UK loses its status as a Member State, and assuming that it does not become an EEA country that applies EU data protection law under the same terms as a Member State, it will be considered a third country with which personal data can only be exchanged if these additional specific requirements are met. This implies significant compliance burdens both for private and public sector bodies.

Furthermore, specifically in the context of public sector exchanges between the EU and the UK (i.e. between UK public bodies on the one hand, and EU public bodies or Member States on the other hand), personal data transfers may be legally impossible without legislative amendments or the negotiation of specific agreements, which may be complex and time consuming. The risk is therefore an exchange interruption, i.e. a period of time in which information exchanges are not legally permissible until such a time where an appropriate legal solution is found.

2.2. Scope of the study

This study will examine what form such legal solutions to allow the continued exchange of personal data would take, considering the legal requirements of the GDPR, the Law Enforcement Directive and Regulation (EC) No 45/2001, and considering that there may be a need for a transitional regime to avoid a "cliff edge" in the current exchanges.

In order to ensure that this study is appropriately grounded in reality, it has been drafted not only on the basis of an examination of the legal framework, prior interactions with other third countries, and key data protection case law, but also by studying information exchanges in certain EU policy areas. Notably, interviews were conducted with representatives from a series of relevant stakeholders in order to determine what their main personal data processing activities are, what the main requirements are, and how they might be able to interact with a third country. The full list of interviewees can be found in Annex II. The insights gained from the interviews are used to complement the desk research conducted on a selection of DGs and Agencies.

The following DGs and Agencies were selected:

1) DG JUST (Justice and Consumers)
2) DG HOME (Migration and Home Affairs)
3) Europol (European Police Office)
4) Frontex (European Agency for Operational Cooperation at the External Borders)
5) EBA (European Banking Authority
6) EASA (European Aviation Safety Agency)
7) DG MOVE (Mobility and Transport)
8) OLAF (European Anti-Fraud Office)
9) Eurojust (European Judicial Cooperation Unit)
10) ESMA (European Securities and Markets Authority)
11) DG SANTE (Health and Food Safety)
12) DG TAXUD (Taxation and Customs Union)
13) DG FISMA (Financial Stability, Financial Services, and Capital Markets Unit)
14) DG TRADE (Trade)
15) eu-LISA (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice)

While the list is of course far from comprehensive, the selected entities have been chosen on the basis of the breadth of personal data that they process, including in some cases sensitive data, e.g. in the context of law enforcement. In this manner, the study can take into account the requirements imposed by specific use cases, ranging from the more mundane to the more delicate, in order to come to a balanced appreciation of challenges and potential resolution strategies. Annex III provides the full overview of the in-depth desk research.

3. INTRODUCTION TO DATA TRANSFER COMPLIANCE CHALLENGES AND BREXIT

3.1. Principles and derogations to data transfers under EU law – legal bases for data transfers

This study aims to examine the potential solutions to organise data transfers after the UK loses its membership status. In order to do so, it is important to appreciate the mechanisms that currently exist and are used to organise data transfers to third countries. As highlighted above, the GDPR, Law Enforcement Directive and Regulation No 45/2001 all build on the same principle, namely that transfers to third countries are only allowed if one or more of an exhaustive list of mitigation measures is taken.

Specifically, Chapter 5 of the GDPR recognises the following legal bases to permit the transfer of personal data to a recipient in a third country:

Table 1 - Legal basis for the transfer of personal data to a third country

• An **adequacy assessment** i.e. a formal Decision from the Commission that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection
• The application of one or more of the following **appropriate safeguards, which do not require any authorisation from a national data protection authority:** (a) a legally binding and enforceable **instrument between public authorities or bodies;** (b) **binding corporate rules in accordance with Article 47 of the GDPR;** **(c) standard data protection clauses** adopted by the Commission; (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission; (e) an **approved code of conduct** pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards; or (f) an **approved certification mechanism** pursuant to Article 42 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards
• The application of one or more of the following **appropriate safeguards with an authorisation from a national data protection authority**: (a) **contractual clauses** between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be inserted into **administrative arrangements between public authorities or bodies** which include enforceable and effective data subject rights.

The provisions in the Law Enforcement Directive (notably Article 35) are comparable, but principally focus on adequacy assessments, international legally binding instruments between public sector bodies, and on decisions from the competent transferring authority; given the subject matter, binding corporate rules, codes of conduct and certification are indeed less viable. Finally, article 9 of Regulation No 45/2001 refers principally to adequacy assessments – that however do not require a Commission decision under this Regulation - and decisions from the European Data Protection Supervisor.

The mechanisms in these three data protection instruments are therefore relatively comparable. In addition to these standardised tools enshrined in the law, it would of course also be possible to conclude a bespoke agreement between the UK and the EU, in which they mutually recognise the essential equivalence of their respective data protection frameworks, based on a substantive comparative assessment.

It is worth underlining that restrictions under EU law only apply to personal data transfers *to* third countries (i.e. export of personal data to a non-EU/EEA destination), and not to transfers *from* third countries (i.e. import of personal data to an EU/EEA destination). Of course, it is highly plausible that the UK, under its own data protection law to be implemented for the post-Brexit era, would introduce similar requirements for the export of personal data to other countries, possibly including EU Member States and EU bodies, which may require an adequacy finding from the UK. This issue however, does not fall within the scope of the present study.

Furthermore, the GDPR and Law Enforcement Directive stress that the applied safeguards should also ensure that onward transfers to other third countries are similarly covered. In other words, a non-EU/EEA recipient of personal data who wishes to transfer this personal data to another non-EU/EEA recipient must apply the same safeguards that were applied to him. The Regulation No 45/2001 presently contains no such explicit rule, although the same logic would need to be applied.

3.2. Implications of Brexit without specific policy measures

The overview of measures above shows that ensuring a continuation of transfers of personal data to the UK can be legally challenging, or at least highly burdensome for the affected parties, if no policy measures (such as EEA membership, adequacy assessments or bespoke arrangements) are undertaken to facilitate these transfers.

For purely private sector parties, transfers of personal data to the UK become significantly more complex and costly. Absent any approved codes of conduct or certification mechanisms – none of which presently exist – most transfers would need to be organised on the basis of standard contractual clauses. This is feasible as examples of other third countries show, but implies an additional contractual and negotiation hurdle that needs to be factored into any business relationship involving data transfers to the UK.

In the public sector, and specifically for transfers of personal data from EU bodies or Member State administrations to UK public bodies, the conclusion of standard contractual clauses would be highly impractical, given the need for government approval and negotiation in every instance where personal data would need to be transferred. In practice, the decisive factor would be whether a legal instrument exists – such as a law, treaty or agreement – that permits the transfer of personal data to a third country in general or to the UK specifically. As will be demonstrated in the following sections in which examples from specific DGs or Agencies are examined, such legal instruments exist in some cases, but their approach and application is somewhat fragmented, Moreover, it would need to be verified whether in a post-Brexit environment the UK would be eligible to participate in them.

The UK Parliament has sought to address these issues to some extent through its adoption on 26 June 2018 of the Withdrawal Act[6], which extends the legal validity of so-called "EU-derived domestic legislation" (including e.g. a UK transposition of the Law Enforcement Directive), as well as so-called "direct EU legislation" i.e. any EU regulation, EU decision or EU tertiary legislation, as it has effect in EU law immediately before exit day (which would include also the GDPR)[7]. However, this alone does not resolve the challenges of Brexit. Firstly, independent of the continuity of EU law, the UK would still become a third country – admittedly one which follows EU law to the letter – and would therefore be legally treated as such. Continued application also poses its own questions: even if the GDPR continues to be applied in the UK, its provisions allowing Member States to participate in the European Data Protection Board would obviously not have legal effect, as the UK would no longer be a Member State. Furthermore and more fundamentally, under the Withdrawal Act, the UK would retain the power to modify any EU-derived domestic legislation or retained law, so that continued compliance is not assured. Finally, while the Withdrawal Act specifies that case law from the Court of Justice of the European Union (CJEU) preceding Brexit is in principle retained, future case law from the Court is not applied, and UK courts will have the power to overturn case law from the European Court in the same manner as national case law.

Thus, the Withdrawal Act offers no assurance of continuity in data protection law in the longer term, and a negotiated agreement addressing these points would still be needed. The UK Government's White Paper on The Future Relationship between the United Kingdom and the European Union[8], which was published after the Withdrawal Act, reiterates the intentions of the Act but does not clarify the issues above. While the Paper stresses the need for regulatory cooperation and rightly emphasises that "it would be in the UK's and the EU's mutual interest to have close cooperation and joined up enforcement action", the fundamental challenge remains that, in order to avoid disruptions of data flows, EU data protection law – including its interpretation by the Court of Justice – must be adhered to. This is a matter of compliance with a fundamental right, which offers limited opportunity for dialogue or negotiation.

As was already noted above, the legal issue from the perspective of EU data protection law only exists for personal data being sent *to* the UK; receipt of personal data *from* the UK is not more problematic than other types of processing. Aside from the political complexities of asymmetric data flows, in practice the exchanges of personal data organised within the EU rely substantially on bilateral communication in order to be useful for both parties, so that the distinction between information flows in one direction rather than another will in most cases be irrelevant: personal data needs to be able to flow both ways.

[6] See http://www.legislation.gov.uk/ukpga/2018/16/contents/enacted/data.htm.

[7] More in detail, Section 3 (2) (a) of the Act grants the applicability of "any EU regulation, EU decision or EU tertiary legislation, as it has effect in EU law immediately before exit day and so far as—
(i)it is not an exempt EU instrument (for which see section 20(1) and Schedule 6),
(ii)it is not an EU decision addressed only to a member State other than the United Kingdom, and
(iii)its effect is not reproduced in an enactment to which section 2(1) applies.
Since the GDPR does not seem to fall in any of the exclusions, applicability of the GDPR would continue.

[8] Future Relationship between the United Kingdom and the European Union, White Paper from the UK Government, published 12 July 2018, 8. See https://www.gov.uk/government/publications/the-future-relationship-between-the-united-kingdom-and-the-european-union.

3.3. General findings with respect to personal data processing and personal data transfers in 15 selected Directorate Generals and Agencies

Some general conclusions can be drawn from the analysis of all 15 selected EU Agencies (EASA, EBA, ESMA, EU Lisa, Eurojust, Europol and Frontex) and European Commission DGs (FISMA, HOME, JUST, MOVE, SANTE, TAXUD and TRADE).[9] Desk research shows that the above-mentioned EU Agencies and DGs, to a greater or lesser extent, engage in different activities whereby the processing and echange of personal data with third countries and/or international organisations occurs.

In the case of EU Agencies, these have been established pursuant to EU legislative acts that set out not only their mandates and how they are organised, but also the means by which they can engage in international cooperation, either with third countries or international organisations. The provisions of the founding acts of these Agencies relating to international cooperation or, where applicable, to the access and exchange of personal data collected and processed by them in the context of their activities regulate several aspects, from the purpose of the personal data exchange to the means of transfer or the conditions of or restrictions to access to the data. Furthermore, both the nature and the purpose of the personal data being processed and exchanged directly relate to the specific mandate or field of activity of each Agency. When lawful, the processing and exchange of such data are regarded as important activities allowing the respective Agency to carry out its duties. Across all, commonly-used tools for setting up and governing the exchange of personal data with third countries or international organisations are (bilateral) cooperation agreements or working arrangements.

Similarly, in the case of European Commission Directorates-General, the lawfulness of the processing and exchange of personal data with third countries or international organisations normally stems from provisions of legal acts relating to the fields of European Union law and policy which they were established to develop. Accordingly, the nature and purpose of the personal data being processed depends on the specific activity or objective in question, ranging from technical databases to be used by experts to the award and management of grants to stakeholder consultations. Therefore, in most cases, the processing of personal data by these DGs is regarded as necessary for the performance of the tasks they carry out in the public interest, as envisaged by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (currently undergoing revision in order to better align its substantive provisions with the GDPR). As a general rule, the exchange of personal data with third countries or international organisations takes place in the context of a specific agreement negotiated on behalf of the EU and/or the Member States, by giving staff or experts from the third country or international organisation access to the data via databases or through the direct transmission by the competent secretariat staff of the DG concerned (including the staff member who is the controller of the processed data).

Finally, in the absence of any concrete agreements or arrangements, the exchange of personal data with third countries or international organisations by either EU Agencies or European Commission DGs falls under and is regulated by Article 9 of Regulation (EC) No 45/2001, mentioned above. This provision details, *inter alia*, the purposes for which personal data may be exchanged, the criteria for finding an adequate level of protection with respect to the intended recipient, possible derogations or exceptions, etc.

[9] All 15 research reports can be found in Annex III. Each report covers the following aspects: introduction of the EU Agency or Directorate-General, nature of the personal data, purpose of the processing, entities involved in the processing, legal basis and lawfulness, cooperation with third countries and actual examples of the latter.

4. ADEQUACY ASSESSMENTS

KEY FINDINGS

- An adequacy assessment appears to be a viable option to support personal data transfers to the UK for the reasonably short term. While it does not permit the UK to participate in the governance of data protection law and policy, and there are no precursors yet for adequacy assessments under the revised data protection regime (and none at all for data exchanges in the law enforcement context), the historical alignment of the UK with EU data protection law would plausibly be a significant accelerating factor.

- Horizontal points of attention in the negotiation will be (1) the requirement for the UK to follow case law from the CJEU in its interpretation and application of data protection law (contrary to the approach adopted in the Withdrawal Act); and (2) onward transfers, particularly in the context of the Law Enforcement Directive, where the UK's relationship towards transatlantic partners might create doubts on the appropriateness of a position that is fully or closely equivalent to that of a Member State .

4.1. Procedure in general and historical cases

The central goal of an adequacy decisions by the European Commission is to formally confirm that the level of data protection in a third country or an international organization is essentially equivalent to the level of data protection in the European Union. It is important to appreciate this point correctly, as it has been affirmed consistently in all prior assessments, as well as through case law of the CJEU[10]: while the term 'adequacy' implies otherwise, the test applied during an assessment is not of adequacy, but equivalence to EU law.

Given the GDPR's recent entry into force and the recent transposition deadline of the Law Enforcement Directive, it is unsurprising that no adequacy decisions have been issued yet under current law. However, under the Data Protection Directive, adequacy assessments have been successfully completed for Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework which is discussed further below). While these assessments were conducted under past law, the GDPR contains a clause (Article 45.9) that provides for their continued legal validity. Adequacy talks are furthermore currently ongoing with Japan and South Korea.

Current adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive. It should therefore be stressed that there is no experience yet in the application of the adequacy model in the context of law enforcement, which is likely to be a complicating factor for a future assessment of the UK.

The procedure applied during an adequacy assessment is summarily prescribed in Article 45 of the GDPR, and in greater detail in a Working Document from the Article 29 Working Party from 1992[11], which has been partially updated in early 2017 to reflect the changing expectations caused by the GDPR and to incorporate the priorities introduced by case law

[10] Notably in the Schrems case; Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§ 73-74).
[11] Working Document WP12 on the Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive; adopted by the Working Party on 24 July 1998.

from the CJEU, notably in the Schrems case[12] that ultimately invalidated the adequacy decision in relation to the US Safe Harbour regime. As of the entry into application of the GDPR, the Article 29 Working Party has been replaced by the so-called European Data Protection Board, which is competent (among other topics) for issuing new guidelines on the interpretation and application of data protection law. Nonetheless, until new guidance is issued by the European Data Protection Board, the Working Document of the Working Party as amended in 2017 remains authoritative on the procedural issues surrounding adequacy assessments.

From a purely legislative perspective, the GDPR requires that the Commission, when assessing the adequacy of the level of protection, in particular takes account of the following elements (emphasis added):

Table 2- Required elements of an adequacy assessment

(a) the **rule of law**, respect for **human rights and fundamental freedoms**, relevant legislation, both general and sectoral, **including concerning public security, defence, national security and criminal law and the access of public authorities to personal data**, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including **rules for the onward transfer** of personal data to another third country or international organisation which are complied with in that country or international organisation, **case-law**, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; (b) the existence and effective functioning of one or more **independent supervisory authorities** in the third country or to which an international organisation is subject, with responsibility for **ensuring and enforcing compliance** with the data protection rules, including adequate enforcement powers, for **assisting and advising the data subjects** in exercising their rights and for **cooperation with the supervisory authorities** of the Member States; and (c) the **international commitments the third country or international organisation concerned has entered into**, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Once these elements have been assessed, a report is created by the Commission, which is then submitted to the European Data Protection Board for an assessment, resulting in a report to the European Commission. If positive, the Commission can publish an affirmative adequacy decision via an implementing act, which can encompass an entire third country, a territory or one or more specified sectors within a third country, or an international organisation. Adequacy is thereafter continuously monitored to ensure that the decision remains justified under the terms of the GDPR.

As the list of criteria already suggests, adequacy assessments are a highly demanding process, requiring a detailed study of not only data protection law and relevant case law in the targeted country, but also a broader appreciation of the institutional framework in which a country operates. It is critically important to determine whether the law on the books corresponds to the reality for data subjects, notably whether countries have a well-functioning legal system that allows recourse in case the law is breached. In order words,

[12] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015.

adequacy assessments not only require appropriate law, but also proof of the effectiveness of the law.

In more practical terms, adequacy assessments are essentially conducted as a study in which the targeted country, sector or territory is examined in order to determine whether essential equivalence is achieved. This is done, as explained in greater detail in the aforementioned Working Document of the Article 29 Working Party, by examining certain data protection 'content' principles and 'procedural/enforcement' requirements, which could be seen as a minimum requirement for protection to be adequate.

The content principles are identified and described by the Working Party in its aforementioned Working Document as follows (emphasis added):

Table 3- Art. 29 Working Party content Principles[13]

1) **Concepts**
Basic data protection concepts and/or principles should exist. These do not have to mirror the GDPR terminology but should reflect and be consistent with the concepts enshrined in the European data protection law. By way of example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data".

2) **Grounds for lawful and fair processing for legitimate purposes**
Data must be processed in a lawful, fair and legitimate manner.
The legitimate bases, under which personal data may be lawfully, fairly and legitimately processed should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interest of the data controller or of a third party which does not override the interests of the individual.

3) The **purpose limitation** principle
Data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.

4) The **data quality and proportionality** principle
Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

5) **Data Retention** principle
Data should, as a general rule, be kept for no longer than is necessary for the purposes for which the personal data is processed.

6) The **security and confidentiality** principle
Any entity processing personal data should ensure that the data are processed in a manner that ensures security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The level of the security should take into consideration the state of the art and the related costs.

7) The **transparency** principle
Each individual should be informed of all the main elements of the processing of his/her personal data in a clear, easily accessible, concise, transparent and intelligible form. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to him/her and other information insofar as this is necessary to ensure fairness. Under certain conditions, some exceptions to this right for information can exist, such as for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

8) The **right of access, rectification, erasure and objection**
The data subject should have the right to obtain confirmation about whether or not data processing concerning him / her is taking place as well as access his/her data, including obtaining a copy of all data relating to him/her that are processed.

[13] Art. 29 Data Protection Working Party, Adequacy Referential (updated), WP254, 17/EN, Adopted on 28 November 2017, A. Content Principles, p. 5-7.

The data subject should have the right to obtain rectification of his/her data as appropriate, for example, where they are inaccurate or incomplete and erasure of his/her personal data when, for example, their processing is no longer necessary or unlawful.

The data subject should also have the right to object on compelling legitimate grounds relating to his/her particular situation, at any time, to the processing of his/her data under specific conditions established in the third country legal framework. In the GDPR, for example, such conditions include when the processing is necessary for the performance of a task carried out in the public interest or when it is necessary for the exercise of official authority vested in the controller or when the processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party.

The exercise of those rights should not be excessively cumbersome for the data subject. Possible restrictions to these rights could exist for example to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 of the GDPR.

The non-existence of the rights to data portability or the restriction of processing in the third country's or international organization's system, should not be an obstacle for it to be recognized as ensuring essential equivalence with the EU framework. However, the existence of these rights would be considered as a plus.

9) Restrictions on **onward transfers**
Further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.

Furthermore, the guidance indicates that provisions should be integrated to address the specific context of special categories of data, direct marketing, and automated decision making and profiling.
The procedural/ enforcement requirements are listed as follows (emphasis added):

Table 4- Procedural / enforcement requirements Art. 29 Working Party[14]

1) **Competent Independent Supervisory Authority**
One or more independent supervisory authorities, tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions in the third country should exist. The supervisory authority shall act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In that context, the supervisory authority should have all the necessary and available powers and missions to ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able, on its own initiative, to conduct investigations.

2) The data protection system must ensure a **good level of compliance**
A third country system should ensure a high degree of accountability and of awareness among data controllers and those processing personal data on their behalf of their obligations, tasks and responsibilities, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials

3) **Accountability**
A third country data protection framework should oblige data controllers and/or those processing personal data on their behalf to comply with it and to be able to demonstrate such compliance in particular to the competent supervisory authority. Such measures may include for example data protection impact assessments, the keeping of records or log files of data processing activities for an appropriate period of time, the designation of a data protection officer or data protection by design and by default.

4) The data protection system must **provide support and help to individual data subjects in the exercise**

[14] Ibid., p. 8.

of their rights and appropriate redress mechanisms
The individual should be able to pursue legal remedies to enforce his/her rights rapidly and effectively, and without prohibitive cost, as well as to ensure compliance. To do so there must be in place supervision mechanisms allowing for independent investigation of complaints and enabling any infringements of the right to data protection and respect for private life to be identified and punished in practice.
Where rules are not complied with, the data subject should be provided as well with effective administrative and judicial redress, including for compensation for damages as a result of the unlawful processing of his/her personal data. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

It is worth highlighting that, in the 2017 revision of the Working Document, a new chapter was introduced to address essential guarantees for law enforcement and national security access. In this Chapter, the Working Party references the Schrems case, in which the prior adequacy decision for the United States of America (USA) – the Safe Harbor mechanism – was invalidated, with the CJEU noting in its ruling that the decision did "not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives, such as national security."

Therefore, the Working Party references a separate Working Document, in which essential guarantees reflecting the jurisprudence of the CJEU and the European Court of Human Rights (ECHR) in the field of surveillance are identified. Four guarantees need to be respected for access to data, whether for national security purposes or for law enforcement purposes, by all third countries in order to be considered adequate:

1) Processing should be based on clear, precise and accessible rules (legal basis)
2) Necessity and proportionality with regards to legitimate objectives pursued need
3) to be demonstrated
4) The processing has to be subject to independent oversight
5) Effective remedies need to be available to the individuals[15]

Thus, the subject matter of law enforcement is likely to face heightened scrutiny, even for adequacy assessments organised under the GDPR (as opposed to assessments under the Law Enforcement Directive).

Given these requirements, it is unsurprising that the process for completing an adequacy assessment may be lengthy and complicated. The presently ongoing assessment of Japan was initiated in January 2017[16], and while this assessment is nearing completion, a final decision has not yet been made. Thus far, a timeline of 18 months for the completion of the assessment process is indicative.

4.2. Application to the UK

Adequacy decisions are thus not a formality, nor a simple and easy process. Part of the complexity of course originates from the need to examine foreign data protection laws in detail, and to appreciate whether the legal system of that country in general is conducive to supporting the effectiveness of the law in question. This is typically not a trivial matter.

In the case of the UK however, such a process should be significantly more expedient, at least for an adequacy decision under the GDPR. The Commission has highlighted in its 2017

[15] Working Document WP 237 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees).
[16] Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection, http://europa.eu/rapid/press-release_STATEMENT-17-1880_en.htm.

Communication on Exchanging and Protecting Personal Data in a Globalised World that the following criteria are taken into account when assessing with which third countries a dialogue on adequacy should be pursued:

1) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
2) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
3) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
4) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level. [17]

Following these criteria, the UK should be a high priority partner for opening adequacy discussions. Furthermore, based on the fact that the UK's data protection law has evolved in tandem with the EU's, and on the fact that the UK has already announced its intention to adopt data protection law which is closely aligned to the GDPR, an adequacy assessment for the UK should be a significantly more expedient process than for non-European countries that do not benefit from this shared history. The UK Government also appears to take this position, as its July 2018 White Paper indicated that "the UK believes that the EU's adequacy framework provides the right starting point for the arrangements the UK and the EU should agree on data protection"[18].

This does not imply that an affirmative adequacy assessment for the UK would automatically follow, since this depends on how exactly the UK adheres to the GDPR, and how it implements the Law Enforcement Directive. A complicating factor will be the issue of the UK's strategic transatlantic cooperation on national security and law enforcement, notably with the USA and in the Five Eyes Alliance, in relation to security and defence, and its own legislation in relation to governmental surveillance powers and information gathering, including the Investigatory Powers Act 2016. Given recurring questions on the treatment and protection of European personal data by some members of this alliance, which were part of the driver behind the CJEU's annulment of the EU-USA Safe Harbor framework, it is likely that guarantees surrounding the onward transfer principle would be sought as a pre-condition to an affirmative adequacy finding. This situation is however not substantially different from that of Canada and New Zealand, both of whom are Five Eyes members who have obtained an affirmative adequacy finding in the past. The compatibility of UK surveillance law with the GDPR will however undoubtedly be a matter for assessment.

However, in addition, the UK's position on immigration law in the Data Protection Act 2018 may cause concern, as the Act explicitly states that "the GDPR provisions listed in sub-paragraph (2) do not apply to personal data processed for any of the following purposes:
(a) the maintenance of effective immigration control, or
(b) the investigation or detection of activities that would undermine the maintenance of effective immigration control, to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b)".

[17] Communication from the commission to the European Parliament and the Council - Exchanging and Protecting Personal Data in a Globalised World, 10 January 2017, COM(2017) 7 final; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN.

[18] Future Relationship between the United Kingdom and the European Union, White Paper from the UK Government, published 12 July 2018, 94. See https://www.gov.uk/government/publications/the-future-re lationship-between-the-united-kingdom-and-the-european-union.

Sub-paragraph (2) of the Act references the data subject rights to transparency, access to data, safeguards for third country transfers, right to erasure, restriction of processing, and objections to processing.

A generic exclusion of these rights, without further mitigating measures or requirement to justify this, may be found to be at odds with the provisions of the GDPR. This is not the sole potential point of contention: in its July 2018 White Paper, the UK Government noted its desire for a partnership that would "respect the sovereignty of the UK and the autonomy of EU decision making. The UK will play no formal role in EU decision making and will make independent decisions in foreign policy, defence and development. National security will remain the sole responsibility of the UK and Member States respectively"[19]. While the same Paper also acknowledges that this relationship must be underpinned by appropriate safeguards, including comprehensive data protection arrangements, it may prove challenging to reconcile the desired complete sovereignty with the need to adhere to EU data protection standards. Thus, an adequacy assessment for the UK is not necessarily a quick and easy process, nor does it have a predictable affirmative outcome.

Furthermore, it is worth repeating the timing challenge: an adequacy assessment is only open to third countries, meaning that the formal assessment could only be initiated *after* Brexit. As such, the adequacy process alone would not be sufficient to avoid disruptions in the free flow of personal data. Thus, while it is positive that the UK Government's White Paper indicates that "The UK is ready to begin preliminary discussions on an adequacy assessment so that a data protection agreement is in place by the end of the implementation period at the latest", the timing in practice may be more challenging: one can discuss, but not formally assess adequacy prior to Brexit.

4.3. A Privacy Shield for the UK?

As was briefly highlighted above, adequacy assessments need not apply to a country as a whole. It is possible for an assessment to target only a specific sector (as is e.g. the case for the Canadian adequacy assessment) or a specific region. In the same manner, the USA have not sought an adequacy assessment for the country as a whole, but have implemented the so-called Privacy Shield in coordination with the European Commission. Under the Privacy Shield arrangement, undertakings in the USA may voluntarily choose to register their participation, indicating in that manner that they have agreed to abide by European data protection principles. As such, European companies that wish to do business with USA based partners can examine whether the company in question is listed in the Privacy Shield register; if so, it can benefit from the adequacy assessment that granted European legal validity to the mechanism.

The Privacy Shield was introduced in response to the Schrems ruling from the CJEU which overturned the legal recognition of the precursor of the Privacy Shield, the Safe Harbor. While the logic and self-certification approach of the Privacy Shield is comparable to that of the Safe Harbor, the Safe Harbor was ultimately terminated due to the fact that national security, public interest, or law enforcement requirements were all explicitly labelled as lawful reasons to override the data protection principles entirely, and due to the lack of effective recourse mechanisms for EU citizens. The Privacy Shield aims to address these issues through stronger safeguards. It should be noted however that the Privacy Shield has not yet been assessed by the CJEU.

Such a self-certification approach could of course also be viable for the UK. However, given the existing legal framework and strong data protection history in the UK, a general adequacy assessment may be preferable, especially when taking into account that the

[19] Future Relationship between the United Kingdom and the European Union, White Paper from the UK Government, published 12 July 2018, Executive Summary. See https://www.gov.uk/government/publications/the-future-relationship-between-the-united-kingdom-and-the-european-union.

negotiation, conclusion and formalisation of a Privacy Shield-like arrangement will likely be more time consuming and significantly less impactful than a general adequacy finding.

5. PERSONAL DATA TRANSFERS BETWEEN THE EU AND THE UK

KEY FINDINGS

- The currently available policy instruments are unable to sustain third country transfers between the EU and UK post-Brexit without further accompanying measures. A tailored ad-hoc solution is necessary, as a minimum and as a complement to an adequacy finding, if these transfers are to be continued
- Ad hoc instruments by definition would be suitable, as they are created to resolve a specific problem, but might be challenging to put in place in the shorter term given the complexities of current data flows. If an ad hoc instrument is applied, a horizontal approach identifying all desired policy areas where data exchange should occur is preferable, rather than an instrument that amends individual legislation; given the breadth and variety in existing rules, the risk of gaps is high. It is worth underlining that, to the extent that there would be a joint desire from the UK and the EU to ensure the UK's continued participation in EU data protection governance (notably by participating in the European Data Protection Board and in the one-stop-shop mechanism), an ad hoc instrument would be the only viable option; no other option – including EEA or European Free Trade Association (EFTA) status – would have this effect.
- If the UK would seek an EEA/EFTA status, this would likely be the outcome of a broader negotiation strategy rather than as a solution to resolve data protection issues alone. Nonetheless, EEA/EFTA status could address some of the issues described above, but not all: EEA/EFTA countries do not contribute to the governance of EU data protection policy in the same manner as Member States do, nor is their participation in national security initiatives assured

5.1. Private sector transfers

While this study principally examines data flows from a public sector perspective due to its greater complexity, it is worth briefly recalling what the implications of Brexit would be for purely private sector transfers (i.e. in a B2B context). In the absence of a bespoke arrangement, an affirmative adequacy assessment of UK data protection law, and EEA status for the UK – all of which could *de facto* ensure that private sector transfers remain possible in largely the same manner as for a Member State – the tools described in section 3.1 of this study are available to private undertakings to organize transfers of personal data to the UK (and presumably also vice versa, although this is subject solely to the UK's own national data protection legislation).

These can be briefly described and assessed as follows:

- **Binding corporate rules** allow a group of undertakings, typically within a large multinational organisation, to adopt and agree to adhere to a common set of legally binding data protection policies that meet the standards of European data protection law. BCRs must be BCRs approved by the competent data protection authorities. After approval and rollout, the entities in the group can transfer personal data between each other freely. BCRs are generally considered to provide a strong and credible level of data protection, and significant efforts have been undertaken to

streamline the approval process. Nonetheless, BCRs have limited potential for resolving Brexit challenges: by design they are limited to a specific exchange context of a group, making them unsuitable for an open data ecosystem. Furthermore, the efforts and knowhow involved in creating BCRs and obtaining an approval from all relevant authorities make BCRs inaccessible to SMEs, or to any organisation that does not have significant data protection knowledge available. For that reason alone, BCRs continue to be highly useful for large multinational groups, but are unsuited to address Brexit.

- **Standard data protection clauses (standard contractual clauses or SCCs)** allow any contracting parties to integrate the template SCCs approved by the Commission in their contracts, in order to ensure the application of European data protection principles. Upon conclusion, data transfers can be organised without further approvals from any data protection authority. As the templates are freely available, they are accessible to anyone. For that reason, they offer significant flexibility and ease of use. Nonetheless, SCCs are not a panacea. Leaving aside the fact that the current SCCs are still undergoing revision to improve alignment with the GDPR, and that appropriate SCC models are not available for all types of data protection roles (e.g. there are no processor to processor SCCs at this time), the main drawback is that SCCs are a purely contractual tool, and therefore by definition require negotiation and integration into all business relationships requiring personal data processing. They do not apply automatically, and while integration into online contracts can be easy (e.g. through simple reference in existing terms and conditions) and painless, for ad hoc business relationships they do establish an additional burden. The expedience with which the EU-US Safe Harbor regime was replaced by the Privacy Shield as described above was partially due to the awareness that, in the absence of such a regime, US companies would be required to principally rely on SCCs, which was seen as an additional administrative burden and cost. The same would apply to Brexit as well.
- **Codes of conduct and certifications which have been approved by a Data Protection Authority (DPA) and by the European Data Protection Board** have a significant potential to facilitate the free flow of data, including between the UK and the EU. However, as conceptualised in the GDPR, it is unlikely that these tools offer short term recourse for a significant number of data flows between the UK and the EU. Firstly, both codes of conduct and certification mechanisms must be clearly defined, including the exact data protection safeguards that they would impose on adhering parties. The creation and approval of such documents is not trivial: there is presently no certification mechanism, and the past 23 years of data protection law in the EU have yielded one code of conduct, namely the Federation of European Direct and Interactive Marketing (FEDMA) code of conduct on direct marketing. The process of finalising a code and negotiating it with European data protection authorities generally takes around 4 years, meaning that they are more cumbersome to put in place than adequacy assessments. Secondly, their scoping is limited to voluntary participants: companies must choose to sign up to a code of conduct or to seek certification. This implies an additional compliance burden that needs to be satisfied on an individual basis, which may be unappealing or inviable especially for SMEs. Finally, it should be stressed that the GDPR is more stringent than the preceding Data Protection Directive in relation to codes of conduct and certification, requiring them to be monitored by specialised monitoring bodies, which must also be approved by a data protection authority. No such monitoring bodies exist at this time, and while this will likely change in the relatively short term, it

means that codes of conduct or certification are presently not an available option for data transfers.

- Finally, the GDPR also permits the use of **ad hoc contractual clauses subject to prior approval of the DPA.** Under this mechanism, specific contractual clauses would need to be developed that sustain bilateral exchanges between the UK and EU, which would need to be approved within the EU, and presumably also by the UK DPA. While conceptually interesting, challenges are the same as for the general SCCs described above: the mechanism is burdensome for companies, and does not ensure that all data exchanges are covered effectively.

Thus, the overview above shows that, even in the absence of a more permanent solution such as bespoke agreement, adequacy finding or EEA status, solutions are available to organise data flows in the private sector. However and more importantly, it also shows that all of these instruments have significant flaws and drawbacks, and a systemic reliance on them – even if only for a purely transitory period – would likely trigger significant compliance costs and burdens, and is likely to leave some data exchanges in a legal gray area due to the need to apply these tools on a transfer to transfer basis. Therefore, it is not advisable to rely on such tools to support continuity of data transfers between the EU and the UK.

5.2. Public sector transfers

In information exchanges between administrations (i.e. from the UK to EU bodies, or to public administrations in other Member States), different concerns and solution mechanisms apply. In this section of the study, we will examine internal market data exchanges, i.e. public sector data exchanges which do not fall within the exclusion of Article 2.2 (d) of the GDPR, relating to transfers by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Such law enforcement transfers will be addressed in the next section.

5.2.1. Internal market data exchanges

Internal market transfers between public administrations face some additional complexities. The most trivial of these is that, while the GDPR remains the generally applicable law, EU bodies must presently still take into account the legal framework of Regulation No 45/2001, which governs the processing of personal data by the European institutions. While this instrument similarly recognises the importance of adequacy decisions as a mechanism for personal data exchanges, it also stresses the possibility of permitting data exchanges on the basis of a legally binding and enforceable instrument between public authorities or bodies, an option also supported by the GDPR. In other words, while data processing in the public sector is generally governed by the GDPR and/or Regulation No 45/2001, additional regulations can be in place that support exchanges of personal data, including towards third countries.

Such additional regulations can be based on the adequacy paradigm, but alternatives also occur, depending on the specificities of the data transfer, i.e. on the nature of the personal data, the purposes of processing, and the entities involved. Such alternatives include[20]:

- National treatment - Foreign persons, entities, and products are generally treated in the same manner as domestic ones, and regardless of the foreign regulatory regime

[20] Drawn from the Commission Staff Working Document on EU equivalence decisions in financial services policy: an assessment, 27 February 2017, SWD(2017) 102 final https://ec.europa.eu/info/sites/info/files/eu-equivalence-decisions-assessment-27022017_en.pdf. The Working Document is thus specific to the financial services market, but the alternatives occur more broadly in other sectors as well.

they should comply with the same requirements as imposed on domestic operators. As a result, there is no need for the domestic regulator to develop a detailed understanding of foreign regulatory regimes.

- Exemptions – Some other countries focus on selected regulatory aspects of cross-border activity of foreign firms. Some of these jurisdictions leave considerable discretion to supervisors and are in position to apply broad exemptions.
- Passporting – This is a system based on a single authorisation/registration which allows for the provision of services within the area under the supervision of a single ("home") authority. However, passporting may require an international treaty or similar legal instrument, including an agreement on a common set of rules which permits market access.
- International agreements – These involve mutual commitments of two or more jurisdictions to reduce overlaps and enhance regulatory and supervisory reliance.

The application of these approaches (equivalence and alternatives) in internal market data exchange depends on the sector; they are common e.g. in the financial sector, but occur less frequently in others. A horizontal application of these alternatives for data protection law in general (without restriction to a specific sector or policy) would not appear viable, due to the fact that their greater flexibility makes them more suitable only for policy areas that are not confronted with significant personal data challenges and sensitivities, or for which there is a national supervisory body with effective monitoring and enforcement powers to ensure that the level of protection is not diminished after a transfer. It would be feasible to examine key policy areas and determine whether the alternatives to adequacy would be feasible for the UK, in the same way and under the same terms as for other countries.

Based on the desk research of the selected DGs and Agencies, such an approach might be appropriate in particular for policy areas that are largely internal market oriented, including financial services, consumer protection, health and food safety, mobility and logistics. By way of example, EASA already has participation from Member States, Switzerland, Norway, Iceland and Liechtenstein, and four international permanent representations in Montreal (Canada), Washington (United States of America), Beijing (China) and Singapore. Similarly, the EBA allows information exchanges with national authorities provided that they are bound to an equivalent duty of professional secrecy.

Mechanisms for transfers with third countries thus already exist in some policy areas, which could be leveraged and integrated into a more general agreement on data transfers between the UK and EU. This implies of course that a legal framework is created that provides a legal basis for these transfers under conditions that ensure essentially equivalent levels of protection in receiving administrations outside the EU; the alternative approaches listed above cannot stand on their own in the absence of appropriate measures to ensure such essential equivalence.

It should be noted that transfers of personal data in many of these policy areas are conditional at least to some extent on legal and policy alignment: given the purpose restriction principle, it should be ensured that personal data, after a transfer, is processed only for purposes which are compatible with those of the originator. Examples include taxation and trade defense: exchanges of information may be difficult to justify in the absence of significant policy alignment which ensures that data would be used only for compatible purposes. Thus, data protection cannot be considered in isolation: it must be ensured that personal data does not become free to use after a transfer.

5.2.2. Three political complexities

Three additional political complexities arise. Firstly, to ensure a full alignment of UK data protection law and policy with that of the EU, it may not be sufficient to ensure that the UK has implemented laws and policies that are essentially equivalent to those of the EU. EU data protection law is shaped by a broad range of interpretations, including decisions from the CJEU and the opinions of the European Data Protection Board (as the successor to the past Article 29 Working Party). Full alignment between the EU and UK in a manner that ensures that data transfers are permissible between the EU and UK as between Member States would imply that these non-legislative sources of law are adhered to in the UK as well.

Similarly, if the objective is to ensure that the UK retains a role as a country contributing to EU data protection regulations and policies – not only as a country receiving such regulations and policies, but as a country contributing to it – a way must be found to integrate the UK into governance bodies such as the European Data Protection Board. This preference was stated by the Prime Minister of the UK[21], indicating that it was "seeking more than just an adequacy arrangement" and that (…) "we will be seeking more than just an adequacy arrangement and want to see an appropriate ongoing role for the ICO. This will ensure UK businesses are effectively represented under the EU's new 'one stop shop' mechanism for resolving data protection disputes".

In addition, the UK Government has stated its desire to participate in the GDPR's so-called one-stop-shop mechanism[22]. This mechanism, established by Articles 56 and 60 of the GDPR allows data controllers who are subject to the jurisdiction of multiple Member States and multiple data protection authorities to communicate with a single lead supervisory authority, who will thereafter liaise as needed with other supervisory authorities concerned. The availability of a one-stop-shop mechanism can therefore increase the effectiveness and efficiency of data protection enforcement actions, and participation of the UK's data protection authority in this mechanism may be seen as mutually beneficial.

This objective is however politically challenging, given that no non-Member State presently has such a status as a contributor (including EEA countries who, contrary to the UK in a post-Brexit scenario, are bound by rulings from the CJEU and opinions from the European Data Protection Board). This objective can therefore only be reached through a bespoke arrangement, since none of the available policy tools – including adequacy assessments – could permit the UK to participate in and contribute to the EU's data protection laws and policies.

Finally, as was already highlighted earlier, the UK's law enforcement and surveillance policy and its position in the Five Eyes Alliance might create stress on the application of the alternative transfer mechanisms. While this may appear like a purely law enforcement issue (examined in greater detail in the next section of this study), it will also create pressure on purely internal market exchanges, notably due to the risk that personal data intended for purely internal market purposes would be re-used for law enforcement purposes as well. Thus, the integration of appropriate safeguards on purpose limitation, onward transfer, and effective monitoring and supervision will be critical to organise internal market transfers, irrespective of the chosen instrument.

[21] PM speech on the future economic partnership with the European Union, 2 March 2018; see https://www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union.

[22] Future Relationship between the United Kingdom and the European Union, White Paper from the UK Government, published 12 July 2018, 11. See https://www.gov.uk/government/publications/the-future-relationship-between-the-united-kingdom-and-the-european-union.

5.3. National security and law enforcement

As was highlighted above, the GDPR does not apply to transfers by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (briefly referred to in this section as law enforcement processing). Such transfers are instead governed by the Law Enforcement Directive for the Member States, which must be transposed into national law, and by Regulation No 45/2001 for EU bodies and institutions. As described earlier, the Law Enforcement Directive has a separate adequacy assessment process in Article 36, implying that it is possible for a country to receive a general adequacy assessment under the GDPR, or a more targeted assessment which covers only law enforcement under the Law Enforcement Directive, or both. No assessments have yet occurred under the Law Enforcement Directive, and it remains to be seen what the process applied for such assessments would be.

The UK has repeatedly highlighted its desire to continue cooperation with the EU on national security and law enforcement issues. In its July 2018 White Paper, the UK Government noted that "the UK seeks an ambitious partnership covering the breadth of security interests including foreign policy, defence, development, law enforcement and criminal justice cooperation. It should be supported by ongoing cooperation through partnership programmes and key safeguards such as individual rights, data protection and robust governance arrangements, to underpin the trust which is essential to such a close relationship". While no details were provided in the Paper on how this would be achieved, the continuation of personal data exchanges in this context is therefore a political objective from the UK's perspective.

5.3.1. Options for cooperation with third countries

A recent study for the LIBE Committee[23] examined the implications of Brexit for the Area of Freedom, Security and Justice in great detail. The study mapped the UK's participation in legislation and policies on border checks, asylum and immigration, on judicial cooperation in civil and criminal matters, on police cooperation and on the protection of personal data for the purposes of law enforcement. It found systemic challenges and a high risk of disruptions in the free flow of data, not only because of the UK's impending third country status, but also due to the breadth and specificity of legislative instruments in this policy area that establish ad hoc exchange opportunities with third countries. In more practical terms, cooperation with third countries is already possible in some policy areas, depending on specific agreements or recognition processes, but not in others. An affirmative adequacy assessment for such transfers is not a panacea that would resolve all potential challenges.

By way of examples on cooperation options with third countries:

5.3.1.1. The EU-LISA Regulation

The eu-LISA Regulation states that ""Under the relevant provisions of their association agreements, arrangements shall be made in order to specify, inter alia, the nature and extent of, and the detailed rules for, the participation by countries associated with the implementation, application and development of the Schengen acquis and Eurodac-related measures in the work of the Agency, including provisions on financial contributions, staff and voting rights."[24] Thus, subject to the adoption of a bespoke exit agreement with the

[23] European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, The implications of the United Kingdom's withdrawal from the European Union for the Area of Freedom, Security and Justice, Study for the LIBE Committee, December 2017; see http://www .europarl.europa .eu/RegData/etudes/ STUD/2017 /596824/IPOL_STU%282017%29596824_EN.pdf.

[24] Regulation (EU)No. 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, L 286/1, Art.37.

UK, the UK could be permitted to use eu-LISA infrastructure (such as SIS II, Eurodac, etc). Since the UK participates in SIS II, ECRIS, EU PNR, Eurodac and the Prüm Decision, withdrawal from the EU would otherwise imply that the UK will no longer have access to the information held in these databases.

5.3.1.2. The Eurojust legal framework

Similarly to the eu-LISA Regulation, the Eurojust legal framework allows the EU to conclude cooperation agreements and memoranda of understanding with third countries, international organisations or bodies[25]. For example, Eurojust has signed an agreement for the exchange of necessary information, including personal data with OLAF and a memorandum of understanding with Frontex.[26] With respect to third countries Eurojust currently has agreements with nine third countries in which data protection clauses require the signatories to provide a level of protection at least equivalent to that resulting from the principles contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and the amendments thereto as well as the principles laid down in the Eurojust Decision and in the Eurojust rules of procedure on data protection.[27] Possibly a similar structure could be set up with the UK law enforcement authorities. From its inception, the UK has been an active member of Eurojust, both financially and operationally, and it would be harmful to cede any operational activities of Eurojust which necessitate cooperation with or directly involve UK authorities, transitional agreements are imperative. However, the Eurojust legal framework allows ad hoc cooperation in Eurojust casework. In 2017, 93 cases were counted in which cooperation with third states without an agreement took place.[28] If negotiations do not amount to a comprehensive deal, a fall-back option could thus be to work together on an ad hoc casework basis without an agreement.

5.3.1.3. The Europol Regulation

In the same vein, the Europol Regulation (EU) 2016/794[29] introduces (in its Article 25) specific rules and legal bases regarding transfers of data by Europol outside the EU[30]. One possibility would be an adequacy decision of the Commission in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country to which Europol transfers data ensures an adequate level of protection. As there are no such adequacy decisions in place at the moment, the alternative for Europol to regularly transfer data to a third country is to use an appropriate framework resulting from the conclusion of a binding international agreement between the EU and the receiving third country.

There are already international agreements in place which grant Europol the right to exchange personal data with third countries. Current international agreements concluded by Europol with third countries can be divided into two categories: strategic agreements[31] and operational agreements[32]. Strategic agreements focus on the exchange of general

[25] For a more elaborate overview of Eurojust, see: Annex III – A.3 – Eurojust.
[26] See: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/ Practical% 20Agreement%20on%20arrangements%20of%20cooperation%20between%20Eurojust%20and%20OLAF%20(2008)/Eurojust-OLAF-2008-09-24-EN.pdf and http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/ Memorandum%20of%20Understanding%20between%20Eurojust%20and%20Frontex%20(2013)/Frontex-Eurojust-2013-12-18_EN.pdf.
[27] See: http://www.eurojust.europa.eu/about/legal-framework/Pages/eurojust-legal-framework.aspx ; with the exception of the United States.
[28] Eurojust, Annual Report 2017, see: Annex III – A.3 - Eurojust http:// www.eurojust. europa.eu /do cli bra ry/corporate/eurojust%20Annual%20Reports/Annual%20Report%202017/AR2017_EN.pdf.
[29] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA; see https://eur-lex.europa.eu/legal-cont ent/EN/TXT/?uri=CELEX%3A32016R0794
[30] For a more elaborate overview of Europol, see: Annex III – A.4 – Europol.
[31] See https://www.europol.europa.eu/partners-agreements/strategic-agreements.
[32] See https://www.europol.europa.eu/partners-agreements/operational-agreements.

intelligence as well as strategic and technical information, and as such none of these[33] cover the exchange of personal data. The latter however[34] do permit personal data exchanges when required to satisfy operational goals. By way of example, the agreement in place between Europol and Australia permits the provision of personal data to Australia under Article 9, but also includes a number of conditions for such exchanges. Notably, it requires Australia to comply with the following conditions for all transmissions of personal data by Europol to Australia:
1) after receipt, if requested by Europol, Australia shall inform Europol of the use made of the data and the results achieved therefrom;
2) the data shall not be communicated by Australia to third States or bodies, except with the prior consent of Europol;
3) onward transmission of the data by the initial recipient shall be restricted to the competent authorities mentioned in Article 6 of the Agreement and shall take place under the same conditions as those applying to the original transmission;
4) the supply must be necessary in individual cases for the purpose of preventing or combating the criminal offences referred to in Article 3 (1) of the Agreement;
5) any conditions on the use of the data specified by Europol must be respected;
6) when data are supplied on request, the request for the data must specify indications as to the purpose of and the reason for the request. In the absence of this the data shall not be transmitted;
7) the data may be used only for the purpose for which they were communicated;
8) the data shall be corrected and/or deleted by Australia if it emerges that they are incorrect, inaccurate, no longer up to date or should not have been transmitted;
9) the data shall be deleted when they are no longer necessary for the purpose for which they were transmitted.

Furthermore, a series of high level requirements for ensuring the security of the data are specified in the Agreement. Thus, personal data exchanges between Europol and third countries can and do occur, but require specific agreements to be put in place. It is worth noting that this is the case even for countries which have obtained an affirmative adequacy decision (such as Canada), and even for EEA countries (such as Iceland or Liechtenstein).

Finally, when assessing the potential impact of Brexit, it should be noted that Europol applies the originator principle to its information sources. Enshrined for Europol in Article 5 of the Decision of the Management Board of Europol laying down the rules concerning access to Europol documents[35], this principle basically entails that the originator of the data – usually a Member State – determines the level of dissemination to third parties which is permissible. A Member State may e.g. decide to share information with all Member States, or only with Europol. Brexit therefore implies that the UK might choose to no longer permit any level of dissemination of its information, thereby effectively withdrawing its information from Europol's databases. Similar risks apply to other databases, either because of a similar originator principle (which can be found e.g. also in Article 9 of Regulation (EC) No 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents), or because of a strict application of the lawfulness and purpose restriction principles under data protection law: since the legal basis and the purpose of data sharing has disappeared, the data should be deleted. This would negatively impact the effectiveness of such databases.

[33] Currently in place with China, Russia, Turkey and the United Arab Emirates.
[34] Currently in place with Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, the Former Yugoslav Republic of Macedonia, Georgia, Iceland, Liechtenstein, Moldova, Monaco and Montenegro.
[35] See https://www.europol.europa.eu/publications-documents/decision-of-europol-management-board-laying-down-rules-concerning-access-to-europol-documents.

5.3.1.4. Passenger name records

With the goal of combatting serious (transnational) crime and terrorism**,** passenger name records (PNR's) agreements have been signed bilaterally with third countries, including some without an affirmative adequacy finding.[36] Following the PNR Directive, airline carriers transfer personal information data of their passengers to the authorities of Member States. This concerns flights entering or departing the EU and in some instances intra-EU flights.

Regulated by various limitations, PNR data is used for various purposes; it can be employed for the identification of specific individuals by assessing the data against certain risk criteria. Interestingly, according to an opinion released by the CJEU in July 2017, the bilateral PNR agreement as negotiated by Canada and the EU in 2014 must be revised. The Court concluded "that the provisions of the agreement on the transfer of sensitive data to Canada and on the processing and retention of that data are incompatible with fundamental rights."[37] By allowing Canada to retain PNR data for up to five years and leaving an opening for Canadian authorities to disclose that data to non-EU countries, the agreement is not limited to what is strictly necessary. The agreement now needs to be revised taking into account the concerns voiced by the Court. The Canadian example demonstrates the delicacy of these type of agreements. Nonetheless, the mechanism behind the bilateral PNR agreements and the lessons learned from Canada, may be applied to the UK as well.

5.3.1.5. The Frontex Regulation

Numerous provisions of Regulation (EU) 2016/1624 provide a legal basis for Frontex to cooperate with third countries. Nonetheless, one particular provision, Article 54 – "Cooperation with third countries" sets out the key points of such cooperation. Cooperation with non-EU countries is an integral part of Frontex' mandate to ensure implementation of the European integrated border management (IBM) and one of the strategic priorities for the agency's work. As provided for by Article 54(2), such cooperation is usually based on working arrangements signed between the agency and the competent authorities of the non-EU country. In particular, those working arrangements shall specify the scope, nature and purpose of the cooperation and be related to the management of operational cooperation. The draft arrangements shall receive the Commission's prior approval and the Agency shall inform the European Parliament before a working arrangement is concluded.
The examples serve to illustrate that existing regulations for specific data exchanges in the law enforcement context t times already permit cooperation with third countries, even in the absence of an adequacy finding. However, this does not imply that there would be no challenges for the UK, or that an adequacy finding would not be necessary or useful. Rather, the list shows that, even if there is significant legal and policy alignment, and even if an adequacy finding is issued, specific cooperation obligations are still in place that the UK would need to satisfy, such as the necessity to conclude specific agreements or arrangements to allow the UK to exchange information with EU agencies and with its counterparts in Member States. The exit agreement between the UK and EU should thus recognise this point and attempt to provide a broad legal basis to accede to and participate in such agreements, provided that there is political consensus that this is indeed the shared objective of the EU and UK.

5.3.2. Challenges resulting from UK law enforcement law and policy, notably the Investigative Powers Act 2016

A critical point in this respect will be the UK's adherence to EU data protection principles in law enforcement and surveillance activities. This was clearly illustrated in the Tele2 and Watson case before the CJEU[38], where the UK's data retention regime (notably the 2014

[36] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119/132, 27.4.2016.
[37] Court of Justice of the European Union, Opinion 1/15. Press release No 48/17. Luxembourg. 26 July 2017.
[38] CJEU, Tele2 Sverige AB v. Post– och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others. Joined Cases C-203/15 and C-698/15/ Judgement, 2016.

Data Retention and Investigatory Powers Act (DRIPA) was assessed. In this case, the CJEU held that European data protection law precluded general and indiscriminate retention regimes because they exceeded "the limit of what is strictly necessary and cannot be considered to be justified, within a democratic society."[39]

While the DRIPA has in the meantime been repealed and replaced by the Investigative Powers Act 2016 (IPA), it remains to be seen whether this law satisfies the requirements of the Tele2 and Watson ruling. If not, this is likely to have a negative impact on a potential adequacy decision, and on information flows between the EU and UK in general.

The UK's current approach to the Law Enforcement Directive shows its willingness to continue to align to the EU's data protection approach: while the UK could have chosen to opt out from transposing the Directive into UK national law, it has not done so and has taken action to transpose it by including the rules on data processing for law enforcement purposes in its Data Protection Bill 2017. This is a promising step, but in order to integrate the UK into EU national security and law enforcement initiatives, a bespoke legal instrument would be necessary to amend existing EU regulations under which the UK can currently participate in e.g. immigration and asylum policy, and ensuring EU security, including anti-terrorism, organised crime and police cooperation.

[39] Ibid., para. 107.

6. CONCLUDING REMARKS AND POLICY RECOMMENDATIONS

The existing legal mechanisms and policy measures that are presently used to support the exchange of personal data between the EU and third countries can alleviate some of the concerns surrounding Brexit, but none of these, in isolation or collectively, would be sufficient to permit a continuation of personal data flows and cooperation in relation to data protection on the same basis as today. Notably, an affirmative adequacy finding for the UK (both in relation to data protection in general under the GDPR and in relation to law enforcement under the Law Enforcement Directive) would be highly beneficial, but insufficient to allow a continuation of current information flows. While adequacy findings would be adequate for private sector exchanges, in the public sector – both for internal market exchanges and law enforcement exchanges – a multitude of legal instruments exist beyond general data protection law that determine which countries may participate in information exchanges, and on which basis.

An adequacy finding would be a beneficial step in ensuring the continued integration of the UK in such information exchanges – assuming that there is a mutual understanding that this should be the outcome of negotiations – but it would not be sufficient without a broader legal basis in the form of a bespoke legal agreement that would authorise the UK and EU to continue to participate in information exchanges. Furthermore, it should be noted that an adequacy assessment is generally a lengthy process, the initiation of which could only begin after the UK has left the EU. Therefore, an adequacy finding is insufficient to avoid a temporary standstill in information exchanges, which would be mutually detrimental.

Other common legal instruments used in data protection law to organise personal data exchanges – such as standard contractual clauses, binding corporate rules, certification, codes of conduct and approved ad hoc contractual terms – are equally available to the UK after Brexit, but the use of such instruments is generally resource intensive and unsuitable to set up a broad framework for data exchanges that can be used to organise compliance transfers of personal data at a large scale, including particularly for SMEs.

The analysis therefore shows that, if there is a consensus on the need for continuity in existing personal data exchanges between the EU and the UK, and on the need to ensure continued alignment between data protection law and data protection policy between the EU and the UK, the following approach is recommended:

- Firstly, the negotiations between the UK and the EU should contain a standstill clause that allow the UK and the EU to continue personal data exchanges on the same basis as between the EU and Member States. This agreement should be bilateral, and should also apply to Member State public administrations and private undertakings. Summarily, from a data protection perspective the UK would for all intents and purposes continue to be treated as a Member State, for a period of at least 18 months, which is a reasonable amount of time required for the UK to obtain an affirmative adequacy decision.

- Secondly, the adequacy assessment process for the UK should be initiated as soon as reasonably practicable, i.e. as soon as Brexit becomes effective, both under the GDPR and under the Law Enforcement Directive. This will become the main instrument to ensure facilitated personal data exchanges in the private sector after

the conclusion of the 18 month standstill period. Again, this agreement should be bilateral, since EU Member States must also be recognised as adequate under future UK data protection law.

- Thirdly, the negotiated agreement should contain a provision allowing the UK to participate in the development of common EU data protection policy, notably by contributing to positions of the European Data Protection Board, by participating in the one-stop-shop mechanism, and by ensuring a homogeneous application of EU case law in relation to data protection, including in the UK. This point is likely to be highly politically contentious from both perspectives, as there are currently no non-Member States in the European Data Protection Board, nor are there any non-EU/EEA countries participating in the one-stop-shop, and adherence to rulings from the CJEU in the UK is a point of continued discussion. Furthermore, as of 26 June 2018, the implementation of such an agreement would require a revision of the UK's Withdrawal Act, which emphatically foresees the right for the UK to disregard future case law, and to overturn prior case law. Nonetheless, these are priorities which have been expressed on either side of the negotiation.

- Fourthly and finally, it should be recognised that, even with a standstill period in place, and even after an adequacy finding has been issued, the UK remains a third country, and its participation in current data exchange mechanisms is not ensured, as the examples above have shown. Therefore, the EU and UK must agree on policy areas and data exchanges in which they consider mutual data exchanges to be desirable. The negotiated agreement between the EU and UK should list these policy areas and data exchanges in a transversal manner, both in relation to internal market data transfers, and security and law enforcement initiatives, and commit to the amendment of existing regulations or conclusion of appropriate agreements to ensure the effectiveness of this political agreement.

REFERENCES

- Additional rules defining some specific aspects of the application of the rules on the processing and protection of personal data at Eurojust to non-case-related operations, 27 June 2006, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/dataprotection/Additional%20rules%20defining%20specific%20aspects%20of%20the%20application%20of%20Rules%20on%20Processing%20and%20Protection%20of%20Personal%20Data/additional_dp_rules.pdf.
- Agreement between Eurojust and the Republic of Iceland, 2 December 2005, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20Eurojust-Iceland%20(2005)/Eurojust-Iceland-2005-12-02-EN.pdf.
- Agreement between Eurojust and the United States of America, 6 November 2006, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/ Agreement%20Eurojust-USA%20(2006)/Eurojust-USA-2006-11-06-EN.pdf.
- Agreement between the European Community and Bosnia and Herzegovina on the facilitation of the issuance of visas – Declarations, OJ L 334, 19.12.2007, p. 97–107, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:22007A1219 (06)& qid =1395933932709.
- Agreement between the European Community and the Russian Federation on the facilitation of the issuance of visas to the citizens of the European Union and the Russian Federation, OJ L 129, 17.5.2007, p. 27–34, Special edition in Croatian: Chapter 11 Volume 033 P. 189 – 196, https://eur-lex.europa.eu/legal-content/EN/ALL / ?uri=CELEX:22007A0517(01).
- Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, 14 July 2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0714%2801%29.
- Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186, 14.7.2012, p. 4–16, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0714%2801%29.
- Agreement between the Kingdom of Norway and Eurojust, April 2005, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/ Agreement%20Eurojust-Norway%20(2005)/Eurojust-Norway-2005-04-28-EN.pdf.
- Agreement between the United States of America and the European Community on Cooperation in the Regulation of Civil Aviation Safety, consolidated version of March 2016,https://www.easa.europa.eu/sites/default/files/dfu/Consolidated%20version%20of%20the%20Agreement%20between%20the%20USA%20and%20the%20EU%20on%20cooperation%20in%20the%20regulation%20of%20civil%20aviation%20safety.pdf.
- Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, Augustus 2012, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX%3A22012A0811%2801%29.
- Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, p. 5–14, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0811%2801%29.
- Agreement on cooperation between Eurojust and Montenegro, March 2016, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/ Agreement%20on%20cooperation%20between%20Eurojust%20and%20Montenegro% 20(2016)/Eurojust-Montenegro-2016-03-05-EN.pdf.
- Agreement on cooperation between Eurojust and Switzerland, November 2008, http:// www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/ Agreement%20between%20Eurojust%20and%20Switzerland%20(2008)/Eurojust-Swi tzer land-2008-11-27-EN.pdf.

- Agreement on cooperation between Eurojust and the Former Yugoslav Republic of Macedonia, November 2008, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20on%20cooperation%20between%20Eurojust%20and%20the%20former%20Yugoslav%20Republic%20of%20Macedonia%20(2008)/Eurojust-fYROM-2008-11-28-EN.pdf.
- Agreement on cooperation between Eurojust and the Principality of Liechtenstein, June 2013, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/Agreement%20on%20Cooperation%20between%20Eurojust%20and%20the% 20Principality%20of%20Liechtenstein%20(2013)/Eurojust-Liechtenstein 2013-06-07 EN.pdf.
- Agreement on cooperation between Eurojust and the Republic of Moldova, July 2014 ,http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/ Agreement%20on%20cooperation%20between%20Eurojust%20and%20the%20Republic %20of%20Moldova%20(2014)/Eurojust-Republic-of-Moldova-2014-07-10-EN.pdf.
- Agreement on cooperation between Eurojust and Ukraine, June 2016, http:// www. eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/ Agree ment % 20 on%20cooperation%20between%20Eurojust%20and%20Ukraine%20(2016)/Eurojust-Ukraine-2016-06-27-EN.pdf.
- Agreement on Operational and Strategic Cooperation between Australia and the Eu ro pean Police Office, February 2007, https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1.
- Agreement on Operational and Strategic Cooperation between Ukraine and the European Police Office, December 2016, https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1.
- Agreement on Operational Cooperation between the Kingdom of Denmark and the European Police Office, 28.04.2017, https://www.europol.europa.eu/publications-documents/agreement-operational-and-strategic-cooperation-between-kingdom-of-de nmark-and-europol.
- Art. 29 Data Protection Working Party, Adequacy Referential (updated), WP254, 17/EN, Adopted on 28 November 2017.
- Authorised Economic Operator (AEO) - Processing in the AEO database of data contained in an application to issue AEO certificate by customs authorities in the Member States, DPO-3680.1, 1 July 2014, http://ec.europa.eu/dpo-register/ details .htm?id=34427.
- Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§ 73-74).
- CJEU, Tele2 Sverige AB v. Post– och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others. Joined Cases C-203/15 and C-698/15/ Judgement, 2016.
- Commission Decision 2000/518/EC (OJ L 215, 25.8.2000, p. 1), July 2000, http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0518.
- Commission Decision of 16 August 2006 C (2006) 3602 concerning the security of information systems used by the European Commission, http://ec.europa.eu/internal market/imi-net/docs/decision 3602 2006 en.pdf.
- Commission Decision of 16 December 2009 laying down guidelines for the management of the Community Rapid Information System RAPEX established under Article 12 and of the notification procedure established under Article 11 of Directive 2001/95/EC (the General Product Safety Directive) (notified under document C(2009) 9843), https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=CELEX% 3A32010D0015.
- Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, https://eur-lex.europa.eu/legal-content/ EN/ALL/?uri =CELEX %3A32000D0518.

- Commission Decision of 28 April 1999 establishing the European Anti-fraud Office (OLAF) (notified under document number SEC(1999) 802), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999D0352.
- Commission Delegated Decision (EU) 2016/310 of 26 November 2015 on the equivalence of the solvency regime for insurance and reinsurance undertakings in force in Japan to the regime laid down in Directive 2009/138/EC of the European Parliament and of the Council, https://eur-lex.europa.eu/legal-content/ EN/ALL/ ?uri =CELEX%3A32016D0310.
- Commission Implementing Regulation (EU) 2015/1051 of 1 July 2015 on the modalities for the exercise of the functions of the online dispute resolution platform, on the modalities of the electronic complaint form and on the modalities of the cooperation between contact points provided for in Regulation (EU) No 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes, https://eur-lex.europa.eu/legal-content/ EN/TXT /?uri= urise rv % 3AOJ.L .2015.171.01.0001.01.ENG.
- Commission Regulation (EU) No 16/2011 of 10 January 2011 laying down implementing measures for the Rapid alert system for food and feed Text with EEA relevance, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri =CELEX% 3A32011 R0016.
- Commission Staff Working Document on EU equivalence decisions in financial services policy: an assessment, 27 February 2017, SWD(2017) 102 final https://ec.europa.eu/info/sites/info/files/eu-equivalence-decisions-assessment-27022017 epdf
- Commission Staff Working Document on EU equivalence decisions in financial ser vi ces, February 2017, https://ec.europa.eu/info/sites/info/files/eu-equivalence-de ci sions-assessment-27022017 en.pdf.
- Communication (COM (2006) 789) from the Commission to the Council and the European Parliament Investment research and financial analysts (SEC (2006)1655), December 2006, http://eur-lex.europa.eu/procedure/EN/195097.
- Communication from the Commission to the Council and the European Parliament on European contract law, 2001, https://eur-lex.europa.eu/legal-content/ EN/TXT/ ?uri = CELEX:52001DC0398.
- Communication from the commission to the European Parliament and the Council - Exchanging and Protecting Personal Data in a Globalised World, 10 January 2017, COM(2017) 7 final. See https://eur-lex.europa.eu/legal-content/ EN/TXT/ ?uri= COM 3A2017%3A7%3AFIN.
- Communication from the Commission to the European Parliament and the Council - European Contract Law and the revision of the acquis: the way forward, 11 October 2004, https://eur-lex.europa.eu/legal-content/ en/ALL/?uri =CELEX%3 A52004D C0 651.
- Communication from the Commission to the European Parliament and the Council - A more coherent European contract law - An action plan, 15 March 2003, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52003DC0068.
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Agenda on Migration, 13/05/2015, https://ec.europa.eu/home-a ffairs /sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/ba ck gr ound-information/docs/c ommunication on the european agenda on migration en .pdf.
- Council Decision (2004/904/EC) of 2 December 2004 establishing the European Refugee Fund for the period 2005 to 2010, https://eur-lex.europa.eu/legal-content /EN/TXT/?uri=CELEX:32004D09044.
- Council Decision 2000/596/EC of 28 September 2000 establishing a European Refugee Fund, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri= CE LEX % 3A32 000D0596.
- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex europa.eu/legal-content/EN/ALL/?uri=celex%3A32007D0533.

- Council Decision of 6 April 2009 establishing the European Police Office (Europol), OJ L 121, 15.5.2009, p. 37–66, http://eur-lex.europa.eu/legal-content/ EN/ALL/ ?uri = CELEX:32009D0371.
- Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural mattershttps://eur-lex.europa.eu/legal- cont ent/ EN/TXT/?uri =celex:31997R0515
- Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, https://ec.europa.eu/home-affairs/ sites/ homeaffairs/files/e-library/documents/policies/borders-and-visas/ schengen/ docs/ fron tex regulation consolidated 2011 en.pdf.
- Council Regulation (EEC) No 339/93 of 8 February 1993 on checks for conformity with the rules on product safety in the case of products imported from third countries,https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=celex%3A31993R0339.
- Court of Justice of the European Union, Opinion 1/15. Press release No 48/17. Luxembourg. 26 July 2017, https://curia.europaeu/ jcms/upload/docs/ ap pli ca tion/pdf/2017-07/cp170084en.pdf.
- Data protection contractual clauses related to the administrative arrangement between OLAF and [Partner], https://ec.europa.eu/anti-fraud/sites/ antifraud/files/data protection contractual clauses admin arrangements en.pdf.
- Decision N° 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Tele com munication services) to the EEA Agreement, https://eur-lex.europa. eu/legal- cont ent / EN/TXT/?uri=celex%3A22000D1123%2808%29.
- Decision No 1/2010 of the Joint Customs Cooperation Committee of 24 June 2010 pursuant to Article 21 of the Agreement between the European Community and the Government of Japan on Cooperation and Mutual Administrative Assistance in Customs Matters regarding mutual recognition of Authorised Economic Operators programmes in the European Union and in Japan, https:/ec.europa.e u/taxation customs/sites/taxation/files/docs/body/mutual recognition aeo en.pdf.
- Decision No 1926/2006/EC of the European Parliament and of the Council of 18 December 2006 establishing a programme of Community action in the field of consumer policy (2007-2013), https://eur-lex.europa.eu/legal-content/ EN/A LL/?uri=CELEX%3A32006D1926.
- Decision of the Joint Customs Cooperation Committee established under the Agreement between the European Community and the Government of the People's Republic of China on cooperation and mutual administrative assistance in customs matters of 16 May 2014 regarding mutual recognition of the Authorised Economic Operator programme in the European Union and the Measures on Classified Management of Enterprises Program in the People's Republic of China, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A22014D0772.
- Decision of the US-EU Joint Customs Cooperation Committee of 4 May 2012 regarding mutual recognition of the Customs-Trade Partnership Against Terrorism program in the United States and the Authorised Economic Operators programme of the European Union, https://eur-lex.europa.eu/legal- content / EN/ TXT/ uri= CE LE X %3A22012D0290.
- DG FISMA 2016-2020 Strategic Plan, https://ec.europa.eu/info/ sites/info/files/ stra tegic-plan-2016-2020-dg-fisma april2016 en.pdf.
- DG FISMA mission statement, https://ec.europa.eu/info/departments/financial-sta bi lity -financial-services-and-capital-markets-union/mission-statement-financial-sta bi li ty-financial-services-and-capital-markets-union en.
- DG JUST Organogram, https:// ec.europa. eu/info/ sites/info/files/ organogram en 1.pdf.

- DG Migration and Home Affairs, Management Plan 2018 for the DG Migration and Home Affairs, https://ec.europa.eu/info/sites/info/files/management-plan-home-2018_en.pdf.
- DG MOVE mission statement and 2016-2020 Strategic Plan, https://ec.europa.eu/info/sites/info/files/strategic-plan-2016-2020-dg-move_amended_july_en.pdf. DG SANTE mission statement and 2016-2020 Strategic Plan, https://ec.europa.eu/info/departments/health-and-food-safety_en.
- DG Trade 2016 Annual activity report, https://ec.europa.eu/info/ sites/info/files/file import/ aar-trade-2016_en_0.pdf.
- DG Trade Strategic Plan 2016-2020, https://ec.europa.eu /info/sites/info/files/ tradesp_2016_2020_revised_en.pdf.
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119/132, 27.4.2016.
- Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, https://eur-lex.europa.eu/legal-content/ EN/ALL/?uri =celex:32001L0095.
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, https://eur-lex. europa .eu/legal-content/EN/TXT/?uri=celex:32006L0024.
- Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), https://eur-lex.europa.eu/legal- content/ EN/ ALL/?uri=celex%3A32009L0138.
- Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests, http://eur-lex. europa. eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2009.110.01.0030.01.ENG.
- Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0011.
- Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036.
- Draft administrative cooperation arrangement between the "European Anti-Fraud Office" (OLAF) and [The Partner], https://ec.europa.eu/anti-fraud/ sites/antifraud/files/docs/body/aca_third_countries_and_dp_annex_en.pdf
- ESMA Library, https://www.esma.europa.eu/databases-library/esma-library? page=1&f[0]=im_esma_sections%3A367.
- Eurojust legal framework, http://www.eurojust.europa.eu/about/legal-framework/Pages/eurojust-legal-framework.aspx.
- Eurojust, Annual Report 2017, see: Annex III – A.3 - Eurojust http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202017/AR2017_EN.pdf.

- European Commission Anti-dumping and anti-subsidy safeguard, statistics covering the first 11 months of 2017, http://trade.ec.europa.eu/ doclib/docs/2017/december/tradoc_156415.pdf.
- European Commission website, 'the register exporter system', https://ec.europa.eu/taxation customs/business/calculation-customs-duties/rules-origin/general-aspects -preferential-origin/arrangements-list/generalised-system-preferences/ the register exporter system en.
- European Commission website, The Customs 2020 Programme, https://ec.europa.eu/taxation customs/business/customs-cooperation-programmes/customs-2020-programme en.
- European Commission, Passenger Name Records, https://ec.europa.eu/home-affairs/what- we-do/policies/police-cooperation/information-exchange/pnr en.
- European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, 10 January 2017, https://eur-lex.europa.eu/legal-content/ EN/ TXT/?uri=CELEX:52017PC0008.
- European Commission, The Fiscalis 2020 Programme, https://ec.europa.eu/ taxationcustoms/fiscalis-programme en.
- European Council, Guidelines European Council (Art. 50) meeting (15 December 2017). EUCO XT 20011/17, para. 1. See : https://www.consilium. europa.eu/media / 32236/15-euco-art50-guidelines-en.pdf.
- European Data Protection Supervisor website, 'legislation', https://edps.europa. eu/data -protection/data-protection/legislation en.
- European Data Protection Supervisor, official register, http://ec.europa.eu/dpo-re gister/details.htm?id=42968.
- European Parliament Briefing, EU Legislation in Progress, April 2018, Rules for EU institutions' processing of personal data, http://www.europarl.europa. eu/RegData/etudes/BRIE/2017/608754/EPRS BRI(2017)608754 EN.pdf.
- European Parliament briefing, July 2017, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/587369/IPOL BRI(2016)587369 EN.pdf.
- European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, The implications of the United Kingdom's withdrawal from the European Union for the Area of Freedom, Security and Justice, Study for the LIBE Committee, December 2017,http://www.europarl. europa.eu/ RegData/ etudes/ STUD/2017/596824/IPOL STU%282017%29596824 EN.pdf.
- European Parliament, The UK's Potential Withdrawal from the EU and Single Market Access under EU Financial Services Legislation, December 2016, http://www .europarl.europa.eu/RegData/etudes/IDAN/2016/595334/IPOL IDA(2016)595334 EN.pdf
- Europol Operational Agreements, https://www.europol.europa.eu/partners-agree ments/operational-agreements.
- Europol Regulation, OJ L 135, 24.5.2016, p. 53–114, https://eur-lex. europa .eu/ legal -content/EN/TXT/?uri=CELEX%3A32016R0794.
- Europol website, https://www.europol.europa.eu/about-europol.
- Eurosur website, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and -visas/border-crossing/eurosur en.
- Framework Cooperation Arrangement between the European Banking Authority ("EBA") and the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the U.S. Securities and Exchange Commission, and the New York State Department of Financial Services, September 2017, https://www.eba. europa.eu/ do cume nts/ 10180/1762986/Framework+Agreement+-+EBA-US+agencies+-+September +2017.pdf.
- Frontex website, 'data protection', https://frontex.europa.eu/about-frontex/data-protection/.

- Frontex website, 'non-EU countries', https://frontex.europa.eu/partners/non-eu-countries/.
- Frontex website, 'Working Arrangements with non-EU Countries', https:// frontex.eu ropa.eu/about-frontex/key-documents/?category=working-arrangements-with-non-eu-countries.
- International Organisations, https://ec.europa.eu/anti-fraud/ sites/ antifraud /files/list signed acas en.pdf.
- Irion, K., Yakovleva, S. and Bartl, M., Trade and privacy: complicated bedfellows? How to achieve data protection-proof free trade agreements. Independent study commissioned by BEUC et al., 13 July 2016, Amsterdam, Institute for Information Law (IViR), https://www.ivir.nl/publicaties/download/1807.
- Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection, 4 July 2017, http://europa.eu/rapid/press-release STATEMENT-17-1880 en.htm.
- Joint statement on the extension of the Memorandum of Understanding on Administrative Cooperation Arrangements between DG SANCO and AQSIQ, November 2010, https: //ec.europa. eu/info/sites/info/ files/joint sta te me nt of extention of mou on adm coop arrangements between sanco aqsiq en.pdf.
- Management Board Decision No 34/2015 of 10 September 2015 adopting 'Implementing Measures for the application of Regulation (EC) No 45/2001 by Frontex', https://f rontex. europa.eu/assets/Key Documents/MB De ci sion/2015/MB Decision 34 2015 on adoption of data protection IR for administ rative purposes.pdf.
- Memorandum of Understanding on Cooperation Arrangements to access information on derivatives contracts held in European Union trade repositories between the European Security and Markets Authority (EBA) and the Australian Securities & Investments Commission (ASIC), November 2014, https: //www .esma. eu ropa. eu/sites/default/files/library/2015/11/esma asic mou.pdf.
- Memorandum of Understanding on Cooperation between Frontex and Eurojust, 18 December 2013, http://www.eurojust.europa.eu/doclibrary/Eurojust-fra mework/ agreements/Memorandum%20of%20Understanding%20between%20Eurojust%20and%20Frontex%20(2013)/Frontex-Eurojust-2013-12-18 EN.pdf.
- Mission Statement and Strategic Goals, European Commission's Directorate General for Taxation and the Customs Union, https://ec.europa.eu /taxation customs/ sites/taxation/files/resources/documents/common/about/welcome/mission statement en.pdf.
- Official Journal of the European Union, L 107, 19 April 2012, https://eur-lex. eur opa.eu/legal-content/EN/TXT/?uri=OJ:L:2012:107:TOC.
- Official Journal of the European Union, Notice of initiation of an anti-dumping proceeding concerning imports of ferro-silicon originating in Egypt and Ukraine, 2017, https://eur-lex.europa.eu/legal-content/ EN/ALL/ ?uri=u riserv: OJ.C .2017.251.01.0005.01.ENG.
- Official Journal of the European Union, Notice of initiation of an anti-dumping proceeding concerning imports of Low Carbon Ferro-Chrome originating in the People's Republic of China, Russia and Turkey, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=uriserv:OJ.C .2017.200. 01.0 017. 01.ENG& t oc=OJ:C:2017:200:FULL.
- OLAF Administrative Cooperation Arrangements (ACAs) with partner authorities in non-EU countries and territories and counterpart administrative investigative services of International Organisations, November 2017, https://ec.europa.eu/anti-fraud/sites/antifraud/files/list signed acas en.pdf.
- Owen, J., Stojanovic, A and Rutter, J., Trade after Brexit. Options for the UK's relationship with the EU. December 2017, Institute for Government, https://www.instituteforgovernment.org.uk/sites/default/files/publications/IFGJ5896-Brexit-Report-171214-final.pdf.

- Practical agreement on arrangements of cooperation between Eurojust and OLAF, September 2008,http://www.eurojust.europa.eu/doclibrary/Eurojust- framework/agreements/Practical%20Agreement%20on%20arrangements%20of%20cooperation%20between%20Eurojust%20and%20OLAF%20(2008)/Eurojust-OLAF-2008-09-24-EN.pdf.
- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0008.
- Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Arab Republic of Egypt on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Egyptian competent authorities for fighting serious crime and terrorism, December 2017, https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-809-F1-EN-MAIN PART-1.PDF.
- Regulation (EC) 1049/2001, O.J. 2001, L 145, 30 May 2001, https://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:145:0043:0048:EN:PDF.
- Regulation (EC) 45/2001, O.J. 2001, L 008, ("Processing of Personal Data by Comm unity Institutions Regulation"), 12 January 2001, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045.
- Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies, https://eur-lex.e uropa.eu/ LexU ri Serv/LexUriServ.do?uri=OJ:L:2009:302:0001:0031:EN:PDF.
- Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, esta blishing the European Food Safety Authority and laying down procedures in matters of food safety, https://eur-lex.europa.eu/legal-content/ EN/ALL/ ?uri= cel ex% 3A32002R0178.
- Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, https://publications.europa.eu/en/publication-detail/-/pu bli cation /0177e751-7cb7-404b-98d8-79a564ddc629/language-en.
- Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0765.
- Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008R0767.
- Regulation (EC) No 882/2004 of the European Parliament and of the Council of 29 April 2004 on official controls performed to ensure the verification of compliance with feed and food law, animal health and animal welfare rules, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32004R0882.
- Regulation (EC) No 1107/2009 of the European Parliament and of the Council of 21 October 2009 concerning the placing of plant protection products on the market and repealing Council Directives 79/117/EEC and 91/414/EEC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R1107.
- Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), https://eur-lex.europa.eu/legal- content/ EN/TXT/ ?uri= CELEX: 32004R2006.

- Regulation (EEC) No 2913/92, as amended by Regulation (EC) No 648/2005 of the European Parliament and of the Council (OJ L 117, 4.5.2005, p. 13), 13 April 2005, https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=uriserv:OJ.L .2005.117.01. 00 13. 01 .ENG.
- Regulation (EU) 2015/478 of the European Parliament and of the Council of 11 March 2015 on common rules for imports, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L .2015.160.01.0057.01.ENG.
- Regulation (EU) 2015/755 of the European Parliament and of the Council of 29 April 2015 on common rules for imports from certain third countries, https://eur-lex. europa.eu/legal-content/en/TXT/?uri=CELEX:32015R0755.
- Regulation (EU) 2016/1037 of the European Parliament and of the Council of 8 June 2016 on protection against subsidised imports from countries not members of the European Union, http://trade.ec. europa.eu/doclib/docs/ 2016/june/tradoc 154 703 . en. L176- 2016.pdf.
- Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, 14 September 2016, https://eur-lex.europa.eu/legal-content/ EN/TXT/ ?uri= CELEX %3A 32 01 6R 1624.
- Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/ 935/JHA, 2009/936/JHA and 2009/968/JHA, 11 May 2016, https://eur-lex .eu ropa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794.
- Regulation (EU) 2017/2321 of the European Parliament and of the Council of 12 December 2017 amending Regulation (EU) 2016/1036 on protection against dumped imports from countries not members of the European Union and Regulation (EU) 2016/1037 on protection against subsidised imports from countries not members of the European Union, 12 December 2017, https://eur-lex. europa. eu/legal - content/EN/TXT/?uri=CELEX%3A32017R2321.
- Reg ulation (EU) 216/2008, O.J. 2008, L 79/1, ("EASA Regulation"), 20 February 2008, https : // eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008R0216.
- Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32011R1077.
- Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010R1095.
- Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0604.
- Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0524.
- Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a

third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, https://eur-lex.europa.eu/legal-content/ EN/ TXT/ ?uri=celex%3A32013R0603.

- Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32012R0648.
- Regulation (EU)No. 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, L 286/1, Art.37
- Regulation (EU, Euratom) 2015/1929 of the European Parliament and of the Council of 28 October 2015 amending Regulation (EU, Euratom) No 966/2012 on the financial rules applicable to the general budget of the Union, https://eur-lex.europa.eu/legal-content/ EN/TXT/ ?uri=uriserv% 3AOJ.L .2015 .286.01.0001. 01. ENG.
- Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, https://eur-lex.europa.eu/legal-content/ EN/TXT/ ?uri= CELEX %3A32013R0883.
- Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), http://eur-lex.europa.eu/legal-content/ EN/TXT/?uri =uriserv% 3AOJ. L 2004.364.01.0001.01.ENG.
- Rules of Procedure on the processing and protection of personal data at Eurojust, Feb ruary 2005, http://www.eurojust.europa.eu/doclibrary/Eurojust- fra me work /dataprotection/Eurojust%20Data%20Protection%20Rules/Eurojust-Data-Protection-Rules-2005-02-24-EN.pdf.
- Tampere European Council conclusions, 15 and 16 October 1999, http://www. euro parl. europa.eu/summits/tam en.htm.
- Technical Implementation Procedure for Airworthiness and Environmental Certification under the Agreement between the Government of the Federative Republic of Brazil and the European Union on Civil Aviation Safety, consolidated version of March 2017, https:/ /www.easa .europa.eu /sites/ default/ files/ dfu/ TIP %20EASA-ANAC%20Rev%203%20signed.pdf.
- Technical Implementation Procedures for Airworthiness and Environmental Certification under the Agreement on Civil Aviation Safety between the Government of the Canada and the European Union, consolidated version of September 2017, https://www.easa.europa.eu/sites/default/files/dfu/EASA-TCCA% 20Technical%20 Implementation%20Procedures%20for%20airworthiness%20and%20environmental %20certification%2C%20Revision%203%20dated%2018%20Sept%202017.pdf.
- UK government, The exchange and protection of personal data – A future part nership paper, 24 August 2017, https:// assets. publishing. service.gov. uk/ government/uploads/system/uploads/attachment data/fil e/639853/ The exch an ge and protection of personal data.pdf.
- UK government, The future relationship between the United Kingdom and the Euro pean Union, 12 July 2018 (last updated 17 July 2018), https://www.gov.uk/government/publications/the-future-relationship-between-the-united-kingdom-and-the-european-union.
- UK Prime Minister's speech on the future economic partnership with the European Union, 2 March 2018; see https://www.gov.uk/government/speeches/pm-speech-on- our-future-economic-partnership-with-the-european-union.

- Working Arrangement between the European Aviation Safety Agency and the Directorate General of Civil Aviation of the Republic of Turkey on collection and exchange of information on the safety of aircraft using EU airports and airports of non-EU States that participate in the EU SAFA Programme, including airports of the Republic of Turkey, 6 July 2012, https:// www.e asa. europa .eu/ sites/ de fault/ files/ dfu/WA%20SAFA%20Turkey.pdf.
- Working Document WP 237 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 April 2016, http://ec.europa.eu/justice/article-29/documentation/opinion-re commendation/ fi les/2016/wp237 en.pdf.
- Working Document WP12 on the Transfers of personal data to third countries: Appl ying Articles 25 and 26 of the EU data protection directive, 24 July 1998, http:// ec.euro pa . eu/ justice/article-29/documentation/opinion-rec omme ndation /fil es/ 1998/wp12 en.pdf.

ANNEX I: SELECTION OF DGS AND AGENCIES

Table 5– Selected DGs and Agencies

1) DG JUST (Justice and Consumers)
2) DG HOME (Migration and Home Affairs)
3) Eurojust (European Union's Judicial Cooperation Unit)
4) Europol (European Police Office)
5) Frontex (European Border and Coast Guard Agency)
6) DG TAXUD (Taxation and Customs)
7) EASA (European Aviation Safety Agency)
8) DG MOVE (Mobility and Transport)
9) OLAF (European Anti-Fraud Office)
10) ESMA (European Securities and Markets Authority)
11) eu-LISA (European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice)
12) DG SANTE (Health and Food Safety)
13) EBA (European Banking Authority)
14) DG FISMA (Financial Stability, Financial Services, and Capital Markets Unit)
15) DG TRADE

ANNEX II: LIST OF INTERVIEWEES

Table 6- List of interviewees

Organisation	Interviewee	Interview
DG JUST	**Representative** from international data flows and protection	Interview held on 20 June 2018
European Data Protection Supervisor (EDPS)	**Fanny Coudert** (Legal Officer) **Bénédicte Raevens** (Head of Europol Supervision)	Interview held on 11 June 2018
UK Parliament	**John Woodhouse** (Researcher for House of Commons Library)	Interview held on 23 May 2018
Tech UK	**Jeremy Lilley** (Policy Manager - Data Protection and Digital Single Market)	Interview held on 14 May 2018
UK Finance	**Representative** from UK Finance	Interview held on 4 June 2018

ANNEX III: DESK RESEARCH TEMPLATE

Please find below the template designed to ensure consistent reporting on the substantive personal data processing activities of 15 selected European Commission departments and agencies which are likely to involve third country transfers (excluding data processing for purely internal management purposes). The template will be completed in respect of each selected European Commission department and agency on the basis of legislation, case law, etc., to the extent to which they are available to the research team.

1. **Brief introduction to the department/agency**

This section sets out a brief description of the department/agency, its role or main functions / tasks, and the legal basis for its establishment/operation etc.

2. **Nature of personal data**

This section sets out the types of personal data which are exchanged by the department or agency, and whether they comprise personal data which is subject to specific legal protections, such as health data or data relating to criminal activities.

3. **Purposes of processing**

This section sets out the legal and functional objectives of the data processing in which the department/agency engages.

4. **Entities involved**

This section indicates the entities involved in data processing and data exchange activities.

5. **Legal basis**

This section sets out the legal basis for personal data processing and exchanging activities in which the department/agency engages.

6. **Cooperation with third countries**

If/where relevant, this section describes the legal basis for cooperation with third countries and any relevant conditions or procedures regarding such cooperation.

7. **Actual examples**

This section includes a brief description of any actual examples of participation of third countries in the exchange of personal data.

A.1. Directorate-General for Justice and Consumers (DG JUST)

A.1.1. Brief introduction to the Department / Agency

The main task of DG JUST is to develop and carry out the European Commission's policies in the fields of Justice, Fundamental Rights and Consumers in line with the provisions laid down in Chapters 1, 3 and 4 of Title V of the TFEU. This Directorate-General is divided into 5 directorates and was created in 2010.[40]

A.1.2. Nature of personal data

DG JUST processes various personal data. The type of data varies depending on the activity. Below, a selection of the processing activities of DG JUST is presented:

Under Article 17 TFEU, DG JUST is involved in a dialogue with churches, religious associations or communities and philosophical and non-confessional organisations. For the purposes of such dialogue, DG JUST processes the following personal data: title/gender (needed for the right title)/ name, surname, profession/function/position, organisation, postal & e-mail addresses/phone number/fax number, website.[41]

DG JUST also operates a Consumer Protection Cooperation System (CPCS).[42] Within the framework of this system, the following personal data is processed: last name, first name, name of authority, address, phone number, fax number, e-mail address and language knowledge.

With regard to the processing of personal data relating to infringements or suspected infringements of consumer protection legislation, the minimum information requirements for the exchange of information between competent authorities are defined in Chapter 1 of the Annex to the CPC Implementing Rules. Some data fields are mandatory, while others are optional. The data collected may include for instance: Information on infringements or suspected infringements of consumer protection law, if relating to identified or identifiable individuals (processed in structured and free text fields under the "general information" tab, and possibly in attachments); contact information, and other personal data included in contracts, complaints and other documentary evidence) relating to company's employees, witnesses, complainants, consumers, etc. (usually processed in attached documents and, less frequently, in free text fields); data relating to infringements and suspected infringements fall under Art. 10(5) of Regulation (EC) No 45/2001.[43]

For the purposes of RAPEX (European rapid alert system for non-food dangerous products), in respect of which DG JUST is a data controller, the following data is processed:(1) Contact details of European Commission staff: (name, surname, e-mail, country, preferred language); contact details of the contact points and inspectors from the market surveillance authorities of Member States and EFTA/EEA countries: (name, surname, name of the authority, address of the authority, phone, fax, e-mail); (2) Physical persons whose personal data might be included in some cases related to the economic operators of the supply chain and test reports: Contact details of economic operators necessary for the traceability of the dangerous products (manufacturers, exporters, importers, distributors or

[40] Directorate A: Civil and commercial justice; Directorate B: Criminal justice; Directorate C: Fundamental rights and the rule of law; Directorate D: Equality and Union citizenship; Directorate E: Consumers. Cf. DG JUST Organogram, https://ec.europa.eu/info/sites/info/files/organogram_en_1.pdf, last accessed 21/05/2018.
[41] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42968, last accessed 21/05/2018.
[42] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42969, last accessed 21/05/2018.
[43] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, https://eur-lex.europa.eu/legal-content/ EN/ TXT/ ?uri =celex%3A32001R0045, last accessed 21/05/2018. The European Commission adopted a proposal on 10 January 2017 which repeals Regulation (EC) 45/2001 and brings it into line with the GDPR. The proposal is currently under discussion in the European Parliament and the Council of the European Union. The Regulation 45/2001 replacement text should be adopted in time to become applicable at the same time as the GDPR (25th May).

retailers), such as name, address, city, country, contact information, contact address, supporting documents, if any. Moreover, in exceptional cases the field "Contact information" can refer to the physical person representing the manufacturers or authorised representatives, even though Member States are asked to avoid entering any personal data and favour non-personal contact details like generic email addresses. The other fields should be filled in with the data of the company or another legal person. Furthermore, when they have been incidentally included, names of persons who have prepared the test reports may also be stored.[44]

DG JUST is also responsible for the management of the CFR-net (European contract law network), facilitating contacts and teamwork between experts. As a result, various personal data are processed, including: first name, surname, title/profession, country of origin, name of the organisation / law firm / company / federation the experts come from or represent, address, phone number, fax number, e-mail address; fields and years of expertise; area of interest in European contract law. These details are published on the restricted ECL Circa website). Moreover, first names, surnames, titles/profession, country of origin are published on the public EUROPA - SANCO website.[45]

Within the framework of the European Consumer Centres network, DG JUST processes the following personal data of third parties (consumers): language, surname, first name, e-mail address/ telephone/full postal address (street, city, country), and sometimes also fax, and gender (optional fields). Furthermore, the following data is processed in relation to contact persons of traders (all fields optional): name or other identification criteria, address of the trader, website, name of contact person, work telephone number, work fax number, work e-mail address. Moreover, the following information is processed with regard to the contact persons in the out-of-court settlement bodies: name or other identification criteria and address of the body, name of contact person, work telephone number, work fax number, work e-mail address.

Furthermore, the following personal data is collected from the staff of European Consumer Centres which are members of ECC-Net: first name, last name, login, and – optionally – e-mail.[46]

Finally, the online dispute resolution platform, also managed by DG JUST, offers a single point of entry to consumers and traders who aim to resolve contractual disputes arising from online transactions through an alternative dispute resolution (ADR) procedure, i.e. without going to court. However, judicial procedures remain available to the parties should they decide to opt for them.[47]

For purposes of public consultations, organising / managing meetings or allocating grants, DG JUST – as any other DG – also processes the following personal data: name, address, phone and fax numbers, e-mail, website of organisation and contact person.

A.1.3 Purposes of processing

The collection of personal data within the framework of DG JUST's dialogue with the churches is carried out to allow for a "open, regular and transparent" dialogue with churches, religious associations or communities and philosophical and non-confessional organisations as laid down in Article 17 TFEU.[48]

The Consumer Protection Cooperative System is an IT-tool developed to support the application of the CPC Regulation.[49] It is intended to serve as: a repository for information,

[44] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=46127, last accessed 21/05/2018.
[45] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=25257, last accessed 21/05/2018.
[46] http://ec.europa.eu/dpo-register/details.htm?id=42970.
[47] http://ec.europa.eu/dpo-register/details.htm?id=40613.
[48] http://ec.europa.eu/dpo-register/details.htm?id=42968.
[49] Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the

a structured and secure communication system to allow for the exchange of information between competent authorities of the CPC Network. Article 13(1) of the CPC Regulation establishes that information communicated by competent authorities via the CPCS may be processed only for the purposes of "ensuring compliance with the laws that protect consumers' interests", as defined in the Annex to the CPC Regulation. Access to CPCS data by the various actors has been modulated to take account of their respective roles and responsibilities, as defined in the CPC Regulation.[50]

The main purpose of the RAPEX system is a rapid exchange of information on dangerous consumer and professional products found on the European market. The exchange of information is aimed at preventing the supply of products which pose a serious risk to the health and safety environment at the workplace and to the security and where necessary withdrawing or recalling them from consumers. The main purpose of the exchange of data is to identify dangerous products and therefore information is needed on the brand, name, type, model and barcode of the product. Information is also requested about the product's traceability, which includes information on the economic operators. Member States are asked to avoid entering any unnecessary personal data in the system. Consequently, personal data can rarely be found in RAPEX notifications as the main information needed concerns products.[51]

The management of the CFR-net is aimed at facilitating contacts and teamwork between experts; and organisation of the planned workshops, conferences, events, meetings, etc.[52]

The European Consumer Centres' Network (ECC-Net) is an EU-wide network promoting consumer confidence by advising citizens on their rights as consumers and providing easy access to redress, particularly in cases where the consumer has purchased something in a country other than his/her own (cross-border). The aim of the European Consumer Centres is to provide consumers with a wide range of services, from providing information on their rights to giving advice and assistance with their complaints and the resolution of disputes. They also advise on out-of-court-settlement procedures (ADR) for consumers throughout Europe and provide consumers with easy and informed access to such procedures, when they have been unable to reach an agreement directly with the trader.[53]

The Online Dispute Resolution platform is an IT-system developed by the Commission to support the application of the ODR Regulation[54] and the ADR Directive[55]. It serves as an electronic database storing the information processed in accordance with Article 11 of the ODR Regulation, and a structured and secure communication system to allow the exchange of information, including documents, between the different actors of the ADR procedure (complainant, respondent, ADR entity staff and ODR advisors).[56]

Regulation on consumer protection cooperation), http://eur-lex.europa.eu/legal-content/ EN/TXT /?uri=uriserv%3AOJ.L .2004.364.01.0001.01.ENG, last accessed 21/05/2018, hereinafter: CPC Regulation.

[50] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-re gis ter /details.htm?id=42969, last accessed 21/05/2018.

[51] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-re gis ter/ details.htm?id=46127, last accessed 21/05/2018.

[52] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-req ister/details.htm?id=25257, last accessed 21/05/2018.

[53] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-re gi ster/details.htm?id=42970, last accessed 21/05/2018.

[54] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0524, last accessed 21/05/2018.

[55] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0011, last accessed 21/05/2018.

[56] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=40613, last accessed 21/05/2018.

The main purpose of data processing during public Consultations is to collect views of interested parties on the ideas and suggestions of the Commission on the issue outlined in the green paper.

A.1.4. Entities involved

As far as DG JUST's dialogue with the churches is concerned, data is disclosed on a need-to-know basis to staff members in BEPA. Participants of the meetings and a wider public may gain the access to data if personal data are published on internet. Transmission of personal data to the bodies in charge of a monitoring or inspection task is also possible, in accordance with Community legislation.[57]

CPCS recipients of the processing are European Commission officials, in particular for processing operations required for the maintenance of the CPCS IT-tool, and enforcement officials and case handlers working for competent authorities and SLOs in EU and EEA countries.[58]

With regard to RAPEX, the following types of users have access to personal data stored in the system: members of the Commission RAPEX Team (DG JUST, E3 and DG GROW C1) and Helpdesk RAPEX (DG SANTE, A4), European Commission staff (DG GROW other units, DGT), RAPEX Contact Points (inspectors from the market surveillance authorities of Member States and EFTA/EEA countries), inspectors from the market surveillance and customs authorities of Member States and EFTA/EEA countries as well as the Chinese competent authority (AQSIQ) for notifications under RAPEX China.[59]

With regard to the CFR-net, the following entities have the access to the data: ECL CIRCA website: CFR-net experts; National (Member State) experts, Commission officials, identified members of the European Parliament; ECL researchers.[60]

As for the ECC net, the staff members of European Consumer Centres which are members of ECC-Net and European Commission staff can access the data.[61]

As for consultations, access to the data is gained by the unit responsible for the specific consultation within DG JUST. Publication on the internet follows only with the contributor's consent if appropriate.

A.1.5. Legal basis

The Treaty of Lisbon explicitly introduces the idea of a dialogue between European institutions and churches, religious associations or communities as well as philosophical and non-confessional organisations (Article 17 TFEU).[62]

As for the CPCS, the legal basis can be found in Regulation (EC) N° 2006/2004 of the European Parliament and the of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Regulation on consumer protection cooperation, the CPC Regulation).[63]

[57] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42968, last accessed 21/05/2018.
[58] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42969, last accessed 21/05/2018.
[59] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=46127, last accessed 21/05/2018.
[60] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=25257, last accessed 21/05/2018.
[61] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42970, last accessed 21/05/2018.
[62] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42968, last accessed 21/05/2018.
[63] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42969, last accessed 21/05/2018.

The processing of personal data within RAPEX is based on the General Product Safety Directive 2001/95/EC (OJ L 11, 15.1.2002, p. 4–17)[64], Article 12 and Annex II, Regulation 765/2008 of 9 July 2008[65] setting out requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L, 13.08.2009, p. 30)[66], Decision 2010/15/EU of 16 December 2009 laying down the RAPEX guidelines (OJ L, 26.01.2010, p.1)[67].[68]

As for the CFR-net, the legal basis for the activities, including their management and the related processing, is the 2004 Communication from the Commission to the European Parliament and the Council "European contract law and the revision of the acquis: the way forward".[69] This Communication is the follow-up to the 2003 Action Plan on "A more coherent European contract law"[70] and of the 2001 Communication on "European contract law"[71].

The initiative of European contract law has at its origin the 1999 Tampere European Council conclusions which called for a study of the need to approximate civil law for a better functioning of the internal market[72].[73]

The legal basis for the ECC-net is the Action 10 of Decision no 1926/2006/EC of the European Parliament and of the Council of 18 December 2006 establishing a programme of Community action in the field of consumer policy for the years 2007-2013 (OJ L404 of 30/12/2006)[74].[75]

The legal bases for the Online Dispute resolution platform include: Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes[76] and amending Regulation (EC) 2006/2004[77] and Directive 2009/22/EC[78], Commission Implementing Regulation (EU) 2015/1051[79] on the

[64] Can be accessed here: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32001L0095, last accessed 21/05/2018.
[65] To be accessed here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0765, last accessed 21/05/2018.
[66] To be accessed here: Council Regulation (EEC) No 339/93 of 8 February 1993 on checks for conformity with the rules on product safety in the case of products imported from third countries, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31993R0339, last accessed 21/05/2018.
[67] 2010/15/: Commission Decision of 16 December 2009 laying down guidelines for the management of the Community Rapid Information System RAPEX established under Article 12 and of the notification procedure established under Article 11 of Directive 2001/95/EC (the General Product Safety Directive) (notified under document C(2009) 9843), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0015, last accessed 21/05/2018.
[68] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=46127, last accessed 21/05/2018.
[69] To be accessed here: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52004DC0651, last ac cessed 21/05/2018.
[70] To be accessed here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52003DC0068, last ac cessed 21/05/2018.
[71] To be accessed here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52001DC0398, last accessed 21/05/2018.
[72] To be accessed here: http://www.europarl.europa.eu/summits/tam_en.htm, last accessed 21/05/2018.
[73] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=25257, last accessed 21/05/2018.
[74] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32006D1926, last accessed 21/05/2018.
[75]As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42970, last accessed 21/05/2018.
[76] To be accessed here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0524, last accessed 21/05/2018.
[77] Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation), https://eur-lex.europa.eu/legal-content/ EN/ TXT/?uri=CELEX:32004R2006, last accessed 21/05/2018.
[78] Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests, http://eur-lex.europa.eu/legal- content/ EN/ TXT/ ?uri= ur iserv: OJ.L .2009.110.01.0030.01.ENG, last accessed 21/05/2018.
[79] Commission Implementing Regulation (EU) 2015/1051 of 1 July 2015 on the modalities for the exercise of the functions of the online dispute resolution platform, on the modalities of the electronic complaint form and on the modalities of the cooperation between contact points provided for in Regulation (EU) No 524/2013 of the European

modalities for the exercise of the functions of the online dispute resolution platform, on the modalities of the electronic complaint form and on the modalities of the cooperation between the contact points provided for in Regulation (EU) No 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes, and Directive of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) 2006/2004 and Directive 2009/22/EC. The process to include the ADR/ODR legislation in the EEA acquis is currently ongoing. Once concluded, the platform will function EEA-wide.[80]

The legal basis for the consultations is the Article 211 TFEU.

A.1.6. Cooperation with third countries

Data may be transferred to third countries within the framework of the Consumer Protection Cooperative System and RAPEX.

As for the processing within the framework of the Consumer Protection Cooperative System, Article 14(2) of the CPC Regulation foresees that information exchanged under that Regulation may be communicated to competent authorities in third countries under bilateral assistance agreements with those countries, provided the consent of the authority that originally communicated the information has been obtained and in accordance with EU legislation on personal data protection. Article 18 of the CPC Regulation also foresees the possibility of mutual assistance arrangements being signed between the EU and third countries.[81]

However, no transfer of data to third countries is envisaged at this stage. If and when such an agreement was to be negotiated and signed, data protection authorities would be informed by means of a complementary notification.[82]

As for RAPEX, Products of Chinese origin represent a considerable share of dangerous products notified in this system. This has triggered cooperation between the European Commission and China on product safety and food safety, which has taken the form of a Memorandum of Understanding signed in 2006 between the Health and Consumer Protection Directorate-General of the European Commission (the part concerning product safety has since been transferred to DG JUST) and the General Administration of Quality Supervision, Inspection and Quarantine of China (AQSIQ), which was later extended in 2010.[83] The Memorandum of Understanding imposes confidentiality requirements regarding all data transmitted.[84]

Finally, in the absence of any formal arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations (its purpose(s), the criteria for assessing an adequate level of protection in or within the recipient third country or international organisation, the possible derogations and exceptions, etc.) which are not subject to the GDPR.[85]

Parliament and of the Council on online dispute resolution for consumer disputes, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2015.171.01.0001.01.ENG, last accessed 21/05/2018.

[80] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=40613, last accessed 21/05/2018.

[81] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42969, last accessed 21/05/2018.

[82] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42969, last accessed 21/05/2018.

[83] Joint statement on the extension of the Memorandum of Understanding on Administrative Cooperation Arrangements between DG SANCO and AQSIQ, accessible at https://ec.europa.eu/info/sites/info/files/joint_statement_of_extention_of_mou_on_adm_coop_arrangements_between_sanco_aqsiq_en.pdf, last accessed 21/05/2018.

[84] http://ec.europa.eu/dpo-register/details.htm?id=46127.

[85] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, is repealed with effect from 25 May 2018.

A.1.7. Actual examples

According to the provisions of the abovementioned Memorandum of Understanding with regard to RAPEX, AQSIQ receives an extract of the notifications which meet the following criteria: the country of origin of the product is "China", the notification is not covered by a confidentiality request from the notifying Member State, and the product risks must concern the health and/or safety of consumers (professional products are excluded). Only a subset of the RAPEX notifications is sent to AQSIQ. The extract of the RAPEX notification aims exclusively at enabling the identification of the products so that AQSIQ can make sure that such dangerous products will no longer be supplied to the EU market.

While all the information pertaining to the product identification (brand, name, barcode, type/model) is sent, when it comes to traceability information, only data on the manufacturer and exporter in China are exported. Without this information on the responsible manufacturer and exporter, it would be impossible to achieve a high level of consumer protection.

Besides restricting the information sent to the strict minimum necessary (for instance, information on the author and validator of the notification are not sent), adequate safeguards have been put in place to ensure effective personal data protection. As indicated before in general under point 7, Member States are asked to avoid entering any unnecessary personal data in the system. A systematic control mechanism has been established through which the Commission's RAPEX team deletes personal and/or trade sensitive data, if any, before transmission. This includes, in respect of each notification, the manual deletion of personal data from attachments and fields that are transferred to AQSIQ. The only potential personal data that can be sent to AQSIQ are the ones concerning manufacturers and/or exporters in China (i.e. name, address, e-mail address, website, phone number of companies).

Moreover, Member States can request, subject to due justification, confidential handling of a notification or part of it submitted in GRAS RAPEX. The notifications marked as confidential in GRAS-RAPEX are not sent.

From the technical point of view, appropriate measures are in place to ensure data protection and data security: the technical solution for this cooperation is a separated database scheme, with the required subset of information, linked to an interface accessible only to a limited number of officials of AQSIQ (4 users). Access to this interface, using ECAS authentication, is granted exclusively upon approval by the Commission's RAPEX team. AQSIQ has no access to GRAS-RAPEX but only to a Web application using a secure https Internet protocol in which data are displayed as "read only".[86]

Transfer of data to countries outside the EU – albeit within the EEA – also takes place within the ECC-net - Norway and Iceland (which are EEA/EFTA countries and members of the ECC-Net). Transfer of personal data between ECCs in the European Union and ECCs in Norway or Iceland is therefore considered as an Article 8 transfer[87], following the incorporation of Directive 95/46/CE into the Agreement on the European Economic Area.[88]

[86] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=46127, last accessed 21/05/2018.

[87] Article 8 of Regulation 45/2001 stipulates rules regarding transfer to recipients subject to the national law adopted for the implementation of the data protection directive. This includes public authorities in the Member States as well as the private sector and natural persons. Moreover, recipients residing or - in the case of legal persons - established in EEA/EFTA-countries are included. As mentioned above, the European Commission adopted a proposal on 10 January 2017 which repeals Regulation (EC) 45/2001 and brings it into line with the GDPR. The proposal is currently under discussion in the European Parliament and the Council of the European Union. The Regulation 45/2001 replacement text should be adopted in time to become applicable at the same time as the GDPR (25th May).

[88] Decision N° 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement, accessible at https://eur-lex.europa.eu/legal-content/ EN/ TXT/ ?uri= celex % 3A 220 00D 1123%2808%29, last accessed 21/05/2018.

A.2. Directorate-General Migration and Home Affairs (DG HOME)

A.2.1. Brief introduction to the Department / Agency

The tasks of the current DG HOME were originally exercised by DG Justice, freedom and security. DG Migration and Home Affairs was established on 01/07/2010 as DG Home Affairs and acquired its current full name (DG Migration and Home Affairs) on 01/01/2015.

This Directorate-General is responsible for EU policies in matters regarding security, migration, border security and anti-terrorism measures. DG HOME has five functional directorates.[89]

The main tasks for which this DG is responsible have been outlined in the TFEU, Title V, Chapters 1, 2 and 5, and include:[90]

a) Immigration and asylum policy:
   - visa policy, Schengen area;
   - migration and borders (biometrics, repatriation);
   - developing a balanced and comprehensive EU migration policy;
   - creating an EU-wide set of rules for legal migration, while taking into account the interconnection between migration and integration;
   - addressing irregular migration and trafficking in human beings;
   - working to set up a Common European Asylum System.

b) Ensuring EU security:
   - fighting terrorism and organised crime;
   - promoting police cooperation, including international cooperation;
   - preparing to swiftly respond to emerging crises (stricter rules against illicit trafficking of firearms and on trafficking in human beings, combating child sexual abuse, sexual exploitation and child pornography.);
   - fighting against terrorism and the Internal Security Strategy, strictly linked to the broader European Security Strategy.

c) External dimension and funding of the EU home affairs policy:
   - promoting dialogue and cooperation with non-EU countries;
   - contributing to the strengthening of the Union's position as a reliable, active and pragmatic global player.

d) Fostering European citizenship and European civic awareness.

A.2.2. Nature of personal data

DG HOME processes various personal data while carrying out its numerous activities. Below, a selection of the processing activities of DG HOME which are most relevant to this study has been presented.

[89] Directorate A: Strategy and General Affairs; Directorate B: Migration, Mobility and Innovation; Directorate C: Migration and Protection; Directorate D: Security; Directorate E: Migration and Security Funds, Financial Resources and Monitoring.
As outline on the DG Home website – the organigram section: https://ec.europa.eu/home-affairs/who-we-are/dg-home-affairs-chart_en.
[90] According to the DG HOME – About us section: https://ec.europa.eu/home-affairs/who-we-are/about-us_en.

DG Home collects, records, stores, publishes, modifies and deletes the contact details of experts and stakeholders from governmental, non-governmental and supranational organisations in Member States and beyond in the area of anti-trafficking in human beings on the anti-trafficking in human beings website. These contact details include names, positions, organisations, nationalities, postal addresses, email addresses, telephone numbers and fax numbers.[91] No data requiring specific legal protection is analysed during these activities.

DG HOME also manages the European Refugee Fund Projects' Database. This is a web-based database on projects implemented under the European Refugee Fund since the year 2000, containing information on the projects themselves (type, short description, funding) as well as contact information on the implementing organisation. Data is processed by the Commission and in the Member States. Data processed this way include names, first names, e-mail addresses, and postal addresses within the organisation (not visible to others but the administrators of the system).[92]

DG HOME is also responsible for the Critical Infrastructure Warning Information Network (CIWIN) initiative which is a part of the European Programme for Critical Infrastructure Protection (EPCIP). CIWIN offers recognised members of the EU's critical infrastructure protection community the opportunity to exchange and discuss critical infrastructure protection-related information, studies and/or good practices. Within the framework of this initiative, the following data are processed: first names and surnames of persons, e-mail addresses, telephone numbers, categories of user, CIP related field names of organization, functions, addresses, postal codes, cities, and countries. A username and password are set up upon the first registration.[93]

DG HOME is also responsible for collection, recording, storage, consultation, use, transmission, modification, blocking, erasure of personal data required for positive identification of persons wishing to submit contributions to the European Web Site on Integration related processes and/or to accede to specific sections thereof. Hence, the following personal data are collected: name and surname, e-mail address, organisation name, phone number, fax, postal address, country of residence, type of contribution and contribution history.[94]

DG HOME also carries out consultations of stakeholders and/or the public on policy and legislative initiatives. During this process, only data necessary for the participation in the "consultation", such as: title, first name, surname, organisation, country, city, phone, fax, e-mail address, are processed. Personal data may be published following the "consultation" but an opt-out is provided for in the Privacy Statement.[95]

A.2.3. Purposes of processing

The website on anti-trafficking in human beings processes personal data in order to publish certain contact details, with the consent of those involved, on various sections of the website.
Where the contact details are published within the restricted access area of the website, the intention is to enable practitioners in the field of anti-trafficking of human beings to contact one another and exchange information about best practice. Where the contact details are published (with the data subject's consent) on the public area of the website, the intention

[91] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=38840, last accessed 16/05/2018.
[92] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=43068, last accessed 16/05/2018.
[93] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=43067, last accessed 16/05/2018.
[94] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=43069, last accessed 16/05/2018.
[95] As explained in the official register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42609, last accessed 16/05/2018.

is to give interested persons points of contact from which to obtain further information about human trafficking and anti-trafficking efforts.[96]

Data is processed on the European Refugee Fund Projects' Database in order to provide information on the projects themselves (type, short description, funding) and contact information on the implementing organisation. This website is also a tool to promote European co-operation of organisations (governmental and non-governmental) active in field of asylum, in order to share information and best practices.[97]

The purpose of the processing of personal data for the CIWIN is providing secure access and information exchange, management of databases, including management of: communications to users, reports, distribution of reports, information sharing within interest groups, etc.[98]

The European Web Site on Integration collects personal data with the following purposes: (1) to identify data subjects uniquely, as authors of their contributions if they decide to become registered users of the Portal (this allows them to contribute to the content); (2) to provide data subjects with newsletters that will be sent to their unique e-mail addresses; (3) to allow other users to contact consenting data subjects via a web-mail form embedded in the Web Site (the email-addresses are not visible in this case).[99]

The data processing by public consultations/surveys/questionnaires/quizzes by DG HOME is aimed at receiving the views of those concerned by the topics of the "consultations" and to potentially publish them on the Internet.[100]

A.2.4. Entities involved

Regarding the anti-trafficking website, specific EC officials in DG Home Affairs will have direct access to relevant data; in cases in which contractors are involved, the involvement is governed by the data protection clause in the contract between controllers and contractors.[101]

Regarding the European Refugee Fund Projects' Database, recipients include: administrators within the unit of DG Home which is responsible for the database/B2, contact points within the authorities which are responsible for it at Member State level/implementing organisations, the contractor building and maintaining the system, the general public, ERF project promoters (e.g. contact points within the Commission, the Member States' Responsible authorities, local and/or regional administrations, NGOs, International Organisations).[102]

Regarding CIWIN, recipients include officials and other staff of the Joint Research Centre (JRC) and DG HOME, the registered users and the CIWIN system administrators.[103]

Regarding the European Website on Integration-related processes, the entities involved include the Commission officials in Units Shared Resource Directorate (SRD) 3 and Home B1 and B4 (with a direct access to relevant data processing). These persons will not in

[96] Register of the European Data Protection Supervisor http://ec.europa.eu/dpo-register/details.htm?id=38840, last accessed 16/05/2018
[97] Register of the European Data Protection Supervisor http://ec.europa.eu/dpo-register/details.htm?id=43068, last accessed 16/05/2018.
[98] Register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=43067.
[99] Register of the European Data Protection Supervisor http://ec.europa.eu/dpo-register/details.htm?id=43069, last accessed 16/05/2018.
[100] Register of the European Data Protection Supervisor http://ec.europa.eu/dpo-register/details.htm?id=42609, last accessed 16/05/2018.
[101] Register of the European Data Protection Supervisor http://ec.europa.eu/dpo-register/details.htm?id=38840, last accessed 16/05/2018.
[102] Register of the European Data Protection Supervisor http://ec.europa.eu/dpo-register/details.htm?id=43068, last accessed 16/05/2018.
[103] Register of the European Data Protection Supervisor http://ec.europa.eu/dpo-register/details.htm?id=43067, last accessed 16/05/2018.

normal circumstance process such data but they are able if required to introduce corrections – e.g. if the rapid correction of inaccurate data becomes necessary.[104]

As regards the consultations conducted by various DGs, recipients include participants to the "consultation" and a wider public insofar as some of personal data could be published on Internet, without prejudice to a possible transmission to the bodies in charge of a monitoring or inspection task in accordance with Community legislation. When contractors are involved, this is governed by the data protection clause in the contract between controllers (in this case DG HOME) and contractors.[105]

A.2.5. Legal basis

As for the anti-trafficking in human beings website, the legal basis for processing operations on personal data is Article 67 of the TFEU. Personal data is processed and published lawfully in the legitimate exercise of official authority vested in DG Home and in the public interest, namely the establishment of an anti-THB website which aims to provide policy makers and practitioners with a tool for the exchange of information and good practice on anti-trafficking efforts across Europe.[106]

The legal basis for European Refugee Fund Project Database is the Council Decision creating the European Refugee Fund (European Refugee Fund I: 2000/596/EC[107], European Refugee Fund II 2004/904/EC[108]).[109]

The legal basis for CIWIN is the Commission Communication 789 of 12/12/2006[110] on a European Programme for Critical Infrastructure Protection. Registration and participation of data subjects are provided on a purely voluntary basis. The persons concerned have unambiguously given their consents (Art. 5 (d) of Regulation (CE) 45/2001[111]). This processing is lawful under article 5(a) of Regulation (EC) 45/2001.[112]

The legal basis justifying personal data processing within the European Website on Integration is Commission decision C(2006)3632[113] adopting the "annual work programme for grants and contracts in the field of Justice, Freedom and Security for 2006", serving as financing decision for the "Integration of third-country nationals 2006", adopted on 07/08/2006.[114]

---

[104] Register of the European Data Protection Supervisor http://ec.europa.eu/dpo-register/details.htm?id=43069 , last accessed 16/05/2018.
[105] Register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=42609, last accessed 26/05/2018.
[106] Register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=38840
[19] 2000/596/EC: Council Decision of 28 September 2000 establishing a European Refugee Fund, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0596 , last accessed 21/05/2018.
[108] 2004/904/EC: Council Decision of 2 December 2004 establishing the European Refugee Fund for the period 2005 to 2010, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004D09044 , last accessed 21/05/2018.
[109] Register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=43068, last accessed 26/05/2018.
[110] COM (2006) 789: Communication from the Commission to the Council and the European Parliament Investment research and financial analysts (SEC (2006)1655), http://eur-lex.europa.eu/procedure/EN/195097, last accessed 21/05/2018.
[111] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045, last accessed 21/05/2018. The European Commission adopted a proposal on 10 January 2017 which repeals Regulation (EC) 45/2001 and brings it into line with the GDPR. The proposal is currently under discussion in the European Parliament and the Council of the European Union. The Regulation 45/2001 replacement text should be adopted in time to become applicable at the same time as the GDPR (25th May).
[112] Register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=43067, last accessed 26/05/2018.
[113] Commission Decision of 16 August 2006 C (2006) 3602 concerning the security of information systems used by the European Commission, http://ec.europa.eu/internal_market/imi-net/docs/decision_3602_2006_en.pdf, last accessed 21/05/2018.
[114] Register of the European Data Protection Supervisor, http://ec.europa.eu/dpo-register/details.htm?id=43069, last accessed 26/05/2018.

The processing operations on personal data linked to the launching of a "consultation" are necessary for the management and functioning of the Commission, as mandated by the treaties, and more specifically Article 5 of TEU, Article 13 TEU and Articles 244-250 TFEU, and in accordance with Article 1 and Article 11 of TEU.[115]

A.2.6. Cooperation with third countries

An increasing number of third countries are requesting passenger name record (PNR) data from air carriers operating flights from the territory of the European Union. The EU has so far concluded international PNR agreements with the United States, Canada and Australia, allowing air carriers to transfer PNR data to these third countries. Such cooperation can bring major security gains, in areas like foreign terrorist fighters travelling to conflict zones for terrorist training, drugs trafficking or travelling sex offenders.

In 2010 the Commission issued a Communication "On the global approach to transfers of Passenger Name Record data to third countries" to set out the elements of the EU's external PNR policy. This Communication established a set of general criteria that must be fulfilled by future bilateral PNR agreements, including, in particular, a number of data protection principles and safeguards.[116]

When negotiating the PNR agreements with third countries, DG HOME is the main European Commission negotiator.[117]

Furthermore, the EU's legal migration policy, for which DG HOME is responsible, includes EU's Mobility Partnerships, as explained in the Commission Communication: "The Global Approach to Migration and Mobility" (COM/2011/743 final). These are the most elaborate bilateral cooperation frameworks in the field of migration. They offer a political framework for comprehensive, enhanced and tailor-made dialogue and cooperation with partner countries, including a set of targets and commitments as well as a package of specific support measures offered by the EU and interested Member States. They include the negotiation of visa facilitation and readmission agreements.[118] Some of these agreements, negotiated by DG HOME, also include provisions on the exchange of personal data.

Finally, in the absence of any formal arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations which are not subject to GDPR.[119]

A.2.7. Actual examples

The general criteria mentioned above formed the basis of the renegotiations of the PNR Agreements with the US, Australia and Canada, leading to the conclusion of new PNR Agreements with the two first mentioned countries. The envisaged new EU-Canada Agreement has not entered into force because in November 2014 the Parliament voted to seek the opinion of the CJEU as to whether the draft Agreement is compatible with the Treaties and the Charter of Fundamental Rights. Once the CJEU issues its opinion on the envisaged PNR Agreement with Canada, the Commission intends to review the current approach towards transfers of PNR data to third countries, to address the increasing number of third country requests in a clear and coherent way, including by considering a

[115] http://ec.europa.eu/dpo-register/details.htm?id=42609
[116] https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en.
[117] For example, see Management Plan 2018 for the DG Migration and Home Affairs, https://ec.europa.eu/info/sites/info/files/management-plan-home-2018_en.pdf, last accessed 21/05/2018, p.22, 23.
[118] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, A EUROPEAN AGENDA ON MIGRATION, 13/05/2015, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/background-information/docs/communication_on_the_european_agenda_on_migration_en.pdf, last accessed 31/05/2018, p.16.
[119] General Data Protection Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR"); effective as of 25 May 2018.

model agreement setting out the requirements third countries have to meet to be able to receive PNR data from the EU.[120]

Examples of clauses relating to PNR data in the PNR agreements include for instance Article 10(3) in the EU PNR Agreement with Australia[121] and Article 5 and 6 in the EU-USA PNR Agreement.[122]

As mentioned above, some of the agreements negotiated within the migration policy framework, the mobility partnerships such as the visa facilitation agreements also include provisions on processing personal data. For instance, the agreement with Bosnia and Herzegovina in its Article 4 sets out data needs to be provided in the written request for a VISA.[123] For example, for the invited person, the required data includes name and surname, date of birth, sex, citizenship, number of the identity document, time and purpose of the journey, number of entries and where relevant the name of the spouse and children accompanying the invited person (Article 4(2)(a)). An equivalent provision is also included in Article 4 of the VISA facilitation agreement with Russia.[124]

[120] https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en.

[121] Article 10.3: The Australian Information Commissioner will, in particular, hear claims lodged by an individual regardless of his or her nationality or country of residence, concerning the protection of his or her rights and freedoms with regard to the processing of personal data. The individual concerned will be informed of the outcome of the claim. The Australian Information Commissioner will further assist individuals concerned in the exercise of their rights under this Agreement, in particular, rights of access, rectification and redress. Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0714%2801%29 , last accessed 18/05/2018.

[122] Article 5(1): DHS shall ensure that appropriate technical measures and organisational arrangements are implemented to protect personal data and personal information contained in PNR against accidental, unlawful or unauthorised destruction, loss, disclosure, alteration, access, processing or use., Article 6(1): To the extent that PNR of a passenger as collected includes sensitive data (i.e. personal data and information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning the health or sex life of the individual), DHS shall employ automated systems to filter and mask out sensitive data from PNR. In addition, DHS shall not further process or use such data, except in accordance with paragraphs 3 and 4, Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0811%2801%29 , last accessed 18/05/2018.

[123] Agreement between the European Community and Bosnia and Herzegovina on the facilitation of the issuance of visas – Declarations, OJ L 334, 19.12.2007, p. 97–107 (BG, ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV), https://eur-lex.europa.eu/legal-content /EN/ ALL/ ?uri =CE LEX :22007A1219(06)&qid=1395933932709 ,last accessed 31/05/2018.

[124] Article 4(2)(a) requires the following data in a VISA application: for the invited person — name and surname, date of birth, sex, citizenship, number of the identity document, time and purpose of the journey, number of entries and name of minor children accompanying the invited person; Agreement between the European Community and the Russian Federation on the facilitation of the issuance of visas to the citizens of the European Union and the Russian Federation, OJ L 129, 17.5.2007, p. 27–34 (BG, ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV. Special edition in Croatian: Chapter 11 Volume 033 P. 189 – 196, https://eur-lex.europa.eu/legal- content/ EN/ALL/?uri=CELEX:22007A0517(01), last accessed 31/05/2018.

A.3. Eurojust

A.3.1. Brief introduction to the Department / Agency

Eurojust was established by Decision 2002/187/JHA[125] as a body of the European Union with legal personality to stimulate and to improve coordination and cooperation between competent judicial authorities of the Member States.

In the context of investigations and prosecutions, concerning two or more Member States, of certain criminal behaviour (serious crime), Eurojust has the following objectives:[126]

- Stimulate and improve the coordination, between competent authorities of Member States;
- Improve cooperation between the competent authorities of the Member States; and
- To otherwise support the competent authorities of the Member States, in order to render their investigations and prosecutions more effective.

At the request of a Member State's competent authority, Eurojust may also assist investigations and prosecutions concerning only that Member State and a non-Member State where an agreement establishing cooperation has been concluded with that State or where in a specific case there is an essential interest in providing it.[127]

Articles 13-21 set out the provisions concerning the exchange of information with Member States and between national members, as well as the provisions and restrictions related to the processing of personal data.

The latest chapter in the development of Eurojust is contained in the Lisbon Treaty, namely in Chapter 4, Articles 85 and 86. Article 85 mentions Eurojust and defines its mission, "*to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States […]*". Article 86 states that, "*in order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust*".

A.3.2. Nature of personal data

Article 15 limits the processing of personal data by Eurojust to the following personal data of persons who, under national legislation of Member States concerned are suspected of having committed or participated in a criminal offence, in respect of which Eurojust has competence, or who have been convicted of such an offence:

a) surname, maiden name, given names and any alias or assumed names;
b) date and place of birth;
c) nationality;
d) sex;
e) place of residence, profession and whereabouts of the person concerned;
f) social security numbers, driving licences, identification documents and passport data;
g) information concerning legal persons if it includes information relating to identified or identifiable individuals who are the subject of a judicial investigation or prosecution;
h) bank accounts and accounts with other financial institutions;

[125] Council Decision 2002/187/JHA of 28 February 2002 has since been amended by Council Decision 2003/659/JHA of 18 June 2003 and Council Decision 2009/426/JHA of 16 December 2008.
[126] Article 3(1).
[127] Article 3(2).

i) description and nature of the alleged offences, the date on which they were committed, the criminal category of the offences and the progress of the investigations;
j) the facts pointing to an international extension of the case;
k) details relating to alleged membership of a criminal organisation;
l) […][128]
m) vehicle registration data;
n) DNA profiles established from the non-coding part of DNA, photographs and fingerprints.

In addition, Eurojust may only process the following personal data on persons who are regarded as witnesses or victims in a criminal investigation or prosecutions:

a) surname, maiden name, given names and any alias or assumed names;
b) date and place of birth;
c) nationality;
d) sex;
e) place of residence, profession and whereabouts of the person concerned;
f) the description and nature of the offences involving them, the date on which they were committed, the criminal category of the offences and the progress of the investigations.[129]

Data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life may only be processed by Eurojust when such data are necessary for the national investigations concerned, as well as for coordination within Eurojust.

A.3.3. Purposes of processing

Insofar as is necessary to achieve its objectives, Eurojust may, within the framework of its competence and in order to carry out its tasks, process personal data, by automatic means or in structured manual files. Eurojust may carry out its tasks through its national members or acting as a College.[130] More specifically, Eurojust may ask the competent authorities of Member States to:

a) undertake an investigation or prosecution of specific acts;
b) accept that one of them may be in a better position to undertake an investigation or to prosecute specific acts;
c) coordinate between the competent authorities of the Member States concerned;
d) set up a joint investigation team in keeping with the relevant cooperation instruments;
e) provide it with any information that is necessary for it to carry out its tasks;
f) take special investigative measures;[131]
g) take any other measure justified by the investigation or prosecution[132].[133]

In addition, Eurojust shall:

[128] Article 15 (l) provided that Eurojust could process telephone numbers, e-mail addresses and data referred to in Article 2(2)(a) of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. However, this directive has been declared void ab initio by the Court of Justice.
[129] Article 15(3) allows for Eurojust to process, for a limited period of time, other personal data relating to the circumstances of an offence where they are of immediate relevance to an ongoing investigation, provided the DPO is immediately informed.
[130] Article 5; Article 10 states that the College shall consist of all national members.
[131] Only when acting through its national members.
[132] Only when acting through its national members.
[133] Articles 6(1)(a) and 7(1)(a).

- ensure that the competent authorities of the Member States concerned inform each other on investigations and prosecutions of which it has been informed;
- assist the competent authorities of the Member States, at their request, in ensuring the best possible coordination of investigations and prosecutions;
- give assistance in order to improve cooperation between the competent national authorities;
- cooperate and consult with the European Judicial Network, including making use of and contributing to the improvement of its documentary database; and
- in the cases referred to in Article 3(2) and (3) and with the agreement of the College, assist investigations and prosecutions concerning the competent authorities of only one Member State.[134] [135]

A.3.4. Entities involved

Eurojust itself is composed of members of national prosecutors' offices, judges, and senior police officers. It either executes its tasks "through one or more national members" or as a College (i.e. acting as all national members).

Article 26 provides that Eurojust shall establish and maintain cooperative relations with at least:

- Europol;
- OLAF;
- Frontex;
- The Council (in particular its Joint Situation Centre); and
- The Judicial Training Network.

It may conclude agreements or working arrangements with these entities.

In addition, Article 26a provides that it may establish and maintain cooperative relations with:

- Third States;[136]
- International organisations and their subordinate bodies governed by public law;
- Other bodies governed by public law which are based on an agreement between two or more States; and
- Interpol.

Thus, Eurojust has cooperation agreements and memoranda of understanding with several entities.[137]

As an example, Eurojust has signed a practical agreement on arrangements of cooperation with OLAF.[138] Point 6(1) of the agreement provides that when Eurojust and OLAF collaborate on a specific case, they will exchange any necessary information, including

[134] Only when acting through its national members.
[135] Articles 6 and 7.
[136] For third countries with an Agreement with Eurojust, the Agreement identifies the competent authority of the country concerned.
[137] The agreements with EU partners, third States and other organisations can be found at http://www.eurojust.europa.eu/about/legal-framework/Pages/eurojust-legal-framework.aspx
[138] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/_Practical%20Agreement%_20on%20_arrang_ements%20of%20cooperation%20between%20Eurojust%20and%20OLAF%20(2008)/Eurojust-OLAF-2008-09-24-EN.pdf

personal data, in order to achieve the purpose of the agreement itself. The purpose of the agreement is to enhance the fight against fraud, corruption or any other criminal offence or illegal activities affecting the European Communities' financial interests and to define to this end the modalities for close cooperation between the parties.

Similarly, Eurojust has a memorandum of understanding with Frontex.[139] This provides for the exchange of general information, the exchange of strategic information, and the exchange of best practices. However, Article 4(4) of the memorandum states that the exchange of information or experience provided for in this Memorandum of Understanding shall not include the transmission of operational information, including data relating to an identified or identifiable natural person.

A.3.5. Legal basis

The legal basis is Articles 14, 15 and 16 of the Eurojust Decision and Rules of Procedure on the Processing and Protection of Personal Data at Eurojust,[140] and Additional rules defining some specific aspects of the application of the rules on the processing and protection of personal data at Eurojust (concerning non-case-related data).[141]

Article 14 of the Eurojust Decision establishes that Eurojust can process personal data, within the framework of its competences, insofar as it is necessary to carry out its tasks. Article 15 sets out the limits on the categories of personal data that can be processed in relation to suspects and witnesses. Article 16 sets out in detail the establishment of, functioning of and access to the case management system.

Article 30 of the Rules of Procedure on the Processing of Personal Data at Eurojust, provides for the following bases for processing non-case-related personal data:

a) processing is necessary for compliance with a legal obligation to which the controller is subject; or
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
c) the data subject has unambiguously given his or her consent;
d) processing is necessary in order to protect the vital interests of the data subject;
e) processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 4 of the present rules.

A.3.6. Cooperation with third countries

Article 26a provides the legal basis for Eurojust to enter into agreements with third countries, concerning the exchange of information, including personal data.

Such agreements may be concluded after consultation by Eurojust with the Joint Supervisory Body concerning the provisions on data protection, and after the approval of the Council, acting by qualified majority. Eurojust shall inform the Council of any plans it has for entering into any such negotiations and the Council may draw any conclusions it deems appropriate.

---

[139] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework /agreements/ Memorandum% 20of% 20 Un der standing%20between%20Eurojust%20and%20Frontex%20(2013)/Frontex-Euroju st-2013-12-18_EN.pdf

[140] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/dataprotection/Eurojust%20Data%20Protection%20Rules/Eurojust-Data-Protection-Rules-2005-02-24-EN.pdf

[141] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ dataprotection/ Additional%20rules% 20d efining %20specific %20a spects%20 of%20the%20ap plication%20of%20Rules% 20on%20Processing% 20and%20Protection%20of%20Personal%20Data/additional_dp_rules.pdf

Article 27 provides that before Eurojust exchanges any information with this third country, the national member of the Member State which submitted the information shall give his consent to the transfer of that information. In appropriate cases, he will consult the competent authorities of the member states.

Article 27b provides that Eurojust may, with the agreement of the Member States concerned, coordinate the execution of requests for judicial cooperation issued by a third State where these requests are part of the same investigation and require execution in at least two Member States. Such requests may also be transmitted to Eurojust by a competent national authority.

A.3.7. Actual examples

Eurojust currently has agreements with several third countries (Ukraine,[142] Montenegro,[143] Moldova,[144] Liechtenstein[145], Switzerland,[146] FYR Macedonia,[147] USA,[148] Iceland[149] and Norway[150]).
These agreements contain clauses on data protection, and generally require the parties to guarantee a level of protection at least equivalent to that resulting from the principles contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and the amendments thereto as well as the principles laid down in the Eurojust Decision and in the Eurojust rules of procedure on data protection.

In the agreement with the United States, however, the data protection clause states that the parties shall act in full accord with their respective laws when they process personal data pursuant to the agreement, and establishes principles of "fairness", "data minimisation", "storage limitation" and "accuracy" to which the parties commit.[151]

[142] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20on%20cooperation%20between%20Eurojust%20and%20Ukraine%20(2016)/Eurojust-Ukraine-2016-06-27-EN.pdf
[143] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20on%20cooperation%20between%20Eurojust%20and%20Montenegro%20(2016)/Eurojust-Montenegro-2016-03-05-EN.pdf
[144] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/Agreement% 20on% 20coo per a tion %20between%20Eurojust%20and%20the%20Republic%20of%20Moldova%20(2014)/Eurojust-Republic-of-Moldova-2014-07-10-EN.pdf
[145] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/Agreement% 20on% 20 Coo pe ration%20between%20Eurojust%20and%20the%20Principality%20of%20Liechtenstein%20(2013)/Eurojust-Liechtenstein 2013-06-07 EN.pdf
[146] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/ Agreement% 20between% 20 Euro just %20and%20Switzerland%20(2008)/Eurojust-Switzerland-2008-11-27-EN.pdf
[147] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ agreements/ Agreement% 20on% 20 coo peration %20between%20Eurojust%20and%20the%20former%20Yugoslav%20Republic%20of%20Macedonia%20(2008)/Eurojust-fYROM-2008-11-28-EN.pdf
[148] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20Eurojust-USA% 20 (20 06)/ Eurojust- USA-2006-11-06-EN.pdf
[149] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20Eurojust-Iceland% 20 (2005) /Eurojust-Iceland-2005-12-02-EN.pdf
[150] http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20Eurojust-Nor way % 2 0(2005)/Eurojust-Norway-2005-04-28-EN.pdf
[151] These principles are drafted less comprehensively than the principles in Article 5 of the GDPR, and Directive 2016/680/EU. For example, the form of data minimisation set out in the agreement mentions adequacy and relevance, but not a commitment to ensure the personal data is not "excessive" (Directive 2016/680/EU) or "limited to what is necessary" (GDPR).

A.4. European Police Office (Europol)

A.4.1. Brief introduction to the Department / Agency

The European Police Office (hereinafter: Europol) is an EU agency headquartered in the Hague, the Netherlands. The current legal basis for Europol is Regulation (EU) 2016/794 of the European Parliament and the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (hereinafter: Europol Regulation).[152]

According to Article 4(1) of this Regulation, Europol's tasks include, inter alia: collecting, storing, processing, analysing and exchanging information, including criminal intelligence; notifying the Member States without delay of any information and connections between criminal offences concerning them; coordinating, organising and implementing investigative and operational actions to support and strengthen actions by the competent authorities of the Member States; participating in joint investigation teams, providing information and analytical support to Member States in connection with major international events; preparing threat assessments, strategic and operational analyses and general situation reports; supporting Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, including by providing operational, technical and financial support; supporting Member States' actions in preventing and combating forms of crime which are facilitated, promoted or committed using the internet. Europol, as the Central Office for combatting euro counterfeiting, shall also encourage the coordination of measures carried out to fight euro counterfeiting by the competent authorities of the Member States or in the context of joint investigation teams, where appropriate in liaison with Union bodies and the authorities of third countries (Article 4(4) Europol Regulation). Europol shall provide strategic analyses and threat assessments to assist the Council and the Commission in laying down strategic and operational priorities of the Union for fighting crime. Europol shall also assist in the operational implementation of those priorities (article 4(5) Europol Regulation).

Hence, Europol supports law enforcement authorities throughout the EU on crime fighting activities in all its mandated areas such as trafficking in human beings, illicit drugs, facilitated illegal immigration, terrorism, VAT fraud, cybercrime, euro counterfeiting. It serves as a:[153]

- support centre for law enforcement operations;
- hub for information on criminal activities;
- centre for law enforcement expertise.

A.4.2. Nature of personal data

As provided in Article 18(5) Europol Regulation, Annex II to the Europol Regulation specifies which personal data are processed by Europol and under which circumstances.

a) *For the purposes of cross-checking (in accordance with Article 18(2)(a) Europol Regulation)*
Personal data concerning the following persons may be processed: persons suspected of having committed or having taken part in a criminal offence (in respect of which Europol is competent), or who have been convicted of such an offence (Annex II (A)(1)(a); and persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to

[152] Europol Regulation, OJ L 135, 24.5.2016, p. 53–114, to be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794, last accessed 22/05/2018.
[153] Europol website, https://www.europol.europa.eu/about-europol, last accessed 22/05/2018.

believe that they will commit criminal offences in respect of which Europol is competent (Annex II (B)(1)(b).

The following data can be processed with reference to such persons: surname, maiden name, given names, alias/assumed names; date and place of birth; nationality; gender; place of residence, profession and whereabouts of the person concerned; social security numbers, driving licences, identification documents and passport data; other characteristics likely to assist in identification – e.g. specific objective physical features such as DNA profile, established from non-coding part of DNA (where necessary) (Annex II (A)(2)(a-g)). Furthermore, the following data can be processed in reference to the above-described persons: criminal offences, alleged criminal offences and when, where and how they were (allegedly) committed, means which were or which may have been used to commit those criminal offences, including information concerning legal persons, departments handling the case and their filing references, suspected membership of a criminal organisation; convictions, where they relate to criminal offences in respect of which Europol is competent; inputting party.

b) *For the purpose of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information (Article 18(2) (b-d) Europol Regulation)*

For these purposes, personal data of the following persons may be processed: persons convicted/suspected of having committed/taken part in a criminal offence (in respect of which Europol is competent); persons regarding whom there are factual indications or reasonable grounds to believe that they will commit such criminal offences; persons who might be called on to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings; victims of one of the offences under consideration or with regard to whom certain facts give reason to believe that they could be the victims of such an offence; contacts and associates; persons who can provide information on the criminal offences under consideration (Annex II (B)(1)(a-f)). The following data (inter alia) can be processed with reference to such persons: personal details (such as full names, parents' names, date and place of birth, nationality, gender, place of residence/domicile, marital status), physical description, means of identification (e.g. ID/passport/driving licence number, visual images, fingerprints, DNA profiles established from non-coding part of DNA), data relating to education, occupation and skills, economic and financial information (e.g. bank details, cash assets, property /tax data),behavioural data (e.g. places frequented, lifestyle, drug abuse), contacts and associates, means of communication and transport used, information in relation to criminal conduct (previous history, suspected involvement in criminal activities, geographical range of criminal activities, video / photographic images, references to other information systems in which information on the person is stored e.g. police/customs agencies, international organisations), information on legal persons associated with the data (e.g. legal form, capital) (Annex II (B)(2)a-l)).

Hence, as is clear from the above, personal data processed by Europol includes many categories of sensitive personal data (according to Article 9 GDPR) and data requiring specific legal protection (genetic and biometric data, data relating to health and ethnic origin, data relating to criminal activities of the data subjects). Furthermore, as explained in Article 30 Europol Regulation, processing of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18, shall be allowed if it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives.

A.4.3. Purposes of processing

Article 18 Europol Regulation lists the purposes in which processing personal data is allowed. According to Article 18(2) Europol Regulation, personal data may only be processed for the following purposes:

- cross-checking aimed at identifying connections or other relevant links between information related to persons who are convicted / suspected of having committed or taken part in a criminal offence (in respect of which Europol is competent), and persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences (in respect of which Europol is competent) (Article 18(2)(a)),
- analyses of a strategic or thematic nature (Article 18(2)(b)),
- operational analyses (Article 18(2)(c)), and
- facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations (Article 18(2)(d)).

In relation to processing for purposes of operational analysis, for every such project the Executive Director shall define the specific purpose, categories of personal data and categories of data subjects, participants, duration of storage and conditions for access, transfer and use of the data concerned, and shall inform the Management Board and the EDPS thereof (Article 18(3)(a) Europol Regulation). Personal data may only be collected and processed for the purpose of the specified operational analysis project (article 18(3)(b) Europol Regulation).

A.4.4. Entities involved

Europol may receive data from EU Member States, EU bodies, third countries, international organisations, private persons and private parties, in accordance with Article 17(1)(a-c) Europol Regulation. As specified in Articles 19-24 of Europol Regulation, Europol may also transfer data to EU Member States, Eurojust, OLAF, EU bodies, third countries and international organisations.

A.4.5. Legal basis

Subject to restrictions included in the Europol Regulation (as per Article 19(3) Europol Regulation), personal data processed by Europol may be transferred to and accessed by Member States, EU bodies, third countries and international organisations.

a) *Member States*
Article 20(1) Europol Regulation grants access to Europol data processed for the purposes of cross-checking and analysis of a strategic or thematic nature to Member States and Europol staff (with exceptions). Article 20(2) Europol Regulation grants Member States an indirect access on the basis of a hit/no hit system to information provided for the purposes of operational analysis.

b) *OLAF and Eurojust*
Furthermore, Article 21(1) Europol Regulation requires Europol to take all appropriate measures to enable Eurojust and OLAF, within their respective mandates, to have indirect access on the basis of a hit/no hit system to information provided for the purposes of cross-checking, analysis of strategic or thematic nature and operational analysis.

c) *EU bodies, third countries, international organisations*
Moreover, according to Article 24 Europol Regulation, Europol may directly transfer personal data to a Union body, insofar as such transfer is necessary for the performance of its tasks or those of the recipient Union body (not withstanding restrictions from Article 19).

As per Article 23(6) Europol Regulation, personal data may also be transferred to EU bodies, third countries and international organisations, but only if necessary for preventing and combating crime falling within the scope of Europol's objectives and in accordance with this Regulation, and if the recipient gives an undertaking that the data will be processed only for the purpose for which they were transferred. This, however, excludes special categories of personal data, which as per Article 30(5) Europol Regulation shall not be transmitted to Member States, Union bodies, third countries or international organisations unless such transmission is strictly necessary and proportionate in individual cases.

d) *Private parties*

As specified in Article 26(1) Europol Regulation, Europol may process personal data obtained from private parties, which are necessary for the performance of Europol's tasks provided they are received via a national unit in accordance with national law, via a contact point of a third country or an international organisation with which Europol has concluded, before 1 May 2017, a cooperation agreement allowing for the exchange of personal data in accordance with Article 23 of Decision 2009/371/JHA or via an authority of a third country or an international organisation which is the subject of an adequacy decision or with which the Union has concluded an international agreement pursuant to Article 218 TFEU.

According to Article 26(5)(a) and (b) Europol Regulation, Europol may not transfer personal data to private parties. Exceptions may arise on a case-by-case basis where strictly necessary and subject to any restrictions included in the Regulation (Articles 19) when the transfer is undoubtedly in the interests of the data subject, and either the data subject's consent has been given or the circumstances allow a clear presumption of consent, the transfer is absolutely necessary in the interests of preventing the imminent perpetration of a crime, including terrorism, or the transfer of personal data which are publicly available is strictly necessary for the preventing and combating forms of crime promoted or committed online.

A.4.6 .Cooperation with third countries

According to Article 25 Europol Regulation, Europol may transfer personal data to an authority of a third country or to an international organisation, insofar as such transfer is necessary for the performance of Europol's tasks (not withstanding restrictions on such transfers, stemming from Article 19(2) and (3) Europol Regulation). Such a transfer may be based on an adequacy decision of the Commission[154], finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection; an international agreement concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, or a cooperation agreement allowing for the exchange of personal data concluded, before 1 May 2017, between Europol and that third country or international organisation in accordance with Article 23 of Decision 2009/371/JHA[155].

Europol may conclude administrative arrangements to implement such agreements or adequacy decisions.

[154] Based on Article 36 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680, last acces sed 23/05/2018.

[155] Council Decision of 6 April 2009 establishing the European Police Office (Europol), OJ L 121, 15.5.2009, p. 37–66, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009D0371, last accessed 23/05/2018 (in force until 30/04/2017).

Furthermore, the Executive Director of Europol may authorise the transfer of personal data to third countries or international organisations on a case-by-case basis: 1) if the transfer is necessary in order to protect the vital interests of the data subject or of another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; 2) if it is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country; 3) it is necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions; or 4) it is necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal sanction. Such derogations may not be applicable to systematic, massive or structural transfers (Article 25(5) Europol Regulation).

Furthermore, no special categories of personal data (sensitive personal data) may be transferred to third countries unless such transmission is strictly necessary and proportionate in individual cases according to Article 30(5) Europol Regulation.

A.4.7. Actual examples

a) Denmark

Since May 2016 and the entry into force of the current Europol Regulation, as a result of a national referendum, Denmark is no longer a member of Europol. It is considered a third country as it does not participate in measures pursuant to Title V Part Three TFEU. Europol concluded an Operational and Strategic Cooperation Agreement with Denmark.[156] This agreement provides rules for the exchange of personal data and introduces a Danish liaison officer to Europol[157]. Denmark is admitted as non-voting observer on Europol's management board.[158] Moreover, even though Denmark cannot directly access Europol's data processing systems (as it is not a member, pursuant to the Agreement, Europol must assign eight Danish-speaking staff, responsible for inputting and retrieving data coming from the Danish Authorities, 24/7 (including the right to modify, correct and delete such data)[159]. The Agreement with Denmark is legally binding and falls within the scope of jurisdiction of the CJEU.[160] Furthermore, every year Denmark needs to contribute to the budget of Europol according to its GDP[161] and has to comply with a number of EU law provisions.[162]

b) Third countries

The Europol Regulation as described above introduces (in its Article 25) specific rules and legal bases regarding transfers of data by Europol outside the EU. One possibility would be an adequacy decision of the Commission in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country to which Europol transfers data ensures an adequate level of protection. Since there is no such adequacy decision in place at the moment, the other alternative for Europol to regularly transfer data to a third country is to use an appropriate framework

[156] Agreement on Operational Cooperation between the Kingdom of Denmark and the European Police Office, 28.04.2017, https://www.europol.europa.eu/publications-documents/agreement-operational-and-strategic-cooperation-between-kingdom-of-denmark-and-europol, last accessed 23/05/2018.
[157] Article 9 Operational and Strategic Cooperation Agreement with Denmark.
[158] Article 8(1)(d) Operational and Strategic Cooperation Agreement with Denmark.
[159] Article 8 and Article 10(6) Operational and Strategic Cooperation Agreement with Denmark.
[160].Articles 18-20 Operational and Strategic Cooperation Agreement with Denmark.
[161] Article 22 Operational and Strategic Cooperation Agreement with Denmark.
[162] According to Article 10(4) of the Europol-Denmark Agreement, these provisions on personal data included in Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA and Articles 24-48 Europol Regulation.

resulting from the conclusion of a binding international agreement between the EU and the receiving third country.

On 20 December 2017, the Commission adopted eight Recommendations for Council Decisions to authorise the opening of negotiations for international agreements between the European Union (EU) and eight third countries of the Middle East and North African (MENA) region, i.e. Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.[163] Such international agreements would provide the required legal basis for the exchange of personal data between Europol and the authorities of these third countries competent to fight serious crimes and terrorism.

According to Article 218 TFEU, the Commission will be responsible for negotiating these international agreements with third countries on behalf of the EU. With these eight Recommendations, the Commission seeks to obtain authorisation from the Council of the EU to start the negotiations with the eight third countries identified. Once the negotiations are completed, the European Parliament will have to give its consent to the texts of the agreements negotiated to formally conclude these agreements, while the Council will have to sign the agreement.

There are already international agreements in place which grant Europol the right to exchange personal data with third countries. Examples of such agreements include the agreements on the use of passenger name records, which to date the EU has signed with Canada[164], the USA and Australia. The agreement with Australia for instance provides, in its article 6, that the Australian Customs and Border Protection Service shall ensure the availability of relevant and appropriate analytical information obtained from PNR data to police or judicial authorities of the Member State of the European Union concerned, or to Europol or Eurojust within the remit of their respective mandates. Furthermore, a police or judicial authority of a Member State of the European Union, or Europol or Eurojust within the remit of their respective mandates, may request access to PNR data or relevant and appropriate analytical information obtained from PNR data which is necessary in a specific case to prevent, detect, investigate, or prosecute within the European Union a terrorist offence or serious transnational crime. The Australian Customs and Border Protection Service shall make such information available.[165] A corresponding provision is also included in Article 18 of the EU-USA PNR agreement.[166]

Furthermore, operational agreements which Europol concluded with third countries before 01/05/2017 also constitute a legal basis allowing for the exchange of information including personal data (in accordance with Article 25(1)(c) Europol Regulation). There are 17 such agreements in place.[167] These agreements include clauses specifying in detail the ways in which personal data can be transferred as

[163] The decision can be accessed here: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-809-F1-EN-MAIN-PART-1.PDF, last accessed 23/05/2018.
[164] This agreement, however needs to be revised, following the decision of the CJEU of 27/07/2017, https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf, last accessed 23/05/2018.
[165] Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ L 186, 14.7.2012, p. 4–16, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0714%2801%29, last accessed 23/05/2018.
[166] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, p. 5–14, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22012A0811%2801%29, last accessed 23/05/2018.
[167] With Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, Macedonia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland, Ukraine and the US, accessible at Europol website, https://www.europol.europa.eu/partners-agreements/operational-agreements, last accessed 23/05/2018.

well as security safeguards that each of the parties needs to implement.[168] Europol also hosts liaison officers from 13 of these 17 third countries with which it had concluded the operational agreements.[169] Liaison officers enable third country law enforcement agencies to be represented at Europol's headquarters. As such, they facilitate communication and cooperation. It needs to be noted though that Europol's operational agreements are not legally binding and may be terminated with little notice.[170]

[168] E.g. Article 9 Agreement on Operational and Strategic Cooperation between Australia and the European Police Office; Article 11 Agreement on Operational and Strategic Cooperation between Ukraine and the European Police Office, both can be accessed here: https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1, last accessed 23/05/2018.
[169] E.g. Article 9 of the agreement with Ukraine, Article 14 agreement with Australia, both can be accessed here: https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1, last accessed 23/0/5/2018.
[170] Cf. e.g. article 18 of the agreement with Australia, introducing an arbitrator system, and Article 20, foreseeing a 3-month notice period.

A.5. European Border and Coast Agency (Frontex)

A.5.1. Brief introduction to the Department / Agency

Frontex was established in 2004 as the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union European, by Council Regulation (EC) 2007/2004.[171] This Regulation was repealed in 2016 by Regulation (EU) 2016/1624 establishing Frontex, the European Border and Coast Agency, as the EU's border agency.[172]

The Agency's mission is to promote, coordinate and develop European border management in line with the EU Charter of Fundamental Rights and the concept of Integrated Border Management. [173]

Within the field of its mission, Frontex shall:

(a) monitor migratory flows and carry out risk analysis as regards all aspects of integrated border management;

(b) carry out a vulnerability assessment including the assessment of the capacity and readiness of Member States to face threats and challenges at the external borders;

(c) monitor the management of external borders through liaison officers of the Agency in Member States;

(d) assist Member States in circumstances requiring increased technical and operational assistance at external borders by coordinating and organising joint operations, taking into account that some situations may involve humanitarian emergencies and rescue at sea in accordance with Union and international law;

(e) assist Member States in circumstances requiring increased technical and operational assistance at external borders, by launching rapid border interventions at the external borders of those Member States facing specific and disproportionate challenges, taking into account that some situations may involve humanitarian emergencies and rescue at sea in accordance with Union and international law;

(f) provide technical and operational assistance to Member States and third countries in accordance with EU and international law, in support of search and rescue operations for persons in distress at sea which may arise during border surveillance operations at sea;

(g) set up and deploy European Border and Coast Guard teams, including a rapid reaction pool, that are to be deployed during joint operations and in rapid border interventions and within the framework of the migration management support teams;

(h) set up a technical equipment pool to be deployed in joint operations, rapid border interventions and in the framework of migration management support teams, as well as in return operations and return interventions;

(i) support Member States with screening, debriefing, identification and fingerprinting of migrants. Officers deployed by the agency refer and provide initial information to

[171] Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union. This Regulation is no longer in force.
[172] Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC.
[173] See: https://frontex.europa.eu/about-frontex/mission-tasks/.

people who need, or wish to apply for, international protection, cooperating with the European Asylum Support Office (EASO) and national authorities.

(j) support the development of technical standards for equipment, especially for tactical-level command, control and communication as well as technical surveillance to ensure interoperability at Union and national level;

(k) deploy the necessary equipment and border guards and other relevant staff from the rapid reaction pool for the practical execution of the measures needed to be taken in a situation requiring urgent action at the external borders;

(l) assist Member States in circumstances requiring increased technical and operational assistance to implement the obligation to return returnees, including through the coordination or organisation of return operations;

(m) within the respective mandates of the agencies concerned, cooperate with Europol and Eurojust and provide support to Member States in circumstances requiring increased technical and operational assistance at the external borders in the fight against organised cross-border crime and terrorism;

(n) set up pools of forced-return monitors, forced-return escorts and return specialists;

(o) set up and deploy European return intervention teams during return interventions;

(p) assist Member States on training of national border guards, other relevant staff and experts on return, including the establishment of common training standards;

(q) participate in the development and management of research and innovation activities relevant for the control and surveillance of the external borders, including the use of advanced surveillance technology, and develop pilot projects regarding matters covered by this Regulation;

(r) develop and operate, in accordance with Regulation (EC) No 45/2001 and Framework Decision 2008/977/JHA, information systems that enable swift and reliable exchanges of information regarding emerging risks in the management of the external borders, illegal immigration and return, in close cooperation with the Commission, Union bodies, offices and agencies as well as the European Migration Network;

(s) provide the necessary assistance for the development and operation of the EUROSUR and, as appropriate, for the development of a common information-sharing environment, including interoperability of systems, in particular by developing, maintaining and coordinating the EUROSUR framework;

(t) cooperate with the European Fisheries Control Agency and the European Maritime Safety Agency, each within its mandate, to support the national authorities carrying out coast guard functions, by providing services, information, equipment and training, as well as by coordinating multipurpose operations;

(u) assist Member States and third countries in the context of technical and operational cooperation between them in the matters covered by this Regulation.

Furthermore, the Agency shall provide the public with accurate and comprehensive information about its activities.[174]

A.5.2. Nature of personal data

Frontex is entitled pursuant to Article 47(1) of the funding Regulation[175] to process the following categories of personal data:

[174] Frontex's tasks are set out in Article 8, Regulation (EU) 2016/1624.

(a) personal data related to individuals suspected of involvement in the facilitation of illegal migration, human trafficking or other cross-border crimes, like terrorism, but only in the situations strictly foreseen in that provision;

(b) personal data regarding persons who cross the external borders without authorisation and whose data is collected by the European Border and Coast Guard teams, including when acting in the framework of the migration management support teams;

(c) license plate numbers, vehicle identification numbers, telephone numbers or ship identification numbers which are linked to the persons referred to in (a) and (b), and which are necessary for investigating and analysing routes and methods used for illegal immigration and cross-border crime.

Frontex is authorised under very strict conditions foreseen in Article 48 of the Funding Regulation to process personal data of certain groups of returnees. Furthermore, according to Article 49 of the Funding Regulation, it may process personal data concerning ship identification numbers.[176]

A.5.3. Purposes of processing

Frontex processes personal data for the following main purposes:

- performing its tasks of organising and coordinating joint operations, pilot projects, rapid border interventions and in the framework of the migration management support teams;
- performing its tasks of organising and coordinating return operations and return interventions;
- facilitating the exchange of information with Member States, EASO, Europol or Eurojust;
- risk analysis by the Agency;
- identifying and tracking vessels in the framework of EUROSUR[177].[178]

Please note that administrative / management purposes are not listed because they are out of scope.

A.5.4. Entities involved

The Agency only processes personal data for the abovementioned purposes. Furthermore, the entities involved in data exchanging activities are:

- The Agency;
- The Union institutions, bodies, offices, agencies (e.g. Europol, Eurojust), competent authorities of Member States,[179] and international organisations.

Furthermore, according to Article 44 of the Funding Regulation, "the Agency may take all necessary measures to facilitate the exchange of information relevant for its tasks with Ireland and the United Kingdom if it relates to the activities in which they participate in accordance with Article 51 and Article 62(5)".

[175] Regulation (EU) 2016/1624.
[176] Article 13(2) of Regulation (EU) No. 1052/2013.
[177] The European Border Surveillance system (EUROSUR) is a multipurpose system for cooperation between the EU Member States and Frontex in order to improve situational awareness and increase reaction capability at external borders. The aim is to prevent cross-border crime and irregular migration and contribute to protecting migrants' lives. See also: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/eurosur_en.
[178] Article 46, paragraph 1, Regulation (EU) 2016/1624.
[179] Article 47, paragraph 2, Regulation (EU) 2016/1624.

The Frontex Regulation only allows sharing of strategic information with third country but not the exchange of personal data.[180]

A.5.5. Legal basis

Frontex, as an EU agency processes personal data in accordance with the provisions of Regulation 45/2001/EU,[181] as provided for by Article 45 of the Funding Regulation (EU) 2016/1624. In line with Article 45(2) of the Funding Regulation, Specific Implementing Measures have been adopted by Frontex in order to ensure compliance with Regulation (EC) 45/2001 when processing personal data.[182] It should be noted that the European Commission adopted a proposal on 10 January 2017 which repeals Regulation (EC) 45/2001.[183] The Regulation 45/2001 replacement text should be adopted in time to become applicable at the same time as the GDPR.[184]

A.5.6. Cooperation with third countries

Numerous provisions of Regulation (EU) 2016/1624 provide the legal basis for Frontex to cooperate with third countries. Nonetheless, one particular provision, Article 54 – "Cooperation with third countries" sets out the key points of such cooperation. Cooperation with non-EU countries is an integral part of Frontex's mandate to ensure implementation of the European integrated border management (IBM) and one of the strategic priorities for the agency's work.[185] As provided for by Article 54(2), such cooperation is usually based on working arrangements[186] signed between the agency and the competent authorities of the non-EU country. In particular, those working arrangements shall specify the scope, nature and purpose of the cooperation and be related to the management of operational cooperation. The draft arrangements shall receive the Commission's prior approval and the Agency shall inform the European Parliament before a working arrangement is concluded.

The type of cooperation outlined in Frontex's agreements with third countries includes also information processing and exchange; however, those do not include processing and/or exchanging of personal data.

A.5.7. Actual examples

No actual examples.

[180] Article 45, paragraph 4, Regulation (EU) 2016/1624; See also: https://db.eurocrim.org/db/en/doc/2945.pdf .
[181] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; see also: https://frontex.europa.eu/about-frontex/data-protection/.
[182] See: https://frontex.europa.eu/assets/Key_Documents/MB_Decision/2015/MB_Decision_34_2015_on_adoption_of_data_protection_IR_for_administrative_purposes.pdf; https://frontex.europa.eu/about-frontex/data-protection/.
[183] See: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0008.
[184] See: https://edps.europa.eu/data-protection/data-protection/legislation_en.
[185] See: https://frontex.europa.eu/partners/non-eu-countries/
[186] Frontex has concluded working arrangements with the authorities of 18 countries: Albania, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Canada, Cape Verde, the former Yugoslav Republic of Macedonia, Georgia, Kosovo, Moldova, Montenegro, Nigeria, the Russian Federation, Serbia, Turkey, Ukraine and the United States.
The agency has also signed working arrangements with the CIS Border Troop Commanders Council and the MARRI Regional Centre in the Western Balkans. See also: https://frontex.europa.eu/partners/non-eu-countries/; see also the list of working arrangements with non-EU Countries: https://frontex.europa.eu/about-frontex/key-documents/?category=working-arrangements-with-non-eu-countries .

A.6. The Directorate General Taxation and Customs Union's (DG TAXUD)

A.6.1. Brief introduction to the Department / Agency

The Directorate General Taxation and Customs Union's (TAXUD)[187] mission is to develop and manage the Customs Union and to develop and implement tax policy across the EU for the benefit of citizens, businesses and the Member States. Particular attention is given to the Internal Market, by making sure it functions smoothly and efficiently.[188] Article 3.1 (a) of Treaty on the Functioning of the EU (TFEU) provides that the Customs Union is an exclusive competence of the European Union built on the principles of free movement of goods within the Union and a common external tariff towards third countries.[189]

The Directorate General works to provide solutions in the tax and customs fields to Member States and economic operators, thus enabling them to respond to current economic, social and environmental challenges, both at European and international level. More specifically the Directorate General's activity aims at:[190]

- Simplifying and modernising the tax and customs administrative rules and procedures with which European economic operators must comply;
- Assisting Member States to correctly apply the EU tax and customs acquis as well as monitoring the proper transposition and application of tax and customs legislation;
- Managing and securing our common external border, combating the flow of illegal trade and reinforcing the security of the international supply chain;
- Developing a coherent, modern and simple VAT system;
- Working towards a coherent direct tax strategy designed to limit distortions which arise from the interaction of the different tax systems of the Member States, with particular emphasis on company taxation and capital income;
- Working at an international level to improve transparency and information exchange and to ensure coherence between taxation, customs and wider objectives of the Union particularly in the areas of commercial policy, development aid and "Wider Europe";
- Reinforcing candidate countries' capacity to apply the community customs and tax acquis;
- Adapting energy taxation to the needs of a low carbon economy;
- Assisting Member States to combat fraud and tax evasion.

A.6.2. Nature of personal data

When carrying out its tasks, DG TAXUD processes personal data which are likely to involve third country transfer. For example:

[187] DG TAXUD is composed by the following five Directorates: Directorate A – Customs; Directorate B - Digital delivery of Customs and Taxation Policies; Directorate C - Indirect Taxation and Tax Administration; Directorate D - Direct taxation, Tax Coordination, Economic Analysis and Evaluation; Directorate E - International and General Affairs.

[188] Mission Statement and Strategic Goals, European Commission's Directorate General for Taxation and the Customs Union. Available at:https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/common/about/welcome/mission_statement_en.pdf.

[189] See also Articles 28 and 29 of TFEU.

[190] *Ibidem*.

a) DG TAXUD processes data contained in an application to issue Authorised Economic Operator (AEO) certificates by customs authorities in the Member States.[191] The types of personal data exchanged are: name, organisation, street and number, country, postal code, city, phone, fax, e-mail, address.

b) DG TAXUD leads the Programme Information and Collaboration Space (PICS)[192] which is an online collaboration tool for Tax and Customs professionals working in national administrations across Europe. In this context, the following information is provided by the users: personal information (picture, prefix, first Name, surname and country); contact details (office and mobile phone, e-mail and languages in which the user can be contacted); professional information (organisation, job title and areas of expertise).

c) DG TAXUD controls and manages the Economic Operators Identification and Registration system (EORI),[193] it works as a central database to which all customs authorities in Member States and the Commission have access. It enables customs to verify the EORI number declared in the summary declarations and customs declarations or in applications for authorisations or other customs related actions. This database processes the following personal data: EORI number, full name of the person, address of establishment/address of residence and VAT identification number(s), where assigned by Member States. Moreover, in the case of a natural person, it processes also other data such as date of birth, etc.

d) DG TAXUD has a role of joint controller on all data of the Registered Exporters system (REX).[194] The data encoded in the REX system are given by the data subject on a voluntary basis in the application form he has to submit to his competent authorities or customs authorities to request its registration as registered exporter. The data fields of the data subject are: name; full address (including country); EORI (for EU exporters) or TIN number[195] (for third countries); contact details of the exporter including telephone and fax number as well as e-mail address where available; type of activity; indicative description of goods which qualify for preferential treatment, including indicative list of Harmonised System headings; consent for publication of the data fields on a public website; registration number; date of registration; date from which the registration is valid; date until which the registration is valid (if the registration is revoked).

A.6.3. Purposes of processing

a) The purpose of the processing of personal data in the Authorised Economic Operator (AEO) database is the management of the EU applications and certificates in order to allow the MS competent customs authorities to manage centrally the AEO applications, from the acceptance to the rejection or the issue of the AEO certificate, the AEO certificates and their whole life-cycle including the suspension, revocation, suspension withdrawal, revocation annulment, revocation suspension, revocation suspension withdrawal and re-assessment. [196]

[191] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=34427.
[192] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=38627.
[193] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=34447.
[194] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/_de tails.htm?id=41667.
[195] These numbers are identification numbers of exporters in their countries.
[196] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-regi ster/details.htm?id=34427

b) In relation to the Programme Information and Collaboration Space (PICS), the online collaboration platform supports the objective of the programmes namely to support the functioning and modernisation of the Customs Union in order to strengthen the internal market by means of cooperation between participating countries, their customs authorities and their officials (Customs 2020); and to improve the proper functioning of the taxation systems in the internal market by enhancing cooperation between participating countries, their tax authorities and their officials (Fiscalis 2020).[197]

c) The EORI system[198] was established in order to implement the security measures introduced by the Regulation laying down the Union Customs Code.[199] They will be more effective if the persons concerned can be identified by a common number that is unique to each individual person and valid throughout the Union.

d) Finally, the Registered Exporters system (REX)[200] put in place a register containing all exporters entitled to make statements on origin for goods they export in the context of preferential trade arrangements that the EU has with third countries. On statements on origin, exporters need to indicate the Registration Number they receive after their successful registration. If an exporter is not registered, he has not received a Registration Number and he is not in a position to correctly fill in the statements on origin he makes out. The register of data is also to be used by the counterparty receiving a statement on origin for validating that the Registration Number indicated on it corresponds to the one of the exporter and that this exporter has still a valid (not revoked) registration.[201]

A.6.4. Entities involved

a) Authorised Economic Operator (AEO).[202]

The European Commission is the entity which controls and manages the AEO central database. The European Commission provides and manages the technical infrastructure but not the data as such. The responsibility for entering, modifying and deleting data lies with the national competent customs department. The Commission can only consult the data for monitoring and statistical purpose. The data subjects are the AEO applicant having submitted their AEO application and designated contact persons the processed data refer to and identify. Moreover, the access to all personal data related to an application is granted to authorised officers in the customs authorities of the Member States and to the European Commission.

b) Programme Information and Collaboration Space (PICS).[203]

The project is managed by DG TAXUD Units R3 and R5. PICS and all its data is stored on DIGIT infrastructure. The system is operated by DG TAXUD's ITSM2 contractor who also provides the support to end-users. The recipients of the data are all users of PICS with the correct access rights. PICS users are officials from the

[197] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=38627
[198] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=34447
[199] Regulation (EEC) No 2913/92, as amended by Regulation (EC) No 648/2005 of the European Parliament and of the Council (OJ L 117, 4.5.2005, p. 13).
[200] The REX system starts being used for the GSP scheme as from 1 January 2017.
[201] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=41667
[202] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=34427.
[203] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=38627.

European Commission and from national administration from participating countries. Members from third countries are accepted in exceptional situations when content needs to be shared with them. In these situations, they receive the status of "external users" and can access specific parts of PICS without seeing personal information of other users.

c) Economic Operators Identification and Registration system (EORI).[204]

Member States are the controllers with respect to the processing of the data they have entered in EORI central database. The European Commission is the entity which controls and manages the EORI central database. The Commission's role is just to provide the infrastructure that allows the "pooling" of data received from Member States. As such, the Commission does not alter the content of the database. It merely replicates national records. The access to all personal data related to an application is granted to authorised officers in the customs authorities of the Member States and the European Commission.

d) Processing of data stored in the Registered Exporters system (REX).[205]

Competent authorities in beneficiary countries and customs authorities in Member States introduce in the REX system the data they receive from their exporters in the application form they must submit to become registered exporters. The European Commission is the entity which controls and manages the REX system. The European Commission provides and manages the technical infrastructure but not the data as such. Moreover, data in the REX system are accessed by authorised officers in competent authorities in beneficiary countries and in customs authorities in Member States. The REX system implemented by the European Commission is used by beneficiary countries of the GSP schemes of the EU, of Norway and of Switzerland. For this reason, Norway and Switzerland need to access the data in the system. If the consent is given by the data subject, the data are published on the TAXUD website and are publicly available. If a Member State replicates the data in a national system, access to the data is governed by the national provisions on data protection in the Member State implementing Directive 95/46/EC.[206]

A.6.5. Legal basis

a) Authorised Economic Operator (AEO):[207] the concept of AEO has been introduced by the security amendments to the Community Customs Code and to its implementing provisions:

- Article 5a of Regulation (EC) no 648/2005 of the European Parliament and of the Council of 13 April 2005 amending Council Regulation (EEC) no 2913/92 establishing the Community Customs Code;
- Articles 14 a) to 14 x) of Commission Regulation (EC) No 1875/2006 of 18 December 2006 amending Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code.

[204] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-re gister/details.htm?id=34447.
[205] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=41667.
[206] The General Data Protection Regulation (GDPR), the new EU-wide data protection instrument will become directly applicable on 25 May 2018, replacing Directive 95/46/EC.
[207] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=34427

b) Programme Information and Collaboration Space (PICS):[208] the legal basis for personal data processing is:

- Regulation (EU) No 1294/2013 of the European Parliament and of the Council of 11 December 2013 establishing an action programme for customs in the European Union for the period 2014-2020 (Customs 2020).
- Regulation (EU) No 1286/2013 of the European Parliament and of the Council of 11 December 2013 establishing an action programme to improve the operation of taxation systems in the European Union for the period 2014-2020 (Fiscalis 2020)

c) Economic Operators Identification and Registration system (EORI):[209] the legal basis for the EORI number and the EORI database is Commission Regulation (EC) No 312/2009 of 16 April 2009 amending Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code. The provisions on the EORI number neither limit nor undermine the rights and obligations derived from rules governing the requirement to register for, and obtain, any identification number which may be required in individual Member States in fields other than customs, such as taxation or statistics. Moreover, the EORI database enables customs to verify the EORI number declared in the summary declarations and customs declarations or in applications for authorisations or other customs related actions. The processing operations on personal data in this context are necessary and lawful under article 5 (a) of Regulation (EC) 45/2001[210] ('necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof').

d) Processing of data stored in the Registered Exporters system (REX):[211] the rules concerning the Registered Exporters system are part of the GSP rules of origin and are laid down in Commission Implementing Regulation (EU) No 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code. The application form for requesting registration in the REX system is Annex 22-06 of Commission Implementing Regulation (EU) No 2015/2447.

The Registered Exporters system will be used for the Overseas Countries and Territories. For this reason, the rules concerning the Registered Exporters system are repeated in Annex VI of Council Decision 2013/755/EU on the association of the overseas countries and territories with the European Union (the Overseas Association Decision).

In addition to the GSP and the Overseas Association Decision, Article 68 of Commission Implementing Regulation (EU) No 2015/2447 envisages that the Registered Exporter system may also be used in bilateral/multilateral preferential arrangements the EU has with third countries, in which it is provided that a

[208] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=38627

[209] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=34447

[210] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The European Commission adopted a proposal on 10 January 2017 which repeals Regulation (EC) 45/2001 and brings it into line with the GDPR. The proposal is currently under discussion in the European Parliament and the Council of the European Union. The Regulation 45/2001 replacement text should be adopted in time to become applicable at the same time as the GDPR (25th May).

[211] European Commission, Register of the Data Protection Officer. Available to non-EU countries at: http://ec.europa.eu/dpo-register/details.htm?id=41667.

document on origin may be completed by an exporter in accordance with the relevant Union legislation.

A.6.6. Cooperation with third countries

a) Authorised Economic Operator (AEO)[212]

The objective of mutual recognition of AEO status is that one customs administration in one country recognises the AEO authorisation issued under the programme in the other country/party and agrees to provide substantial, comparable and, where possible, reciprocal benefits/facilitations to the mutually recognised AEOs. The practical implementation of a Mutual Recognition Agreement requires that some details are exchanged between the customs authorities of partner countries. Data exchange is subject to the prior consent of the authorised economic operator and to the customs authorities of partner countries taking appropriate measures to ensure data protection, security, confidentiality and integrity. Currently data are exchanged with Japan, the United States of America and China (for more information, please see question 7).

b) Programme Information and Collaboration Space (PICS)[213]

PICS users are mainly from EU Member States, but the Customs and Fiscalis Regulations extended the list of participating countries for the following reasons:

- Customs 2020, recital 3: in order to support the accession process of the candidate countries, the customs administrations of these countries benefit fully from the Programme and by extension from PICS. Moreover, to support the customs reforms in the countries participating in the European Neighbourhood Policy, their administrations can benefit from the Programme when appropriate; in this respect, they benefit from PICS when participating in specific projects financed by the Programme.
- Fiscalis 2020, recital 5: in order to support the accession process of the candidate countries, the tax administrations of these countries benefit fully from the Programme and by extension from PICS.

Regarding the transfer of personal data to non-EU participating countries, when connecting for the first time, users from within the European Union will be offered the three following options:

- they can refuse their personal information to be disclosed to all non-EU participants;
- they can consent to disclose their personal information only to users from national administrations in non-EU participating countries;
- they can consent to disclose their personal information to all users from non-EU participating countries.

Consequently, users from non-EU countries will see only anonymised information on PICS for users who will have selected the relevant option.

c) Economic Operators Identification and Registration system (EORI)[214]

The European Union concludes agreements with third countries with a view to recognising the Authorised Economic Operators' (AEO) programme and the other country's trade partnership programme and to facilitating customs controls relating to security and safety. Based on these agreements the name, address and

[212] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=34427.
[213] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=38627.
[214] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=34447

identification number of traders is exchanged. Data exchange is subject to the prior consent of the authorised economic operator and the customs authorities of partner countries take the appropriate measures to ensure data protection, security, confidentiality and integrity.

d) Processing of data stored in the Registered Exporters system (REX)[215]

In addition to the access to the data from Norway[216] and Switzerland[217] (as explained in question 4), Norway and Switzerland have the possibility to replicate the data concerning the EU exporters and the exporters of the beneficiary countries of their GSP scheme.

Finally, it should also be noted that, in the absence of any formal arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations which are not subject to Directive 95/46/EC (repealed by the General Data Protection Regulation).[218]

A.6.7. Actual examples

a) Currently, within the processing in the AEO database of data contained in an application to issue AEO certificates by customs authorities in the Member States,[219] data are exchanged with Japan,[220] the United States of America[221] and China.[222]

The data exchanged with Japan, the United States and China are a restricted subset of the information contained in the EOS system, since only the following is exchanged:

(a) name;
(b) address;
(c) status of membership;
(d) validation or authorisation date;
(e) suspensions and revocations;
(f) the unique authorisation or identification number (in a form mutually determined by the customs authorities).

The protection of personal data is ensured by specific provisions. Regarding data transfer, treatment of data exchanged with the United States is subject to the binding data protection safeguards set out in section V (Treatment of data) of the aforementioned Decision. The same approach is taken with respect to the data exchange with China and binding data protection safeguards are set out in Article 6

[215] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=41667
[216] As the data protection Directive 95/46/EC applies to all countries of the EEA, which includes all EU countries, Iceland, Liechtenstein and Norway, it is admitted that Norway provides adequate level of data protection.
[217] In accordance with Commission Decision 2000/518/EC (OJ L 215, 25.8.2000, p. 1; http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0518), Switzerland provides adequate protection of personal data.
[218] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, is repealed with effect from 25 May 2018.
[219] http://ec.europa.eu/dpo-register/details.htm?id=34427.
[220] Decision No 1/2010 of the Joint Customs Cooperation Committee of 24 June 2010 pursuant to Article 21 of the Agreement between the European Community and the Government of Japan on Cooperation and Mutual Administrative Assistance in Customs Matters regarding mutual recognition of Authorised Economic Operators programmes in the European Union and in Japan.
[221] Decision of the US-EU Joint Customs Cooperation Committee of 4 May 2012 regarding mutual recognition of the Customs-Trade Partnership Against Terrorism program in the United States and the Authorised Economic Operators programme of the European Union.
[222] Decision of the Joint Customs Cooperation Committee established under the Agreement between the European Community and the Government of the People's Republic of China on cooperation and mutual administrative assistance in customs matters of 16 May 2014 regarding mutual recognition of the Authorised Economic Operator programme in the European Union and the Measures on Classified Management of Enterprises Program in the People's Republic of China.

(Treatment of Data) of the Decision. Lastly, data exchanged with Japan are covered by European Commission decision 2011/197/EU of 27 July 2011 which recognises that an adequate level of protection is offered by Japan to personal data transferred from the EU by the European Commission to Japan in view of the mutual recognition of AEO programmes.

b) Within the Programme Information and Collaboration Space, exchange of information with non-EU countries takes place to support the accession process of the candidate countries (Customs 2020 Programme[223] and Fiscalis 2020 Programme[224]). In this context, the following candidate and potential candidate countries have joined the programme: Albania, Bosnia and Herzegovina, the former Yugoslav Republic of Macedonia, Montenegro, Serbia and Turkey.

c) Data in the REX system is accessed by authorised officers in competent authorities in beneficiary countries and in customs authorities in Member States. The REX system implemented by the European Commission is used by beneficiary countries of the GSP schemes of the EU, of Norway and of Switzerland. The following table shows the GSP beneficiary countries that are currently applying the REX system and the countries which will effectively apply the REX system when they comply with the 2 pre-requisites:[225]

Table 7– GSP beneficiary countries

GSP beneficiary countries	Effective application date of the REX system (*)	End of the transition period
Afghanistan	REX system not yet applied	31/12/2018
Angola	25/04/2018	30/06/2018
Armenia	01/01/2018	31/12/2018
Bhutan	01/01/2017	30/06/2018
Bolivia	08/05/2018	31/12/2018
Burundi	REX system not yet applied	30/06/2018
Central African Republic	REX system not yet applied	31/12/2017
Chad	REX system not yet applied	30/06/2018
Comoros	06/01/2017	30/06/2018
Congo	REX system not yet applied	30/06/2018
Cook Islands	17/04/2018	30/06/2018
Democratic Republic Congo	REX system not yet applied	30/06/2018

[223] European Commission website, The Customs 2020 Programme. Available at: https:// ec. eu ro pa .eu/taxation_customs/business/customs-cooperation-programmes/customs-2020-programme_en.
[224] European Commission, The Fiscalis 2020 Programme. Available at: https://ec.europa.eu/taxation_customs/fiscalis-programme_en .
[225] For more information, please visit the European Commission website. Available at: https://ec.europa.eu/taxation_customs/business/calculation-customs-duties/rules-origin/general-aspects-preferential-origin/arrangements-list/generalised-system-preferences/the_register_exporter_system_en

Djibouti	REX system not yet applied	31/12/2017
Equatorial Guinea	REX system not yet applied	31/12/2017
Eritrea	REX system not yet applied	31/12/2018
Ethiopia	07/03/2017	31/12/2017
Gambia	REX system not yet applied	31/12/2018
Ghana	REX system not yet applied	31/12/2018
Guinea	REX system not yet applied	31/12/2018
Guinea Bissau	05/12/2017	30/06/2018
India	01/01/2017	30/06/2018
Ivory Coast	REX system not yet applied	31/12/2018
Kenya	01/01/2017	31/12/2017
Kiribati	04/04/2018	30/06/2018
Laos	01/01/2017	31/12/2017
Liberia	REX system not yet applied	31/12/2017
Malawi	01/01/2018	31/12/2018
Mali	REX system not yet applied	31/12/2017
Micronesia	REX system not yet applied	31/12/2017
Mozambique	REX system not yet applied	30/06/2019
Myanmar	01/01/2018	31/12/2018
Nauru	REX system not yet applied	31/12/2017
Nepal	01/01/2017	30/06/2018
Niger	REX system not yet applied	31/12/2018
Niue Island	28/06/2017	31/12/2017
Pakistan	06/03/2017	31/12/2017
Rwanda	07/03/2018	31/12/2018
Sao Tomé & Principe	REX system not yet applied	30/06/2018
Sierra Leone	REX system not yet applied	31/12/2017
Solomon Islands	20/09/2017	30/06/2018
Somalia	REX system not yet applied	31/12/2017

South Sudan	REX system not yet applied	31/12/2017
Sri Lanka	01/01/2018	31/12/2018
Sudan	REX system not yet applied	31/12/2018
Swaziland	01/01/2018	31/12/2018
Syria	REX sytem not yet applied	31/12/20
Tanzania	REX system not yet applied	31/12/2018
Timor Leste	REX system not yet applied	31/12/2017
Togo	REX system not yet applied	30/06/2018
Tonga	REX system not yet applied	30/06/2018
Tuvalu	REX system not yet applied	31/12/2017
Yemen	REX system not yet applied	30/06/2018
Zambia	01/01/2017	30/06/2018

Source: European Commission. Last update 23.05.2018

A.7. European Aviation Safety Agency

A.7.1. Brief introduction to the Department / Agency

The European Aviation Safety Agency (hereinafter referred to as "EASA") was established in 2002 by Regulation (EU) 216/2008 (hereinafter referred to as "EASA Regulation").[226]

Its member states are all the EU Member States, Switzerland, Norway, Iceland and Liechtenstein. It has four international permanent representations in Montreal (Canada), Washington (United States of America), Beijing (China) and Singapore.

EASA's mission is to: ensure the highest common level of safety and environmental protection for EU citizens; provide a single regulatory and certification process among Member States; facilitate the internal aviation single market and create a level playing field; work with other international aviation organisations and regulators.

The agency's tasks are: to draft implementing rules in all fields pertinent to its mission; to certify and approve products and organisations in fields where it has exclusive competence (e.g. airworthiness); to provide oversight and support to Member States in fields where it has shared competence (e.g. Air Operations, Air Traffic Management); to promote the use of European and worldwide standards; to cooperate with international actors in order to achieve the highest safety level for EU citizens globally (e.g. EU safety list, Third Country Operators authorisations).

The legal basis for the establishment of EASA is Article 80(2) of the Treaty establishing the European Community (EC Treaty) – today Article 100(2) of the Treaty on the Functioning of the European Union (TFEU). Both provisions envisage "appropriate provisions" to be laid down for sea and air transport.

A.7.2. Nature of personal data

Article 15(1) of the EASA Regulation provides that the Commission, EASA and National Aviation Authorities from the different Member States shall exchange any information available to them in the context of its application and its implementing rules. This provision also determines that entities entrusted with the investigation of civil aviation accidents and incidents, or with the analysis of occurrences, are entitled to access such information. Article 15(3) further obliges national aviation authorities to, in accordance with their national legislation, "take necessary measures to ensure appropriate confidentiality of the information received by them".

According to Article 16, without prejudice to applicable rules of criminal law, including national rules on access to information by judicial authorities, and without applying to cases of gross negligence:

i) the source of the information must be protected;

ii) Member States shall refrain from instituting proceedings in respect of unpremeditated or unintentional infringements of the law which came to their attention only because they were reported pursuant to the Regulation; and

iii) Member States shall ensure that employees who provide information in application of the Regulation are not subject to any prejudice on the part of their employer.

Finally, the framework service contracts signed between EASA and National Aviation Authorities include legal provisions on confidentially binding both parties, including in the case of access to EASA's information system on occurrence reporting.

[226] Regulation (EU) 216/2008, O.J. 2008, L 79/1, ("EASA Regulation").

A.7.3. Purposes of processing

EASA processes personal data in view of the performance of its tasks carried out in the public interests on the basis of European Union law or in the legitimate exercise of official authority vested in it or in a third party to whom the data are disclosed. Within its internal system of occurrence reporting, for instance, the purpose of the processing of personal data is to use the information to improve the level of aviation safety since the success of EASA's task in this regard depends on the reliability and completeness of the occurrence information reported.

A.7.4 .Entities involved

EASA is the controller of the processed personal data. Access is strictly given to EASA employees dealing directly with the task for which the data has been collected or any external project managers, experts or team leaders working on behalf of EASA.

A.7.5. Legal basis

The legal basis for the processing of personal data by EASA is Article 5 of Regulation (EC) 45/2001[227] (the processing of personal data is lawful when it is necessary for the performance of tasks carried out in the public interest) and Article 15 of the EASA Regulation mentioned above. Pursuant to the latter, EASA must observe the highest possible level of confidentiality. In addition, the processing of personal data must be in compliance with Regulation (EC) 1049/2001.[228]

In accordance with this legal framework, EASA must guarantee the confidentiality of the occurrence information and the protection of personal data in its internal system and expects that others who hold, process, access and use such data declare their intentions to respect the obligations by which it is bound.

A.7.6. Cooperation with third countries

Article 27 of the EASA Regulation provides that EASA shall assist the EU and the Member States in their relations with third countries, in particular by assisting them in the harmonising of rules and mutual recognition regarding approvals attesting the satisfactory application of rules. The same provision allows for the cooperation between EASA and aeronautical authorities of third countries and the international organisations competent in the matters covered by the Regulation in the framework of working arrangements concluded with these bodies, in accordance with EU law and subject to prior approval of the European Commission.

In light of the foregoing, EASA assists non-European authorities when they certify European products and services and issues European certificates for non-European products. It does so through Bilateral Agreements and Working Arrangements.

The European Union – with EASA supporting the European Commission during their negotiation and implementation – has concluded several Bilateral Aviation Safety Agreements (BASA) with different third countries such as the United States of America, Canada and Brazil.

Furthermore, Working Arrangements (WA) are usually signed between EASA and the authority of a non-EU country, or a regional or international organisation. These cover

[227] Regulation (EC) 45/2001, O.J. 2001, L 008, ("Processing of Personal Data by Community Institutions Regulation"). Please note that, in the context of the comprehensive reform of the EU's legal framework for data protection, Regulation 45/2001 will soon be replaced by a Regulation "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data", proposed by the European Commission in January 2017 (https://eur-lex.europa.eu/procedure/EN/2017_2). The aim of the latter is to align the current legislation with the General Data Protection Regulation (GDPR) that has been fully applicable since 25 May 2018. For more information please see. http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608754/EPRS_BRI(2017)608754_EN.pdf (April 20 18), last accessed 18 May 2018. Furthermore, by reason of Article 58(4) of the EASA Regulation, the information gathered by EASA is subject to Regulation (EC) 45/2001.

[228] Regulation (EC) 1049/2001, O.J. 2001, L 145, ("Public Access to Documents Regulation").

matters of technical nature and are typically used to facilitate EASA's tasks of certification or the validation by a foreign authority of EASA certificates. EASA directly negotiates and concludes these arrangements which, unlike Bilateral Aviation Safety Agreements, do not allow for mutual recognition of certificates.

Finally, it should also be noted that, in the absence of any formal agreements or arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations which are not subject to Directive 95/46/EC (now repealed by the General Data Protection Regulation).[229]

A.7.7. Actual examples

A first example in this context is the Bilateral Aviation Safety Agreement (BASA) concluded between the EU and the United States of America[230] in 2011. Article 9 envisages the exchange of safety data relating to accidents or incidents involving civil aeronautical products or regulated entities (upon request and in a timely manner) to Technical Agents from both parties. It also envisages the exchange of other safety information "in accordance with the procedures developed by the Technical Agents".

Moreover, Article 10 states that both the EU and the United States of America recognise that information related to the Agreement submitted by a regulated entity or a party may contain intellectual property, trade secrets, confidential business information, proprietary data "or other data held in confidence by that regulated entity or another person (restricted information)". As such, unless required by law, the Agreement prohibits any party from copying, releasing or showing information identified as restricted to anyone other than an employee of that party without prior written consent of the person or entity possessing confidentiality interests in the restricted information. Pursuant to this Article, the European Union is obliged to treat any restricted information it shares with Aviation Authorities or other (similar) entities as sensitive, thereby having to ensure that such information is not copied, released or shared with anyone else but the responsible employee without due consent being given beforehand.

The other two BASA Agreements celebrated with Brazil and Canada, in 2013 and 2011 respectively, include identical obligations.[231]

The second example is the Working Arrangement between EASA and Turkey[232] focusing on the collection and exchange of information relating to safety of aircraft which includes, *inter alia*, pilot reports, incident reports and complaints. The exchange of information and cooperation between the parties, as well as its confidentiality, is regulated by Articles 5 and 6 of the working arrangement. According to those provisions, the Directorate General of

[229] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, is repealed with effect from 25 May 2018.

[230] Agreement between the United States of America and the European Community on Cooperation in the Regulation of Civil Aviation Safety, consolidated version of March 2016, retrieved from https://www.easa.europa.eu/sites/default/files/dfu/Consolidated%20version%20of%20the%20Agreement%20between%20the%20USA%20and%20the%20EU%20on%20cooperation%20in%20the%20regulation%20of%20civil%20aviation%20safety.pdf, last accessed on 03 May 2018.

[231] Technical Implementation Procedure for Airworthiness and Environmental Certification under the Agreement between the Government of the Federative Republic of Brazil and the European Union on Civil Aviation Safety, consolidated version of March 2017, retrieved from https://www. easa.europa .eu/ sites/ default/files/dfu/TIP%20EASA-ANAC%20Rev%203%20signed.pdf, last accessed on 03 May 2018; Technical Implementation Procedures for Airworthiness and Environmental Certification under the Agreement on Civil Aviation Safety between the Government of the Canada and the European Union, consolidated version of September 2017, retrieved from https://www.easa.europa.eu/sites/default/files/dfu/EASA-TCCA%20Technical%20Implementation%20Procedures%20for%20airworthiness%20and%20environmental%20certification%2C%20Revision%203%20dated%2018%20Sept%202017.pdf, last accessed on 03 May 2018

[232] Working Arrangement between the European Aviation Safety Agency and the Directorate General of Civil Aviation of the Republic of Turkey on collection and exchange of information on the safety of aircraft using EU airports and airports of non-EU States that participate in the EU SAFA Programme, including airports of the Republic of Turkey, 2012, retrieved from https:/ /www. easa. europa. eu/sites/ default/ files/ dfu/ WA%20SAFA%20Turkey.pdf, last accessed on 04 May 2018.

Civil Aviation of the Republic of Turkey "shall, in accordance with its national legislation, take all necessary measures to ensure appropriate confidentiality of the information received" under the arrangement and shall use the information "solely for the exercise of its responsibilities related to the improvement of civil aviation safety". Any change to these measures and/or legislation must be notified to EASA. Similarly, EASA is bound by relevant EU legislation to ensure appropriate confidentiality of the information it receives, as well as of its use.

A.8. Directorate-General for Mobility and Transport (DG MOVE)

A.8.1. Brief introduction to the Department / Agency

The Directorate-General for Mobility and Transport of the European Commission (hereinafter referred to as "DG MOVE") was created in February 2010 and is responsible for developing and implementing EU policies in the field of transport. DG MOVE's mission is to ensure that transport policies are designed for the benefit of all sectors of society through the use of legislative proposals and programme management, including the financing of projects. In addition to developing EU policies in the transport sector and handling State aid files, DG MOVE manages, for instance, the Connecting Europe Facility funding programme for the Trans-European Transport Network. It includes the following agencies: European Maritime Safety Agency, European Aviation Safety Agency, Executive Agency for Small and Medium-Enterprises, Innovation and Networks Executive Agency. It is furthermore involved in two Joint Undertakings, SESAR Joint Undertaking and Shift2Rail Undertaking.

The legal bases for the EU's common transport policy – including the "sustainable mobility" model taking on greater importance until 2020 – are Article 4(2)(g) and Title VI of the Treaty on the Functioning of the European Union (TFEU).[233]

A.8.2. Nature of personal data

As an EU body, there are different circumstances under which DG MOVE might process (and exchange) personal data. Two concrete examples are given below.

The first example[234] is the processing and exchanging of personal data by DG MOVE in the context of the award and management of grants. The data is provided by applicants and beneficiaries of the programmes and initiatives managed by DG MOVE. Applicants are the legal entities that apply for funding through the submission of proposals, whereas the beneficiaries are the successful applicants/participants in funded research projects. The information provided may be included in the Early Detection and Exclusion System Database (EDES-Database) managed by the European Commission, pursuant to Regulation (EU) 2015/1929 on the financial rules applicable to the general budget of the EU.[235] The database contains information on economic operators that could represent a threat to the Union's financial interests, economic operators who are in one of the exclusion situations listed in Article 106(1) and economic operators on which financial penalties are imposed. The data subjects are the staff of applicants/beneficiaries with concrete roles in the proposals/projects (primary coordinator contacts, coordinator contacts, participant contacts, tasks manager, team members, etc.).

The second example[236] is the processing and exchanging of personal data by DG MOVE in the context of registration, selection and management of independent experts. This includes experts who advise or assist in, for instance, the evaluation of proposals or the design of Union research and innovation policy (including preparation of future programmes). Just like with the first example given in the previous paragraph, the information provided may be included in the Early Detection and Exclusion System Database (EDES-Database) managed by the European Commission, pursuant to Regulation (EU) 2015/1929 on the financial rules applicable to the general budget of the EU.

[233] Please see DG MOVE's mission statement and 2016-2020 Strategic Plan here: https://ec.europa.eu/info/sites/info/files/strategic-plan-2016-2020-dg-move_amended_july_en.pdf, last accessed 15 May 2018.
[234] Please see Register of the European Data Protection Officer, European Commission, in particular http:// ec. europa.eu/dpo-register/details.htm?id=44449, last accessed on 11 May 2015.
[235] Regulation (EU, Euratom) 2015/1929, O.J. 2015, L 286/1 ("Financial Rules Applicable to General Budget of the Union Regulation").
[236] Please see Register of the European Data Protection Officer, European Commission, in particular http:/ /ec.europa.eu/dpo-register/details.htm?id=44448, last accessed on 11 May 2015.

A.8.3. Purposes of processing

The purpose of the processing operations relating to the award, management and follow-up of grants, prizes and financial instruments is to ensure, among other goals, that: proposals are evaluated against the announced criteria in a transparent and effective manner; the best proposals are selected for funding; the ensuing grant agreements are concluded and implemented according to the contractual provisions and in conformity with sound financial management of the EU budget.

The purpose of the processing operations regarding the registration, selection and management of independent experts by DG MOVE is to select and manage (including reimbursements of expenses and payment where appropriate).

In both examples, the purpose of the processing of personal data is carried out in the performance of public interest tasks that DG MOVE is charged with, in accordance with Article 5 of Regulation (EC) 45/2001.[237]

A.8.4. Entities involved

In the context of both examples given above, the controller of the processed data is the Head of the Innovation and Research Unit within DG MOVE. Also, with regard to both examples, the personal data collected is exchanged with: EU institutions and bodies; Member States; third parties in the European Economic Area (EEA) and in countries for which the Commission has adopted an adequacy decision; third parties in countries with no adequacy decision, with additional safeguards; the public.

A.8.5. Legal basis

The legal basis for the processing of personal data by DG MOVE in the contexts previously described is Article 5 of Regulation (EC) 45/2001. The processing is therefore lawful due to either of the following reasons: it is necessary for the performance of public interest tasks, namely the management of Horizon 2020 and other related Programmes and Initiatives managed by DG MOVE; it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; the data subject has given unambiguous prior-consent.

The data processed in the two cases at hand fall under Article 27 of Regulation (EC) 45/2001 and have, subsequently, been prior-checked by the European Data Protection Supervisor.

A.8.6. Cooperation with third countries

In line with Regulation (EC) 45/2001, the personal data collected by DG MOVE in the context of the two activities specified *supra* might be transferred to recipients other than Community institutions and bodies: i) which are subject to Directive 95/46/EC,[238] provided they establish that the data are necessary for the performance of a tasks carried out in the public interest or subject to the exercise of public authority or if they establish the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced; ii) which are not subject to Directive

[237] Regulation (EC) 45/2001, O.J. 2001, L 008, ("Processing of Personal Data by Community Institutions Regulation").

[238] Directive 95/46/EC, O.J. 1995, L 281/31 ("Processing and Free Movement of Personal Data Directive"). Please note that, in the context of the comprehensive reform of the EU's legal framework for data protection, Regulation 45/2001 will soon be replaced by a Regulation "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data", proposed by the European Commission in January 2017 (https://eur-lex.europa.eu/procedure/EN/2017_2). The aim of the latter is to align the current legislation with the General Data Protection Regulation (GDPR) that has been fully applicable since 25 May 2018. For more information please see http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608754/EPRS_BRI(2017)608754_EN.pdf (April 2018) , last accessed 18 May 2018.

95/46/EC provided that the conditions set out in Article 9 (1),(2),(6) and (7) of Regulation (EC) 45/2001 are met.

Article 9(1): "Personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out."

Article 9(2): The adequacy of the level of protection afforded by the third country or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the rules of law, both general and sectoral, in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation."

Article 9(6): "By way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if: (a) the data subject has given his or her consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract entered into in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which, according to Community law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in Community law for consultation are fulfilled in the particular case."

Article 9(7): "Without prejudice to paragraph 6, the European Data Protection Supervisor may authorise a transfer or a set of transfers of personal data to a third country or international organisation which does not ensure an adequate level of protection within the meaning of paragraphs 1 and 2, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses."

A.8.7. Actual examples

The two examples used throughout this report, i.e. the award and management of grants and the registration, selection and management of independent experts, are two instances where DG MOVE might cooperate with third countries through the exchange of personal data.

A.9. European Anti-Fraud Office (OLAF)

A.9.1. Brief introduction to the Department / Agency

The European Anti-Fraud Office (hereinafter referred to as "the OLAF"), was established in 1999 by European Commission Decision 1999/352/EC of 28 April 1999 establishing the European Anti-Fraud Office (hereinafter referred to as "OLAF Decision").[239] It was designed to detect, investigate and stop fraud with EU funds financing a wide range of projects and programmes through the EU budget.

The OLAF fulfils its mission by: carrying out independent investigations into fraud and corruption involving EU funds in view of ensuring that all EU taxpayers' money reaches projects that can create jobs and growth in Europe; contributing to strengthening citizens' trust in the EU institutions by investigating serious misconduct of EU staff and members of the EU institutions; developing a sound EU anti-fraud policy.

The OLAF can therefore investigate matters relating to fraud, corruption and other offences affecting the EU financial interests concerning: all EU expenditure (the main spending categories are Structural Funds, agricultural policy and rural development funds, direct expenditure and external aid; some areas of EU revenue, mainly customs duties; suspicions of serious misconduct by EU staff and members of the EU institutions.

The legal basis for the establishment of the OLAF is Article 162 of the Treaty establishing the European Community (EC Treaty) – today Article 178 of the Treaty on the Functioning of the European Union (TFEU). The former envisaged that the Council could adopt Implementing Decisions relating to the European Regional Development Fund. The latter foresees Implementing Regulations instead of Implementing Decisions and the role of the European Parliament as co-legislator following the ordinary legislative procedure. In addition, the legal basis for the fight against fraud is Article 325 TFEU (former Article 280 of the EC Treaty).

A.9.2. Nature of personal data

The OLAF conducts administrative investigations internally – concerning EU institutions and bodies – and externally – concerning operators located in the Member States and third countries. It is the only service of the European Commission that has appointed its own Data Protection Officer (DPO). Its daily work therefore involves the processing of large amounts of sensitive personal data.

Recital 6 of Regulation (EU) 883/2013 concerning investigations conducted by the OLAF (hereinafter referred to as "OLAF investigations Regulation")[240] clarifies that the OLAF's responsibility as set up by the European Commission extends beyond the protection financial interests and subsequently includes all activities relating to safeguarding the Union interests against irregular conduct liable to result in administrative or criminal proceedings. Accordingly, recital 29 explains that "where it is found that facts brought to light by the final report on an internal investigation could give rise to criminal proceedings, the information to that effect should be transmitted to the national judicial authorities of the member State concerned." Moreover, in the context of the cooperation between the OLAF, Eurojust, Europol and the competent authorities of the Member States, Recital 34 establishes that the OLAF should inform Eurojust, in particular, of cases of suspected fraud, corruption or any other illegal activity affecting the financial interests of the Union and involving serious forms of criminality.

Recital 35 notes: "For the sake of successful cooperation between the Office, the relevant institutions, bodies, offices and agencies of the Union, the competent authorities of the Member States, the competent authorities in third countries, and international organisations, a mutual exchange of information should be organised. Such exchange of information should respect the principles of confidentiality and the rules on data protection

[239] European Commission Decision 1999/352/EC of 28 April 1999, O.J. 1999, L 136 ("OLAF Decision").
[240] Regulation (EU) 883/2013, O.J. 2013, L 248/1 ("OLAF investigations Regulation").

laid down in Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. In particular, the Office should verify that the recipient has the appropriate competence and that the transmission of information is necessary. Exchanges of information with Eurojust should be covered by Eurojust's mandate, which extends to coordination in transnational cases of serious crime."

Finally, Article 10 of the same Regulation focuses on the confidentiality and data protection of the information transmitted or obtained in the course of both external and internal investigations. Information exchanged or gathered through external investigations, in whatever form, "shall be protected by the relevant provisions", whereas information exchanged or gathered through internal investigations "shall be subject to professional secrecy and shall enjoy the protection afforded by the rules applicable to the Union institutions."

A concrete example of personal data processing by the OLAF is the Customs Information System (SIS). This system, managed by the OLAF, contains details of fraud and irregularities that are potential contraventions of Community law in the area of customs, agriculture and/or national laws. It is part of the Anti-Fraud Information System (AFIS). Some of the items of information to be included in respect of personal data in this regard comprise: name, maiden name, forenames, former surnames and aliases; date and place of birth; nationality; sex; number and place and date of issue of the identity papers (passports, identity cards, driving licenses); address; particular objective and permanent physical characteristics; etc. This data may also be transferred to third countries and international organisations.

A.9.3. Purposes of processing

The OLAF processes personal data in view of the performance of its tasks carried out in the public interest on the basis of European Union law.

In the concrete case of its management of the Customs Information System (CIS), the purpose of the processing and exchanging of personal data by the OLAF is to assist national authorities in preventing, investigating and prosecuting operations which are in breach of customs or agricultural provisions.

A.9.4. Entities involved

The OLAF is the controller of the processed personal data. For each individual case or purpose, a certain staff member its Directorate-General will be the specific controller. With regard to the personal data processed within the Customs Information System (CIS), for instance, the controller is the Head of the Unit responsible for the Customs and Tobacco Anti-Fraud Policy.

The recipients of the processed data may vary depending on the context of the task for which the data is processed but are, normally, the relevant staff from the European Commission, the staff from competent authorities of the Member States and the staff from competent third country authorities. Turning again to the Customs Information System (CIS) example, the recipients of the processed data are the staff from the European Commission and the competent authorities of the Member States responsible for the application of Regulation (EC) 515/97 on mutual assistance between the admirative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, as well as the staff from competent third country authorities.[241]

[241] Regulation (EC) 515/97, O.J. 1997, L 82/1 ("Mutual Assistance and Cooperation on the Correct Application of the Law on Customs and Agricultural Matters Regulation").

A.9.5. Legal basis

As a general rule, the legal basis governing the processing of personal data by the OLAF is Article 5 of Regulation (EC) 45/2001[242] (the processing of personal data is lawful when necessary for the performance of tasks carried out in the public interest).

Regarding the specific example of the OLAF's management of the Customs Information System, the legal basis is also Title V of Regulation (EC) 515/97.

A.9.6. Cooperation with third countries

Article 14 of the OLAF investigations Regulation establishes the following:

"Administrative arrangements may be agreed, as appropriate, by the Office with competent authorities in third countries and with international organisations." These arrangements may concern exchange of operational, strategic or technical information and the OLAF must inform the competent authorities of the Member States concerned before it provides information provided by them to the competent authorities in third countries or to international organisations. Article 14(2) also obliges the OLAF to keep a record of all transmissions of personal data, including the grounds for those transmissions, in accordance with Regulation (EC) 45/2001.

Furthermore, it should be noted that, in the absence of any formal arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations (namely its purpose(s), the criteria for assessing an adequate level of protection in or within the recipient third country or international organisation, the possible derogations and exceptions, etc.) which are not subject to Directive 95/46/EC (now repealed by the General Data Protection Regulation).[243]

A.9.7.. Actual examples

A few recent examples of Administrative Cooperation Arrangements (ACAs) signed between the OLAF and partner authorities in non-EU countries and territories and counterpart administrative investigative services of international organisations[244] are:

- Administrative Cooperation Arrangement between the OLAF and the Australian Customs and Border Protection Service (June 2013);
- Administrative Cooperation Arrangement between the OLAF and the Bureau of Foreign Trade (BOFT) of Taiwan (November 2016);
- Administrative Cooperation Arrangement between the OLAF and the Customs Service of the Republic of Moldova (May 2013);
- Administrative Cooperation Arrangement between the OLAF and the General Administration of China Customs (June 2015);
- Administrative Cooperation Arrangement between the OLAF and the General Finances Inspection Office of Democratic the Republic of Congo (December 2016).

---

[242] Regulation (EC) 45/2001, O.J. 2001, L 008, ("Processing of Personal Data by Community Institutions Regulation"). Please note that, in the context of the comprehensive reform of the EU's legal framework for data protection, Regulation 45/2001 will soon be replaced by a Regulation "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data", proposed by the European Commission in January 2017 (https://eur-lex.europa.eu/procedure/EN/2017_2). The aim of the latter is to align the current legislation with the General Data Protection Regulation (GDPR) has been fully applicable since 25 May 2018. For more information please see http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608754/EPRS_BRI(2017)608754_EN.pdf (April 2018) , last accessed 18 May 2018.

[243] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, repealed is repealed with effect from 25 May 2018.

[244] See current list here: https://ec.europa.eu/anti-fraud/sites/antifraud/files/list_signed_acas_en.pdf, last accessed on 09 May 2018.

These cooperation agreements generally include the following activities: exchange of information, operational assistance, joint or parallel investigations, technical assistance, access to information systems and databases, strategic analysis and training and staff exchange. Exchange of information pursuant to these arrangements consists of providing the other partner, spontaneously or upon request, with information which might be relevant for the other partner in terms of the purpose of each arrangement, in conformity with the rules on confidentiality and data protection. When cooperating on specific cases, partners may exchange any relevant information, including personal data, in order to achieve the purpose of the respective arrangement. Such information should contain sufficient elements to identify: the persons, companies or entities suspected of being involved; the nature of fraud, corruption or other illegal activities; any other relevant circumstances. Regarding data protection, these arrangements will normally entail that all transfers of personal data by the OLAF to the partner and the processing of personal data received from the partner are subject to the requirements of Regulation (EC) 45/2001. As for the transfers of personal data held by the partner to the OLAF and the processing of personal data received from the OLAF by the partner are made in conformity with the contractual data protection clauses annexed to the respective arrangement.[245] These data protection contractual clauses – concerning the rules to be observed when transferring or otherwise processing personal data in the framework of an administrative cooperation agreement - generally determine, among other aspects, that the data processing shall be guided by the following principles: purpose limitation; data quality and proportionality; transparency; security and confidentiality; data subjects' rights of access, rectification, deletion and objection; special protection of special categories of data.[246]

[245] It seems that copies of the aforementioned agreements are not publicly available. Therefore, the information provided as to their content, and that of similar arrangements, is based on a Draft Administrative Cooperation Arrangement, retrieved from https://ec.europa.eu/anti-fraud/sites/ antifraud/ files/ docs/ body/ aca third countries and dp annex en.pdf, last accessed on 09 May 2018.

[246] For further details, see https://ec.europa.eu/anti-fraud/sites/ antifraud/ files/data protection contr actual clauses admin arrangements en.pdf, last accessed 23 May 2015.

A.10. European Securities and Markets Authority (ESMA)

A.10.1. Brief introduction to the Department / Agency

The European Security and Markets Authority (hereinafter referred to as "the ESMA") was established in 2010 by Regulation (EU) 1095/2010 (hereinafter referred to as "ESMA Regulation").[247] It is an independent EU authority that contributes to the stability of the European Union's financial system by enhancing the protection of investors and promoting stable and orderly financial markets.

It achieves its mission by: assessing risks to investors, markets and financial stability; completing a single rulebook for EU financial markets; promoting supervisory convergence; and directly supervising credit rating agencies and trade repositories. It not only fosters supervisory convergence amongst service regulators, but it also aims to do so across financial sectors by working closely with the other European Supervisory Authorities competent in the field of banking (EBA) and insurance and occupational pensions (EIOPA).

The legal basis for the establishment of the ESMA is Article 114 of the Treaty on the Functioning of the European Union (TFEU) which foresees the adoption of "measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market".

A.10.2. Nature of personal data

Article 29(1)(b) of the ESMA Regulation provides that the ESMA shall promote "an effective bilateral and multilateral exchange of information between competent authorities, with full respect for the applicable confidentiality and data protection provisions provided for in the relevant Union legislation".

Article 31(a) provides that the ESMA, while fulfilling a general coordination role between competent authorities (especially in situations where adverse developments could potentially jeopardise the orderly functioning and integrity of the financial markets or the stability of the financial system in the Union), shall equally facilitate the exchange of information between the competent authorities.

Article 35(3) establishes that, upon a duly justified request from a competent authority, the ESMA shall provide any information it has collected that is necessary to carry out its tasks in full compliance with professional secrecy obligations laid down in sectoral legislation and in Article 70 of the same Regulation.

Article 70(2) subsequently determines:

"Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial institutions cannot be identified." It also determines that the ESMA shall nonetheless not be prevented from using the information for the enforcement of the acts it has been mandated to carry out, in particular for legal procedures for the adoption of decisions.

In any case, Article 70(3) clarified that the ESMA is not prevented from exchanging information with national supervisory authorities in accordance with its Regulation and other Union legislation applicable to financial institutions. That information shall be subject to conditions of professional secrecy that the ESMA must implement through internal rules of procedure.

While carrying out its activities, the ESMA makes some e-services available on its website through which it may collect and process personal data, namely: information services that provide users with easy and effective access to information; interactive communication

[247] Regulation (EU) 1095/2010, O.J. 2010, L 331/84, ("ESMA Regulation").

services that allow better contacts with the ESMA's target public; transaction services that allow access to all basic forms of transactions with the ESMA, e.g. procurement, financial operations, recruitment, event enrolment, etc. Personal information may thus be required in order to provide these services.

A concrete example: in the context of its supervision of Credit Rating Agencies, the ESMA (in particular the unit responsible for this area) collects personal data of its staff and of employees of supervised authorities (e.g. education and training details, employment details, financial details). This data may be transferred to third countries or international organisations.

A.10.3. Purposes of processing

The ESMA processes personal data in view of the performance of its tasks carried out in the public interest on the basis of European Union law or in the legitimate exercise of official authority vested in it or in a third party to whom the data are disclosed. In the concrete case of supervision of Credit Rating Agencies, for example, personal data is collected and processed solely in order to enable the respective ESMA staff to carry out its supervision tasks.

A.10.4. Entities involved

The ESMA is the controller of the processed personal data. As a general principle, the ESMA only processes personal data when that is necessary for the performance of its tasks carried out in the public interest on the basis of the Treaty on the Functioning of the European Union (TFEU), on the basis of relevant legislation or in the legitimate exercise of official authority vested in the ESMA or in a third party to whom the data are disclosed. All processing operations are notified to the ESMA's Data Protection Officer and, if necessary, to the European Data Protection Supervisor.

A.10.5. Legal basis

The legal basis for the processing of persona data by the ESMA is Article 5 of Regulation (EC) 45/2001[248] (the processing of personal data is lawful when necessary for the performance of tasks carried out in the public interest) and Article 71 of the EASMA Regulation.

Member States must also comply with their obligations under the General Data Protection Regulation (GDPR) 2016/679 (which has repealed Directive/95/46/EC and has been applicable since 25 May 2018) when processing personal data.[249]

The legal basis for the processing of personal data in the context of the supervision of Credit Rating Agencies is also Regulation (EC) 1060/2009.[250]

A.10.6. Cooperation with third countries

Article 33 of the ESMA Regulation foresees that the ESMA may develop contacts and enter into administrative arrangements with supervisory authorities, international organisations and the administrations of third countries.

[248] Regulation (EC) 45/2001, O.J. 2001, L 008, ("Processing of Personal Data by Community Institutions Regulation"). Please note that, in the context of the comprehensive reform of the EU's legal framework for data protection, Regulation 45/2001 will soon be replaced by a Regulation "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data", proposed by the European Commission in January 2017 (https://eur-lex.europa.eu/procedure/EN/2017_2). The aim of the latter is to align the current legislation with the General Data Protection Regulation (GDPR) has been fully applicable since 25 May 2018. For more information please see http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608754/EPRS_BRI(2017)608754_EN.pdf (April 2018) , last accessed 18 May 2018.

[249] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, is repealed with effect from 25 May 2018.

[250] Regulation (EC) 1060/2009, O.J. 2009, L 302/1 ("Credit Rating Agencies Regulation").

In addition, it should also be noted that, in the absence of any formal arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations which are not subject to Directive 95/46/EC (now repealed by the General Data Protection Regulation).

A.10.7. Actual examples

Pursuant to the abovementioned Article 33, the ESMA has, among others,[251] concluded a Memorandum of Understanding (MoU) on cooperation arrangements to access information on derivatives contracts held in European Union trade repositories with the Australian Securities & Investments Commission (ASIC).[252]

In light of Article 76(1) of Regulation (EU) 648/2012 (on OTC derivatives, central counterparties and trade repositories),[253] relevant authorities of third countries that do not have any trade repository established in their jurisdiction may contact the ESMA with a view to establishing cooperation arrangements to access information on derivatives contracts held in EU trade repositories. Such is the case of Australia.

Article 6 of the Memorandum establishes the following: "Each Authority will process any personal data contained in the information obtained as contemplated by or under this MoU solely for the purpose of fulfilling its responsibilities and mandates as defined in the Laws and Regulations of the Authority and complying with the requirements set out in the data protection laws and regulations applicable in the jurisdiction of the Authority."

Furthermore, Article 4 provides that before using any non-public information for any purposes other than the ones provided for in the Memorandum, the Authority receiving the information must first consult and obtain the written consent of the other Authority for the intended use. Should consent be denied, "the Authorities will consult to discuss the reasons for withholding approval of such use and the circumstances, if any, under which the intended use by the Authority might be allowed".

[251] For further information on other examples of international cooperation please see the list provided by ESMA https://www.esma.europa.eu/databases-library/esma-library?page=1&f[0]=im_esma_sections%3A367, last accessed 23 May 2015.
[252] Memorandum of Understanding on Cooperation Arrangements to access information on derivatives contracts held in European Union trade repositories between the European Security and Markets Authority (EBA) and the Australian Securities & Investments Commission (ASIC), November 2014, retrieved from https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_asic_mou.pdf, last accessed on 08 May 2018.
[253] Regulation (EU) 648/2012, O.J. 2012, L 201/1 ("EMIR Regulation").

A.11. European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)

A.11.1. Brief introduction to the Department / Agency

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) was established by Regulation (EU) No 1077/2011 of the European Parliament and of the Council,[254] having regard to the Treaty on the Functioning of the European Union.

The core function of the eu-LISA is to fulfil the operational management tasks for the Schengen Information System (SIS II), the Visa Information System (VIS) and Eurodac and, if so decided, other large-scale IT systems in the area of freedom, security and justice. EU-LISA is also responsible for technical measures required by the tasks entrusted to it, which are not of a normative nature. Those responsibilities should be without prejudice to the normative tasks reserved to the Commission alone or to the Commission assisted by a Committee in the respective legislative instruments governing the systems operationally managed by the Agency.[255]

In addition, it should perform tasks relating to training on the technical use of SIS II, VIS and Eurodac and other large-scale IT systems which might be entrusted to it in the future.[256]

A.11.2. Nature of personal data

By operating Eurodac, eu-LISA collects and processes the digitised fingerprints of asylum seekers. Eurodac allows national authorities to share and exchange information. The UK currently uses this system.

By operating SIS II, eu-LISA allows information exchanges between national border control, customs and police authorities ensuring that the free movement of people within the EU can take place in a safe environment. It also contains alerts on missing persons, in particular children, as well as information on certain property, such as banknotes, cars, vans, firearms and identity documents that may have been stolen, misappropriated or lost. It should be noted that the UK does not currently use this system.

In operating VIS, eu-LISA processes data and decisions relating to applications for short-stay visas to visit, or to transit through, the Schengen Area. The system can perform biometric matching, primarily of fingerprints, for identification and verification purposes. It should be noted that the UK does not currently use this system.

A.11.3. Purposes of processing

EU-LISA mostly processes personal data in pursuit of the three above-mentioned tasks – operating Eurodac, SIS II and VIS.

[254] Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
[255] Ibid., Recital 10.
[256] Ibid., Recital 11.

A.11.4. Entities involved

a) Regarding VIS:[257]
   - eu-LISA;
   - Member State visa authorities;
   - Competent asylum authorities of the Member States; and
   - Third countries, pursuant to Art 31(2) of Regulation 767/2008.

b) Regarding Eurodac:[258]
   - eu-LISA;
   - Europol;
   - Member State National Access Points;
   - Designated authorities of the Member States; and
   - Verifying authorities of the Member States.

c) Regarding SIS II:[259]
   - eu-LISA;
   - Designated authorities (N.SIS II Offices) of the Member States; and
   - Competent authorities of Member States.

A.11.5. Legal basis

Eu-LISA processes personal data in accordance with the provisions of Regulation 45/2001[260], and the Decision of the Management Board of eu-LISA in relation thereto.[261] In relation to the principle tasks set out above which require the processing of personal data, Article 5(a) of Regulation 45/2001 provides that eu-LISA may process personal data lawfully if the processing is necessary for the performance of a task carried out in the public

[257] See REGULATION (EC) No 767/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008. Concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).
[258] See Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.
[259] See Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).
[260] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Please note that, in the context of the comprehensive reform of the EU's legal framework for data protection, Regulation 45/2001 will soon be replaced by a Regulation "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data", proposed by the European Commission in January 2017 (https://eur-lex.europa.eu/procedure/EN/2017_2). The aim is to align the Regulation with the General Data Protection Regulation (GDPR) that has been fully applicable since 25 May 2018. For more information please see http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608754/EPRS_BRI(2017)608754_EN.pdf (April 2018) last accessed 18 May 2018.
[261] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice - Decision of the Management Board on implementing rules relating to Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed. Article 5(b) provides that processing is lawful if it is necessary for compliance with a legal obligation to which eu-LISA is subject.

Thus, the processing of personal data which is required by the various legal provisions establishing the VIS, SIS II and Eurodac and those providing that eu-LISA is responsible for the operational management thereof would be lawful within the meaning of Article 5(a) of Regulation 45/2001.[262]

In addition, without prejudice to the general provisions regarding lawfulness of processing, Article 7 of Regulation 45/2001 provides the conditions for transfer of personal data from eu-LISA to other EU institutions and bodies, Article 8 governs the transfer of personal data between eu-LISA and a recipient other than a community institution or body which is subject to the GDPR, while Article 9 applies to the transfer of personal data between eu-LISA and recipients, other than community institutions and bodies, which are not subject to GDPR. Article 10 contains the rules on processing of special categories of personal data by eu-LISA.

A.11.6. Cooperation with third countries

Article 37 of Regulation 1077/2011 provides:

"Under the relevant provisions of their association agreements, arrangements shall be made in order to specify, inter alia, the nature and extent of, and the detailed rules for, the participation by countries associated with the implementation, application and development of the Schengen acquis and Eurodac-related measures in the work of the Agency, including provisions on financial contributions, staff and voting rights."

Should the UK wish to continue using the Eurodac facility, this continued involvement could be specified in whatever agreement it enters into with the EU post-Brexit. In such circumstances, eu-LISA could rely on Article 5(a) of Regulation 45/2001 for processing of personal data.

Regulation 1077/2011 does not make provision for the involvement of third countries in the management and operation of eu-LISA. Furthermore, the possibilities for sharing personal data with third countries are quite limited. Article 54 of Council Decision 2007/533/JHA states that data processed in SIS II pursuant to the Decision shall not be transferred or made available to third countries or international organisations. Article 55 notes that this is subject to derogation in relation to an agreement entered between the European Union and Interpol.

In relation to VIS, Article 31(1) of Regulation 767/2008 contains a similar prohibition on sharing information with third countries or international organisations, while Article 31(2) contains a derogation allowing the following data to be transferred to a third country in certain individual cases:

- Surname; surname at birth; first name(s); sex; date, place and country of birth;
- Current nationality and nationality at birth;
- Type and number of the travel document, the authority which issued it and the date of issue and expiry;
- Residence;
- In the case of minors, surname and first name(s) of applicant's father and mother.

In relation to Eurodac, Article 35 of Regulation 603/3013 prohibits transfers of personal data to third countries or international organisations, without prejudice of the rights of

[262] Provided, of course that the other relevant provisions of the Regulation are adhered to.

Member States to transfer personal data to countries to which Regulation 604/2013[263] applies.

Thus, in the absence of the UK executing some kind of association agreement, it would be difficult to maintain transfers of personal data between eu-LISA and the UK. This would have an impact on Eurodac, in particular, as the UK currently participates in that programme.

A.11.7. Actual examples

Associated countries (Norway, Iceland, Switzerland and Liechtenstein) participate in eu-LISA. As regards SIS II and VIS, Regulation 1077/2011 is a development of the provisions of the Schengen acquis, within the meaning of their Agreement with the European Union. Meanwhile, as regards Eurodac, it constitutes a new measure, so it applies subject to their decision to implement it in their internal legal order, which they have. Such countries have the right to participate in the Management Board of eu-LISA.

[263] Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person.

A.12. Directorate-General for Health and Food Safety (DG SANTE)

A.12.1. Brief introduction to the Department / Agency

The Directorate-General for Health and Food Safety of the European Commission (hereinafter referred to as "DG SANTE") has the mission to: improve human health; support the modernisation of Europe's health systems; ensure that all food, feed and medical products marketed in the EU are safe and that EU standards are promoted globally; protect animal health and welfare and plant health; contribute to a well-functioning and fair internal market in food, feed, agricultural and medical products. DG SANTE therefore proposes legislation and supports projects within the sectors it is responsible for. It oversees the following bodies/agencies: the European Food Safety Authority (EFSA), the European Medicines Agency (EMA), the European Centre for Disease Prevention and Control (ECDC), the Community Plant Variety Office (CPVO), the Consumers, Health, Agriculture and Food Executive Agency (CHAFEA) and the European Chemicals Agency (ECHA).

The legal bases for the operation of DG SANTE's activities are Articles 114 (internal market), 168 (public health) and 13 (animal welfare) of the Treaty on the Functioning of the European Union (TFEU).[264]

A.12.2. Nature of personal data

As an EU body, there are different circumstances under which DG SANTE might process (and exchange) personal data. Three examples have been selected and are presented below:

a) Personal data (e.g. contact details of staff and inspectors involved) are processed in the Rapid Alert System for Food and Feed (RASFF), a tool for exchange of information between food and feed central competent authorities in the members of the network (EU 28 Member States, EFTA/EEA countries – Norway, Iceland and Liechtenstein -, Switzerland, the Commission, the European Food Safety Authority and the EFTA Surveillance Authority) in cases where a direct or indirect risk to human health deriving from food or feed has been identified and measures have been taken;[265]

b) Personal data (e.g. contact details of staff, auditors, other system users and third parties) are processed in "MisDoc", a complete and secure IT system for the management and planning of audit missions carried out by Commission experts both in EU Member States and third countries, for the management and storage of reports and associated documents and for the follow-up recommendations;[266]

c) Personal data (name, address, e-mail, country, etc. of both users and non-users) are processed in the Plant Protection Products Application Management System (PPPAMS), which includes an "administrative" system accessible by authorised users (where some of them can create and consult applications for plant protection products, for instance, while others can search and consult public information on authorised plant protection products) and a web portal for the general public; in other words, the system permits the exchange of information between applicants (industry and their consultants), competent authorities of the Member States, the Commission and the European Food Safety Authority (EFSA), thus also facilitating

[264] Please see DG SANTE's mission statement and 2016-2020 Strategic Plan here: https:// ec. europa. eu/ info/ departments/health-and-food-safety_en, last accessed 24 May 2018.
[265] Please see Register of the European Data Protection Officer, European Commission, in particular http://ec.europa.eu/dpo-register/details.htm?id=41467, last accessed on 25 May 2015.
[266] Please see Register of the European Data Protection Officer, European Commission, in particular http://ec.europa.eu/dpo-register/details.htm?id=43436, last accessed on 25 May 2015.

the tracking and following-up of applications for authorisation of plant protection products.[267]

A.12.3. Purposes of processing

The purpose(s) of the processing of personal data in the context of the three examples given above is the following:

a) To provide the control authorities with an effective tool for a rapid exchange of information on the products posing a direct or indirect risk to human health deriving from food or feed on the European market; to allow members of the network to immediately identify whether they are affected by a problem, take the appropriate measures, prevent supply of dangerous products or where necessary withdrawing or recalling them from the consumers, thereby ensuring coherent and simultaneous actions and consumer safety;

b) To support the implementation of the Food and Veterinary Office (FVO) audit programme in the verification of the compliance and equivalence with community legislation on feed and food, animal health and animal welfare; the system monitors the audit workflow and stores the information relevant to the audit, including the audit report and supporting documents;

c) To allow for the identification of the industry users or other applicants (e.g. consultants, farmers) applying for the authorisation of a plant protection product; it also allows the identification of the different stakeholders (national competent authorities, Commission, industry and the users from the European Food Safety Authority (EFSA), who only have viewing rights, i.e. their user actions are not relevant or logged) at the various stages of the assessment and authorisation; this information is necessary for the follow-up of the applications for authorisation of plant protection products.

A.12.4. Entities involved

The entities involved in the processing of personal data in the context of the three examples given above are the following:

a) The controller of the processed data is the competent Head of Unit (Alerts, Traceability and Committees); the users who have access to the personal data in the Rapid Alert System for Food and Feed (RASFF) are the different contact points involved: i) from the competent authorities in Member States and EFTA/EEA countries, Switzerland, the Commission, EFSA (European Food Safety Authority) and the EFTA Surveillance Authority; ii) from the Border Inspection Posts; iii) from the competent authorities in third countries - these contact points only have access to notifications concerning their own countries;

b) The controller of the processed data is the competent Head of Unit (Health and food audits and analysis); the recipients of the processed data are third parties (via electronic communication from the Food and Veterinary Office staff and Director), system users, system administrators and the staff responsible for the helpdesk;

c) The controller of the processed data is the competent Head of Unit (Pesticides and Biocides); the recipients of the personal data from the system are the users from the national competent authorities, the European Food Safety Authority (EFSA) and the Commission, industry organisations and their consultants, applicants and the general public.

[267] Please see Register of the European Data Protection Officer, European Commission, in particular http:// ec. eu

A.12.5 Legal basis

The processing of personal data in the context of the three examples given above is lawful and necessary by virtue of Article 5 of Regulation (EC) 45/2001.[268] In addition, other specific legal bases for each of the aforementioned examples can be found in, respectively:

a) Regulation (EC) 178/2002 (Article 50) and Regulation (EU) 16/2011;[269]

b) Regulation (EC) 882/2004 (Articles 45 and 46) and Directive 2000/29/EC (Articles 21 and 27a);[270]

c) Regulation (EC) 1107/2009 (Articles 53 and 57 and Chapter 3 of Section 1).[271]

A.12.6. Cooperation with third countries

In general, in the absence of any formal agreements or arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations (namely its purpose(s), the criteria for assessing an adequate level of protection in or within the recipient third country or international organisation, the possible derogations and exceptions, etc.) which are not subject to Directive 95/46/EC (now repealed by the General Data Protection Regulation).[272]

A.12.7. Actual examples

The examples given throughout this report are also actual examples of activities due to which DG SANTE may exchange personal data with third countries:

a) In the context of the Rapid Alert System for Food and Feed (RASFF), the transfer of personal data to contact points in third countries is necessary and legally required on important public interest grounds, in accordance with Article 9(6)(d) of Regulation (EC) 45/2001 and Article 10 Regulation (EU) 16/2011 ("Rapid alert system for food and feed Regulation"); the latter provision regulates the exchange of information with third countries;

b) In the context of the "MisDoc" IT system for the management and planning of audit missions carried out by the Commission experts, it might be necessary, for logistical reasons related to the organisation of an upcoming Commission audit mission to a third country, to pass the personal contact data of a national expert to the competent authority of the third country concerned; the exchange of personal data will not occur, however, unless express consent has been given by the national expert;

c) In the context of the Plant Protection Products Application Management System (PPPAMS), users from competent authorities of third countries might be given

ro pa.eu/dpo-register/details.htm?id=44727, last accessed on 25 May 2015.

[268] Regulation (EC) 45/2001, O.J. 2001, L 008, ("Processing of Personal Data by Community Institutions Regulation"). Please note that, in the context of the comprehensive reform of the EU's legal framework for data protection, Regulation 45/2001 will soon be replaced by a Regulation "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data", proposed by the European Commission in January 2017 (https://eur-lex.europa.eu/procedure/EN/2017_2). The aim of the latter is to align the current legislation with the General Data Protection Regulation (GDPR) that has been fully applicable since 25 May 2018. For more information please see http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608754/EPRS_BRI(2017)608754_EN.pdf (April 2018), last accessed 18 May 2018.

[269] Regulation (EC) 178/2002, O.J. 2002, L 31/1 ("European Food Safety Authority Regulation") and Regulation (EU) 16/2011, O.J. 2011, L 6/7 ("Rapid alert system for food and feed Regulation").

[270] Regulation (EC) 882/2004, O.J. 2004, L 165/1 ("Official Controls for Compliance with Feed and Food Law, Animal Health and Animal Welfare Rules Regulation") and Directive 2000/29/EC, O.J. 2000, L 169/1 ("Protection of Plants Directive").

[271] Regulation (EC) 1107/2009, O.J. 2009, L 309/1 ("Plant Protection Products Regulation").

access; such is currently the case for Norway and Switzerland and there is, furthermore, a future possibility of access being granted to users from competent authorities in Iceland and Liechtenstein; the access rights granted to users from competent authorities from Switzerland, for example, are given under Article 9(1) and (2) of Regulation (EC) 45/2001 and the respective Commission Decision concluding that there is an adequate protection of personal data provided in Switzerland.[273]

[272] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, is repealed with effect from 25 May 2018.
[273] Commission Decision 2000/518/EC, O.J. 2000, L 215/1.

A.13. European Banking Authority

A.13.1. Brief introduction to the Department / Agency

The European Banking Authority (hereinafter referred to as "the EBA") was established on 1 January 2011 by Regulation (EU) 1093/2010 (hereinafter referred to as "EBA Regulation").[274] It is an independent EU Authority working to ensure effective and consistent prudential regulation and supervision across the European banking sector.

Its objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector. The main task of the EBA is to contribute to the creation of the European Single Rulebook in banking whose objective is to provide a single set of harmonised prudential rules for financial institutions throughout the EU. It also plays an important role in promoting convergence of supervisory practices and has the mandate to assess risks and vulnerabilities in the EU banking sector.

As a specialised EU agency set up by the European Parliament and the Council of the European Union to carry out specific legal, technical or scientific tasks, the EBA works alongside the main EU institutions and provides them with evidence-based advice to help them shape informed policies and laws at EU and national level.

The legal basis for the establishment of the EBA is Article 114 of the Treaty on the Functioning of the European Union (TFEU) which envisages the adoption of "measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market".

A.13.2. Nature of personal data

Article 29(1)(b) of the EBA Regulation envisages that the EBA shall promote "an effective bilateral and multilateral exchange of information between competent authorities, with full respect for the applicable confidentiality and data protection provisions provided for in the relevant Union legislation".

Article 31(a) provides that the EBA, while fulfilling a general coordination role between competent authorities (in particular in situations where adverse developments could potentially jeopardise the orderly functioning and integrity of the financial markets or the stability of the financial system in the Union), shall equally facilitate the exchange of information between the competent authorities.

Article 35(3) establishes that, upon a duly justified request from a competent authority, the EBA shall provide any information it has collected that is necessary to carry out its tasks in full compliance with professional secrecy obligations laid down in sectoral legislation and in Article 70 of the same Regulation.

Article 70(2) subsequently determines:

"Without prejudice to cases covered by criminal law, any confidential information received by persons referred to in paragraph 1 whilst performing their duties may not be divulged to any person or authority whatsoever, except in summary or aggregate form, such that individual financial institutions cannot be identified." It also determines that the EBA shall nonetheless not be prevented from using the information for the enforcement of the acts it has been mandated to carry out, in particular for legal procedures for the adoption of decisions.

In any case, Article 70(3) clarified that the EBA is not prevented from exchanging information with national supervisory authorities in accordance with its Regulation and other Union legislation applicable to financial institutions. That information shall be subject to conditions of professional secrecy that the EBA must implement through internal rules of procedure.

[274] Regulation (EU) 1093/2010, O.J. 2010, L 331/12, ("EBA Regulation").

While carrying out its activities, the EBA makes some e-services available on its website through which it may collect and process personal data, namely: information services that provide users with easy and effective access to information; interactive communication services that allow better contacts with the EBA's target public; transaction services that allow access to all basic forms of transactions with the EBA, e.g. procurement, financial operations, recruitment, event enrolment, etc. Personal information may thus be required in order to provide these services.

A concrete example: if, for instance, a consumer wishes to file a complaint against a credit or financial institution with the EBA, the following personal data will be collected: first and last name, telephone/fax, full address and email.

A.13.3. Purposes of processing

The EBA processes personal data in view of the performance of its tasks carried out in the public interest on the basis of European Union law or in the legitimate exercise of official authority vested in it or in a third party to whom the data are disclosed. In the concrete case of consumer complaints, for example, personal data is collected and processed solely in order to enable the EBA's complaint investigation team to deal with the complaint and to follow-up when necessary.

A.13.4. Entities involved

The EBA is the controller of the processed personal data. In general, the EBA will not disclose information to third parties unless that is necessary for the performance of its tasks carried out in the public interest on the basis of the Treaty on the Functioning of the European Union (TFEU), on the basis of relevant legislation or in the legitimate exercise of official authority vested in the EBA or in a third party to whom the data are disclosed.

All processing operations are notified to the EBA's Data Protection Officer and, if necessary, to the European Data Protection Supervisor.

A.13.5. Legal basis

The legal basis for the processing of personal data by the EBA is Article 5 of Regulation (EC) 45/2001[275] (the processing of personal data is lawful when necessary for the performance of tasks carried out in the public interest) and Article 71 of the EBA Regulation.

Member States must also comply with their obligations under the General Data Protection Regulation (GDPR) 2016/679 (which has repealed Directive/95/46/EC and has been applicable since 25 May 2018) when processing personal data.[276]

A.13.6. A Cooperation with third countries

Article 33 of the EBA Regulation foresees that the EBA may develop contacts and enter into administrative arrangements with supervisory authorities, international organisations and the administrations of third countries.

Additionally, it should also be noted that, in the absence of any formal arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of

[275] Regulation (EC) 45/2001, O.J. 2001, L 008, ("Processing of Personal Data by Community Institutions Regulation"). Please note that, in the context of the comprehensive reform of the EU's legal framework for data protection, Regulation 45/2001 will soon be replaced by a Regulation "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data", proposed by the European Commission in January 2017 (https://eur-lex.europa.eu/procedure/EN/2017_2). The aim of the latter is to align the current legislation with the General Data Protection Regulation (GDPR) has been fully applicable since 25 May 2018. For more information please see http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608754/EPRS_BRI(2017)608754_EN.pdf (April 2018) , last accessed 18 May 2018.

[276] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, is repealed with effect from 25 May 2018.

Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations which are not subject to Directive 95/46/EC (repealed by the General Data Protection Regulation).

A.13.7. Actual examples

Apart from the EBA Regulation, the EBA also carries out its activities, *inter alia*, within the scope of the Capital Requirements Directive.[277] Pursuant to Article 55 this Directive, the Authority and EU Member States may conclude cooperation agreements providing for exchanges of information with the supervisory authorities of third countries or with authorities or bodies of third countries. Such information may only be disclosed if it is subject to a guarantee that professional secrecy requirements (at least equivalent to those referred to in the Directive) are complied with. The purpose of the exchange of information is to perform the supervisory tasks of those authorities and bodies. Furthermore, "where information originates in another Member State, it shall only be disclosed with the express agreement of the authorities which have disclosed it and, where appropriate, solely for the purposes for which those authorities gave their agreement". Moreover, Article 62 of the Directive determines that the processing of personal data shall be carried out in accordance with Directive/95/46/EC – now repealed by the General Data Protection Regulation -[278] and Regulation (EC) 45/2001.

Another concrete example in this context is the framework cooperation arrangement between the EBA and the authorities of the United States of America.[279] This framework arrangement provides a basis for subsequent cooperation arrangements on bank crisis management and resolution between any of the EU Supervisory or Resolution Authorities and any of the participating US Agencies. It therefore seeks to promote resolution planning and cooperation for cross-border institutions.

According to Article 2.15 of the framework cooperation arrangement, any future cooperation arrangements that may provide for the sharing of confidential information must ensure its proper handling and protection by: i) addressing the sharing and protection of confidential information under conditions that are satisfactory to each participating Authority; ii) ensuring the confidentiality provisions of any agreement will continue to apply to all confidential information in the possession of each participating Authority even if the latter ceases to be a party to the cooperation arrangement or the said arrangement is terminated for whatever reason.

[277] Directive 2013/36/EU, O.J. 2013, L 176/338 ("CRD IV or Capital Requirements Directive").
[278] See Article 94 of Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation").
[279] Framework Cooperation Arrangement between the European Banking Authority ("EBA") and the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the U.S. Securities and Exchange Commission, and the New York State Department of Financial Services, September 2017, retrieved from https:// www. eba. europa. eu /do cu me nts/10180/1762986/Framework+Agreement+-+EBA-US+agencies+-+September+2017.pdf, last accessed on 07 May 2018.

A.14. Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA)

A.14.1. Brief introduction to the Department / Agency

The Directorate-General for Financial Stability, Financial Services and Capital Markets Union (hereinafter referred to as "DG FISMA"),[280] which came into existence in 2015, is responsible for initiating and implementing policies relating to the EU's financial sector. It has the mission to monitor the effectiveness of the reforms to secure financial stability and improve the supervision of financial markets put forward by the EU after the financial crisis. Its mission is also to ensure that EU legislation is fully implemented and responds to emerging financial risks.

More concretely, DG FISMA's objectives are to: consolidate financial reforms while adapting them to changed circumstances if needed, and ensuring that EU legislation is properly enforced; present new initiatives to close remaining gaps and ensure that financial markets are well regulated and supervised; initiate policies that contribute to investment, growth and jobs in the EU by enhancing the long-term financing of the economy; make financial services work better for consumers and retail investors; work closely with international partners to promote consistency in regulation and the implementation of agreed standards and principles.

In general, the legal bases for DG FISMA's establishment and operation are Articles 53 (freedom of establishment), 56 (freedom to provide services), 63 (free movement of capital) and 114 (approximation of laws for the establishment and functioning of the internal market) of the Treaty on the Functioning of the European Union (TFEU).

A.14.2. Nature of personal data

As an EU body, there are different circumstances under which DG FISMA might process (and exchange) personal data. One concrete example of such a circumstance is the consultation activities carried out by DG FISMA. The personal data collected and further processed are data necessary for the participation in the respective consultation: name, surname, e-mail address, phone number, etc.

A.14.3. Purposes of processing

The purpose of the processing of personal data in the context of such a consultation is to receive the views of those concerned by the topics of the "consultations" and to potentially publish them on the internet.

A.14.4. Entities involved

The controller of the processed data is the Head of Unit in charge of the consultation procedure. The recipients are the participants to the consultation and a wider public insofar as some of the personal data may be published on the internet. The data might also be transmitted to the bodies in charge of a monitoring or inspection tasks in accordance with EU law.

A.14.5. Legal basis

The legal basis for the processing of personal data by DG FISMA in the context of consultation procedures is Article 5 of Regulation (EC) 45/2001 (consultations are necessary for the management of the European Commission and for the development of

[280] Please see DG FISMA's mission statement here: https://ec.europa.eu/info/departments/financial-stability-financial-services-and-capital-markets-union/mission-statement-financial-stability-financial-services-and-capital-markets-union_en, last accessed 15 May 2018; you can also consult its 2016-2020 Strategic Plan here https://ec.europa.eu/info/sites/info/files/strategic-plan-2016-2020-dg-fisma_april2016_en.pdf, last accessed 15 May 2018.

new polices and the implementation of related programmes – tasks carried out in the public interest).[281] The processing is therefore lawful.

A.14.6. Cooperation with third countries

In the context of third country equivalence in EU banking legislation, DG FISMA (on behalf of the European Commission) is responsible for carrying out technical assessments of equivalence. These assessments of equivalence involve a close exchange of information with third country competent authorities and usually take the form of an implementing act.[282]

A specific example of an equivalence clause, in this case relating to equivalent treatment of third country reinsurers, can be found in Article 172 of the Solvency II Directive.[283]

Article 172(1): "The Commission shall adopt implementing measures specifying the criteria to assess whether the solvency regime of a third country applied to reinsurance activities of undertakings with their head office in that third country is equivalent to that laid down in Title I."

Article 172(2): "The Commission may, in accordance with regulatory procedure referred to in Article 301(2) and taking into account the criteria adopted in accordance with paragraph 1, decide whether the solvency regime of a third country applied to reinsurance activities of undertakings with their head office in that third country is equivalent to that laid down in Title I."

For the purposes of this report, it should be noted that desk research did not produce any concrete examples of what the exchange of information pursuant to these equivalent assessments might include, namely in terms of personal data. As such, the example given below merely seeks to demonstrate how the European Commission relies on information forwarded by the relevant EU bodies that, in turn, may have been provided or exchanged by the third country authority concerned.

Finally, it should also be noted that, in the absence of any formal arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations (namely its purpose(s), the criteria for assessing an adequate level of protection in or within the recipient third country or international organisation, the possible derogations and exceptions, etc.) which are not subject to Directive 95/46/EC (repealed by the General Data Protection Regulation).[284]

A.14.7. Actual examples

A specific example of an equivalence decision pursuant to the aforementioned provision is the one made in relation to reinsurers from Japan, whereby the latter are to be recognised

[281] Regulation (EC) 45/2001, O.J. 2001, L 008, (Processing of Personal Data by Community Institutions Regulation"). Please note that, in the context of the comprehensive reform of the EU's legal framework for data protection, Regulation 45/2001 will soon be replaced by a Regulation "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and the free movement of such data", proposed by the European Commission in January 2017 (https://eur-lex.europa.eu/procedure/EN/2017_2). The aim is to align the Regulation with the General Data Protection Regulation (GDPR) that has been fully applicable since 25 May 2018. For more information please see http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608754/EPRS_BRI(2017)608754_EN.pdf (April 2018) , last accessed 18 May 2018.

[282] Please see the following European Parliament briefing (July 2017): http:// www .eu roparl. europa.eu/RegData/etudes/BRIE/2016/587369/IPOL_BRI(2016)587369_EN.pdf, last accessed 18 May 2018; also, please see Commission Staff Working Document on EU equivalence decisions in financial services (February 2017): https://ec.europa.eu/info/sites/info/files/eu-equivalence-decisions-assessment-27022017_en.pdf, last ac cessed 18 May 2018.

[283] Directive 2009/138/EC, O.J. 2009, L 335/1 ("Solvency II Directive").

[284] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, is repealed with effect from 25 May 2018.

as equivalent to EU reinsurers.[285] Recital 9 of the Commission Decision notes that the European Commission has based its assessment on information provided by the European Insurance and Occupational Pensions Authority (EIOPA) on the regulatory and supervisory system for reinsurance and insurance undertakings in force in Japan.

Here, a similar equivalence decision could be taken in relation to the United Kingdom post-Brexit, thereby allowing it to access the EU single insurance market on the basis of Article 172 of the Solvency II Directive.[286]

[285] Commission Delegated Decision 2016/310/EU, O.J. 2016, L 58/55 ("Equivalence of the solvency regime for insurance and reinsurance undertakings in force in Japan Delegated Decision").
[286] Please see http://www.europarl.europa.eu/ RegData/etudes/IDAN/2016/ 595334/IPOL_IDA(2016)595334_EN .pdf, p. 25, last accessed 18 May 2018.

A.15. Directorate-General for Trade (DG Trade)

A.15.1. Brief introduction to the Department / Agency

DG Trade is in charge of developing and implementing the common trade policy of the European Union in accordance with the objectives set out in Article 207 of the Treaty on the Functioning of the EU. The common commercial policy as it is referred to in the Treaty is one of the exclusive competences of the European Union given to the European Commission in accordance with article 3(e) of the TFEU.[287]

In order to fulfil its mission, DG Trade has two related, but distinct, operational activities: trade policy and trade defence; and is organised into eight directorates.[288] The Director General is supported in managing operations by two Deputy Directors Generals, who bear overall responsibility for Directorates B, C and D; and E, F, G and H respectively. Operational activities are supported by the Policy Coordination, Information and Resources Directorate (A); reporting directly to the Director General.[289] Furthermore, DG Trade's workforce is its most valuable asset covering 740 staff, out of which 200 are placed in 58 of the EU Delegations around the world.[290]

DG Trade is the EU's prime negotiator and guardian of an effectively implemented EU trade policy. DG Trade supports the EU's Trade Commissioner in shaping a trade environment that is good for European citizens, workers, business and consumers and helping world trade and development, thereby boosting competitiveness, jobs and growth in the process.[291] Particularly, as set out in its Strategic Plan 2016-2020, [292] DG Trade pursues the following specific objectives:

- *Specific objective 1 - Trade Negotiations:* A wide coverage of the world's trade through regional, multi-, pluri- and bilateral agreements concluded by the EU, ensuring the best economic conditions and opportunities for consumers, workers, citizens and enterprises, including SMEs, in EU and non-EU countries, particularly in Developing Countries.
- *Specific objective 2 - Effective Implementation*: Effective implementation of the EU's trade and investment policies secured through, *inter alia*, proper monitoring, enforcement and support.
- *Specific objective 3 - Tackling Unfair Trade:* Maintain and improve a transparent, efficient and effective system to combat distortions and unfair trade practices in international trade.
- *Specific objective 4 - A Sustainable Approach to Trade*: Improved sustainable economic, social and environmental conditions for consumers, workers, citizens and businesses in the EU and in non-EU countries, and a special focus on human rights, responsible management of supply chains and good governance.

[287] Strategic Plan 2016-2020, DG Trade, European Commission. Available at: https://e c.europa. eu /info/sites/info/files/trade_sp_2016_2020_revised_en.pdf.
[288] Directorate A - Resources, Information and Policy Coordination; Directorate B - Services and Investment, Intellectual Property and Public Procurement; Directorate C - Asia and Latin America; Directorate D - Sustainable Development; Economic Partnership Agreements-African, Caribbean and Pacific; Agri-food and Fisheries; Directorate E - Neighbouring countries, USA and Canada; Directorate F - WTO, Legal Affairs and Trade in Goods; Directorate G - Trade Strategy and Analysis, Market Access; Directorate H -Trade defence.
[289] 2016 Annual activity report, DG Trade, European Commission. Available at: https://ec.europa. eu/info/ sites/info/files/file_import/aar-trade-2016_en_0.pdf.
[290] Strategic Plan 2016-2020, DG Trade, European Commission. Available at: https:// ec .euro pa. eu /info sites/info/files/trade_sp_2016_2020_revised_en.pdf.
[291] 2016 Annual activity report, DG Trade, European Commission. Available at: https:// ec. euro pa. eu/info /sites/info/files/file_import/aar-trade-2016_en_0.pdf.
[292] Strategic Plan 2016-2020, DG Trade, European Commission. Available at: https:// ec .eur opa. eu/ info/ sites/info/files/trade_sp_2016_2020_revised_en.pdf.

A.15.2. Nature of personal data

DG Trade processes data for the purpose of investigations carried out in the context of Trade Defence Instruments (anti-dumping, anti-subsidy, safeguards).[293] Trade defence instruments allow the European Union to defend its producers against unfair trading practices and against dramatic shifts in trade flows insofar as these are harmful to the Union economy. In the context of the various stages of a TDI investigation (e.g., complaint, pre-initiation standing test, Notice of Initiation, disclosures), companies that are subject to the investigation and other interested parties may submit information relating to identified or identifiable individuals. Examples are name, function and contact details (work and e-mail address, telephone and fax number of an individual). In addition, an investigation file contains sensitive documents for internal use by the relevant case team (the so called "limited file") and documents to which parties including their representatives must have access in the context of the right of defence (the so called "file open for inspection by interested parties"). The file "open for inspection by interested parties" may also contain personal data that are submitted with the consent of the data subjects. No personal data presenting specific risks within the meaning of Article 27 of Regulation 45/2001[294], such that it would require prior checking by the European Data Protection Supervisor (EDPS) is collected.

Moreover, the Hearing Officer for DG Trade processes personal data in order to organise hearings among interested parties participating in trade proceedings, including EU producers, producers in countries outside the EU, EU importers, users and consumers and their associations, State authorities and Commission Services.[295] The personal data processed by the Hearing Officer aims at identifying the persons who participate in the hearing and at hearing their statements and reporting on them. This personal data includes their names, professional contact details and their function in the organisation involved in the trade proceeding and the positions expressed during the hearing.

Finally, DG Trade uses other tools entailing the potential transfer of personal data with third countries.[296] Nevertheless, these tools entail the processing of personal data for purely management purposes, and therefore, they are outside the scope of this research.

A.15.3. Purposes of processing

DG Trade, in the context of Trade defence instruments, processes data for the purpose of investigations.[297] Specifically, the information collected relates to companies and other interested parties that are subject to the investigation.

Regarding the activities of the Hearing Officer for DG Trade,[298] the personal data is processed in order to organise hearings in trade proceedings. The purpose of these hearings is to ensure that the proceedings (i) respect the rights of defence of the interested

[293] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=46548.

[294] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The European Commission adopted a proposal on 10 January 2017 which repeals Regulation (EC) 45/2001 and brings it into line with the GDPR. The proposal is currently under discussion in the European Parliament and the Council of the European Union. The Regulation 45/2001 replacement text should be adopted in time to become applicable at the same time as the GDPR (25th May).

[295] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=40327.

[296] Events Management Tool; Subscription to and management of newsletter for external and internal communication by DG TRADE; Procurement procedures, grant procedures, contract execution, grant implementation and calls for expressions of interest for the selection of experts; etc. For more information: http://ec.europa.eu/dpo-register/search.htm?advancedForm =false&sort=not number& searchPerfo rm ed = true&keyword =&entityName=TRADE& population=on&controllerName =& corporateFlag =on& prior CheckFlag=on& modelsFlag=on.

[297] European Commission, Register of the Data protection Officer. Available at: http://ec.europa.eu/dpo-re gi st er/ details.htm?id=46548.

[298] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-re gis ter /details.htm?id=40327.

parties and (ii) comply with due process rules. The data collected and processed by the Hearing Officer includes information which helps identifying the persons who participate in the hearing. In particular, the Hearing Officer sends an invitation to all participants which contains their names, professional contact details and their function in the organisation involved in the trade proceeding. In addition, a non-confidential summary of the hearing containing the same data and the statements of the parties is attached to the non-confidential files, which are accessible to all interested parties. Finally, the hearings may be recorded and saved in electronic form. The parties participating in the hearing may hear the recordings at the premises of the Commission.

A.15.4. Entities involved

The following entities are involved in the data processing for the purpose of investigations as sub-contractors: case-handlers and staff involved in TDI investigations; Trade Defence Instruments Committee (processor: Head of Unit TRADE.H2); and the Committee on Safeguards and Common Rules for Exports (processor: Head of Unit TRADE.H5). Moreover, the following entities and experts participate in the process as recipients of the information: staff of TRADE TDI Directorate, trade hierarchy, Private Office of the Commissioner, EC officials, national experts and other agents. Finally, the following entities/staff are involved in the process as the data subject: representatives of the companies; other interested parties who are involved in the different stages of an investigation; and the staff in TDI Directorate doing case-handling work. [299]
Regarding the hearings, the data subjects are any individuals who participate in hearings. Normally, data subjects are individuals who represent legal persons (EU producers, producers in countries outside the EU, EU importers, users and consumers and their associations, third countries authorities and the Commission Services). The recipients of the data are the interested parties in the proceeding and Commission services, mainly DG Trade, the Legal Service, DG ENTR and DG TAXUD in accordance with the Commission internal procedures.[300]

A.15.5. Legal basis

The processing of data for the purpose of investigations carried out in the context of Trade Defence Instruments[301] is justified by Article 5a of Regulation 45/2001:[302] "*task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed*". Moreover, as interested parties submit contact details of their representatives in an investigation governed by the relevant Regulation, they are aware that, in line with the provisions contained in the Regulation, the file "*open for inspection by interested parties*" will be made available to other interested parties; therefore, Article 5d of Regulation 45/2001 applies also to the data subject who has unambiguously given his or her consent. Lastly, the following legal provisions are also applicable when processing personal data for the purpose of investigations in the context of Trade Defence:

- Article 207 of the Treaty on the Functioning of the European Union.
- Article 6 (7) and 19 of Regulation (EU) 2016/1036 on protection against dumped imports from countries not members of the European Union.

[299] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=46548
[300] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=40327
[301] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/details.htm?id=46548
[302] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. For more information see footnote 8.

- Article 11 (7) and 29 of Regulation (EU) 2016/1037 on protection against subsidised imports from countries not members of the European Union.
- Articles 5 and 8 of Regulation (EU) 2015/478 of the European Parliament and of the Council of 11 March 2015 on common rules for imports.
- Articles 3 and 5 of Regulation (EU) 2015/755 of the European Parliament and of the Council of 29 April 2015 on common rules for imports from certain third countries.

In relation to the activities of the Hearing Officer for DG Trade,[303] the current hearing officer was nominated by the Commission with effect on 1 January 2014, in accordance with Article 3 of the Decision of the President of the European Commission No C(2012)2 of 29 February 2012 on the function and terms of reference of the hearing officer in certain trade proceedings,[304] with the duty to ensure the best implementation of procedural rights pursuant certain Regulations.[305] In addition, the Hearing Officer processes only personal data necessary to organise, carry out and report on oral hearings in trade proceedings. The oral hearings are part of the rights of defence of interested parties participating in trade proceedings. The right of defence is a fundamental human right. Therefore, the organisation of the hearings, including the processing of personal data to identify the participants, aims at guaranteeing this right and is in the public interest. The legal basis is the Treaties, the secondary legislation regulating trade proceedings and the Decision of the President of the European Commission No C(2012) of 29 February 2012 on the function and terms of reference of the hearing officer in certain trade proceedings. Consequently, the processing of personal data is lawful within the meaning of Article 5(a) of the Data Protection Regulation.

A.15.6. Cooperation with third countries

In relation to protection against dumped imports from countries which are not members of the EU, Article 6 (7) of Regulation 2016/1036 establishes that the complainants, importers and exporters and their representative associations, users and consumer organisations (…) as well as the representatives of the exporting country, may, upon written request, inspect all information made available by any party to an investigation, as distinct from internal documents prepared by the authorities of the Union or its Member States, which is relevant to the presentation of their cases and not confidential (…) Such parties may respond to such information and their comments shall be taken into consideration, wherever they are sufficiently substantiated in the response. Similarly, regarding the protection against subsidised imports from countries which are not members of the EU, Article 11 (7) of Regulation 2016/1037 states that the complainants, the government of the country of origin and/or export, importers and exporters and their representative associations, users and consumer organisations (…) may, upon written request, inspect all information made available to the Commission by any party to an investigation, as distinct from internal documents prepared by the authorities of the Union or its Member States, which is relevant to the presentation of their cases and is not confidential.

Furthermore, in relation to imports from certain third countries and within the context of investigations procedures, Article 3 of Regulation 2015/755 states that "The Commission shall seek all information it deems necessary and, where it considers it appropriate, endeavour to check that information with importers, traders, agents, producers, trade

[303] European Commission, Register of the Data Protection Officer. Available at: http://ec.europa.eu/dpo-register/detai ls.htm?id=40327
[304] OJ L 107, 19.4.2012, p.5.
[305] Regulation (EU) 2016/1036 of the European Parliament and of the Council of 8 June 2016 on protection against dumped imports from countries not members of the European Union; Regulation (EU) 2016/1037 of the European Parliament and of the Council of 8 June 2016 on protection against subsidised imports from countries not members of the European Union; Regulation (EU) 2015/478 of the European Parliament and of the Council of 11 March 2015 on common rules for imports; Regulation (EU) 2015/755 of the European Parliament and of the Council of 29 April 2015 on common rules for imports from certain third countries. For more information: http://ec.europa.eu/dpo-register/details.htm?id=4032.

associations and organisations (…) Interested parties (…) as well as the representatives of the exporting country, may inspect all information made available to the Commission within the framework of the investigation (…). In addition, Article 5 establishes that the Commission and the Member States, including the officials of either, shall not reveal any information of a confidential nature received pursuant to Regulation 2015/755, or any information provided on a confidential basis, without specific permission from the supplier of such information (…) Information shall in any case be considered to be confidential if its disclosure is likely to have a significantly adverse effect upon the supplier or the source of such information.

Finally, it should also be noted that, in the absence of any formal arrangements, personal data may be exchanged by EU institutions and bodies pursuant to Article 9 of Regulation (EC) 45/2001. This provision regulates the transfer of personal data to third countries or international organisations (namely its purpose(s), the criteria for assessing an adequate level of protection in or within the recipient third country or international organisation, the possible derogations and exceptions, etc.) which are not subject to Directive 95/46/EC (repealed by the General Data Protection Regulation).[306]

A.15.7. Actual examples

As an example of the exchange of information for the purpose of investigations, 8 new investigations were initiated in 2017 (excluding re-openings). In 4 of these investigations, the country of origin was P.R. China, and in the other 4 investigations: Egypt, Russia, Turkey and Ukraine.[307] Examples include the anti-dumping proceeding concerning imports of ferro-silicon originating in Egypt and Ukraine[308] and the anti-dumping proceeding concerning imports of Low Carbon Ferro-Chrome originating in the People's Republic of China, Russia and Turkey.[309] Lastly, it should be mentioned that DG Trade is in charge of the EU's common commercial policy and hence conducts trade negotiations with third countries.[310] As an example, the Comprehensive Economic and Trade Agreement (CETA) is a bilateral free trade agreement between the EU and Canada. This agreement also regulates certain exchanges of data. The chapters on financial services, telecommunications, electronic commerce and regulatory co-operation contain special provisions on privacy and data protection, for instance:

> **Article 13.15 Transfer and processing of information**" *1. Each Party shall permit a financial institution or a cross-border financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing if processing is required in the ordinary course of business of the financial institution or the cross-border financial service supplier. 2. Each Party shall maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information. If the transfer of financial information involves personal information, such transfers should be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated*.".[311]

[306] Regulation 2016/679, O.J. 2016, L 119/1 ("GDPR Regulation"); Directive 95/46/EC, O.J. 1995, L 281/31, is repealed with effect from 25 May 2018.

[307] Anti-dumping and anti-subsidy safeguard, statistics covering the first 11 months of 2017, European Commission. Available at: http://trade.ec.europa.eu/doclib/docs/2017/december/tradoc_156415.pdf

[308] Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.C_.2017.251.01.0005.01.ENG

[309] Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2017_.200.01.0017.01.ENG&toc=OJ:C:2017:200:FULL

[310] https://www.ivir.nl/publicaties/download/1807 See also: https://www.institutefor government .org.uk/sites/default/files/publications/IFGJ5896-Brexit-Report-171 214-final.pdf.

[311] It should be mentioned that Chapter 28 Article 3 on "Exceptions" provides for general exceptions that would apply to the relevant chapters on cross-border trade in services, domestic regulations, financial services, telecommunications, electronic commerce and investment.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, examines the available mechanisms for personal data transfers between the EU and the UK after Brexit. The study shows that an adequacy finding for the UK would be beneficial, but insufficient. Notably, and to the extent that there is a consensus on these points, there is a need for a bespoke instrument that establishes a standstill period, and which allows the UK to participate in (i) the development of EU data protection policy, (ii) internal market data transfers, and (iii) security and law enforcement initiatives.

PE 604.976

Print ISBN 978-92-846-3425-5 | doi: 10.2861/252108 | QA-02-18-907-EN-C
PDF ISBN 978-92-846-3424-8 | doi: 10.2861/962634 | QA-02-18-907-EN-N