

Official Journal of the European Union

C 370



English edition

Information and Notices

Volume 62

31 October 2019

Contents

II *Information*

INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

European Commission

2019/C 370/01	Communication from the commission Corresponding values of the thresholds of Directives 2014/23/EU, 2014/24/EU, 2014/25/EU and 2009/81/EC of the European Parliament and of the Council ⁽¹⁾	1
---------------	---	---

IV *Notices*

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

Council

2019/C 370/02	Council Decision of 24 October 2019 on the appointment of a Deputy Executive Director of Europol	4
---------------	---	---

European Commission

2019/C 370/03	Euro exchange rates — 30 October 2019	6
---------------	---	---

2019/C 370/04	Explanatory Notes to the Combined Nomenclature of the European Union	7
---------------	--	---

European External Action Service

2019/C 370/05	Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 1 October 2019 on implementing rules relating to the protection of personal data by the European External Action Service and the application of Regulation (EU) 2018/1725 of the European Parliament and of the Council	9
---------------	---	---

2019/C 370/06	Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 1 October 2019 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the European External Action Service	18
---------------	--	----

EN

⁽¹⁾ Text with EEA relevance.

European Data Protection Supervisor

2019/C 370/07	Summary of the Opinion of the European Data Protection Supervisor on the revision of the EU Regulations on service of documents and taking of evidence in civil or commercial matters (<i>The full text of this Opinion can be found in English, French and German on the EDPS website www.edps.europa.eu</i>)	24
---------------	--	----

NOTICES CONCERNING THE EUROPEAN ECONOMIC AREA

EFTA Surveillance Authority

2019/C 370/08	EFTA Surveillance Authority notice on State aid recovery interest rates and reference/discount rates for the EFTA States applicable as from 1 October 2019 (<i>Published in accordance with the rules on reference and discount rates set out in Part VII of the Authority's State Aid Guidelines and Article 10 of the Authority's Decision No 195/04/COL of 14 July 2004</i>)	28
---------------	---	----

V Announcements

ADMINISTRATIVE PROCEDURES

European Commission

2019/C 370/09	Call for proposals for support for information measures relating to the common agricultural policy (CAP) for 2020	29
---------------	---	----

PROCEDURES RELATING TO THE IMPLEMENTATION OF COMPETITION POLICY

European Commission

2019/C 370/10	Prior notification of a concentration (Case M.9568 — Marcegaglia Plates/Evraz Palini Bertoli) Candidate case for simplified procedure ⁽¹⁾	30
---------------	--	----

OTHER ACTS

European Commission

2019/C 370/11	Publication of a communication of approval of a standard amendment to the product specification for a name in the wine sector referred to in Article 17(2) and (3) of Commission Delegated Regulation (EU) 2019/33	32
---------------	--	----

⁽¹⁾ Text with EEA relevance.

II

(Information)

INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES
AND AGENCIES

EUROPEAN COMMISSION

COMMUNICATION FROM THE COMMISSION

**Corresponding values of the thresholds of Directives 2014/23/EU, 2014/24/EU, 2014/25/EU and
2009/81/EC of the European Parliament and of the Council**

(Text with EEA relevance)

(2019/C 370/01)

The corresponding values in the national currencies other than euros of the thresholds of Directives 2014/23/EU ⁽¹⁾, 2014/24/EU ⁽²⁾, 2014/25/EU ⁽³⁾ and 2009/81/EC ⁽⁴⁾ are the following:

EUR 80 000	BGN	New Bulgarian Lev	156 464
	CZK	Czech Koruna	2 054 080
	DKK	Danish Krone	596 408
	GBP	Pound Sterling	70 778
	HRK	Croatian Kuna	594 576
	HUF	Hungarian Forint	25 484 800
	PLN	New Polish Zloty	341 544
	RON	New Romanian Leu	374 040
	SEK	Swedish Krona	821 512

EUR 139 000	BGN	New Bulgarian Lev	271 856
	CZK	Czech Koruna	3 568 964
	DKK	Danish Krone	1 036 259
	GBP	Pound Sterling	122 976
	HRK	Croatian Kuna	1 033 076
	HUF	Hungarian Forint	44 279 840
	PLN	New Polish Zloty	593 433
	RON	New Romanian Leu	649 895
	SEK	Swedish Krona	1 427 377

⁽¹⁾ OJ L 94, 28.3.2014, p. 1.

⁽²⁾ OJ L 94, 28.3.2014, p. 65.

⁽³⁾ OJ L 94, 28.3.2014, p. 243.

⁽⁴⁾ OJ L 216, 20.8.2009, p. 76.

EUR 214 000	BGN	New Bulgarian Lev	418 541
	CZK	Czech Koruna	5 494 664
	DKK	Danish Krone	1 595 391
	GBP	Pound Sterling	189 330
	HRK	Croatian Kuna	1 590 491
	HUF	Hungarian Forint	68 171 840
	PLN	New Polish Zloty	913 630
	RON	New Romanian Leu	1 000 557
	SEK	Swedish Krona	2 197 545

EUR 428 000	BGN	New Bulgarian Lev	837 082
	CZK	Czech Koruna	10 989 328
	DKK	Danish Krone	3 190 783
	GBP	Pound Sterling	378 660
	HRK	Croatian Kuna	3 180 982
	HUF	Hungarian Forint	136 343 680
	PLN	New Polish Zloty	1 827 260
	RON	New Romanian Leu	2 001 114
	SEK	Swedish Krona	4 395 089

EUR 750 000	BGN	New Bulgarian Lev	1 466 850
	CZK	Czech Koruna	19 257 000
	DKK	Danish Krone	5 591 325
	GBP	Pound Sterling	663 540
	HRK	Croatian Kuna	5 574 150
	HUF	Hungarian Forint	238 920 000
	PLN	New Polish Zloty	3 201 975
	RON	New Romanian Leu	3 506 625
	SEK	Swedish Krona	7 701 675

EUR 1 000 000	BGN	New Bulgarian Lev	1 955 800
	CZK	Czech Koruna	25 676 000
	DKK	Danish Krone	7 455 100
	GBP	Pound Sterling	884 720
	HRK	Croatian Kuna	7 432 200
	HUF	Hungarian Forint	318 560 000

	PLN	New Polish Zloty	4 269 300
	RON	New Romanian Leu	4 675 500
	SEK	Swedish Krona	10 268 900

EUR 5 350 000	BGN	New Bulgarian Lev	10 463 530
	CZK	Czech Koruna	137 366 600
	DKK	Danish Krone	39 884 785
	GBP	Pound Sterling	4 733 252
	HRK	Croatian Kuna	39 762 270
	HUF	Hungarian Forint	1 704 296 000
	PLN	New Polish Zloty	22 840 755
	RON	New Romanian Leu	25 013 925
	SEK	Swedish Krona	54 938 615

IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND
AGENCIES

COUNCIL

COUNCIL DECISION

of 24 October 2019

on the appointment of a Deputy Executive Director of Europol

(2019/C 370/02)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to 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 ⁽¹⁾, and in particular Articles 54 and 55 thereof,

Acting as the authority vested with the power to appoint the Executive Director and Deputy Executive Directors of Europol,

Whereas:

- (1) The term of office of one of the current Deputy Executive Directors of Europol will expire on 31 October 2019. It is therefore necessary to appoint a new Deputy Executive Director of Europol.
- (2) The decision of the Management Board of Europol of 1 May 2017 establishes the rules for the selection, extension of the term of office and removal from office of the Executive Director and Deputy Executive Directors of Europol.
- (3) One of the posts for a Deputy Executive Director of Europol has been deemed to be vacant since 31 January 2019, which is nine months before the end of the term of office of one of the current Deputy Executive Directors of Europol, in accordance with point (a) of Article 3(1) of the decision of the Management Board of Europol of 1 May 2017. A vacancy notice for the post of a Deputy Executive Director of Europol has been published in the *Official Journal of the European Union* on 23 January 2019 ⁽²⁾.
- (4) In accordance with Article 54(2) of Regulation (EU) 2016/794, a shortlist of candidates has been drawn up by a selection committee set up by the Management Board (the 'Selection Committee'). The Selection Committee drew up a duly reasoned report on 8 May 2019.
- (5) On the basis of the report of the Selection Committee and in accordance with Regulation (EU) 2016/794 and the decision of the Management Board of 1 May 2017, the Management Board issued a reasoned opinion on 23 May 2019 on the appointment of a Deputy Executive Director of Europol, in which it proposed a shortlist of three candidates suitable for the post to the Council.
- (6) On 18 July 2019, the Council selected Mr Jürgen EBNER as the next Deputy Executive Director of Europol, and informed the competent committee of the European Parliament about his selection for the purposes of fourth subparagraph of Article 54(2) of Regulation (EU) 2016/794.

⁽¹⁾ OJ L 135, 24.5.2016, p. 53.

⁽²⁾ OJ C 28 A, 23.1.2019, p. 1.

- (7) On 5 September 2019, the selected candidate appeared before the Civil Liberties, Justice and Home Affairs Committee of the European Parliament ('LIBE Committee') and, by a letter dated 18 October 2019, the Council was informed of the opinion adopted by the LIBE Committee in accordance with fourth subparagraph of Article 54(2) of Regulation (EU) 2016/794,

HAS ADOPTED THIS DECISION:

Article 1

Mr Jürgen EBNER is hereby appointed as Deputy Executive Director of Europol for the period from 1 November 2019 to 31 October 2023 at grade AD 14.

Article 2

This Decision shall enter into force on the date of its adoption.

Done at Luxembourg, 24 October 2019.

For the Council
The President
A.-K. PEKONEN

EUROPEAN COMMISSION

Euro exchange rates ⁽¹⁾

30 October 2019

(2019/C 370/03)

1 euro =

Currency			Exchange rate		
Currency			Exchange rate		
USD	US dollar	1,1106	CAD	Canadian dollar	1,4534
JPY	Japanese yen	120,99	HKD	Hong Kong dollar	8,7080
DKK	Danish krone	7,4709	NZD	New Zealand dollar	1,7504
GBP	Pound sterling	0,86200	SGD	Singapore dollar	1,5141
SEK	Swedish krona	10,8010	KRW	South Korean won	1 297,21
CHF	Swiss franc	1,1032	ZAR	South African rand	16,5609
ISK	Iceland króna	138,10	CNY	Chinese yuan renminbi	7,8371
NOK	Norwegian krone	10,2488	HRK	Croatian kuna	7,4606
BGN	Bulgarian lev	1,9558	IDR	Indonesian rupiah	15 600,04
CZK	Czech koruna	25,512	MYR	Malaysian ringgit	4,6423
HUF	Hungarian forint	329,72	PHP	Philippine peso	56,591
PLN	Polish zloty	4,2629	RUB	Russian rouble	70,9556
RON	Romanian leu	4,7577	THB	Thai baht	33,580
TRY	Turkish lira	6,3615	BRL	Brazilian real	4,4611
AUD	Australian dollar	1,6199	MXN	Mexican peso	21,2538
			INR	Indian rupee	78,7705

⁽¹⁾ Source: reference exchange rate published by the ECB.

Explanatory Notes to the Combined Nomenclature of the European Union

(2019/C 370/04)

Pursuant to Article 9(1)(a) of Council Regulation (EEC) No 2658/87 ⁽¹⁾, the Explanatory Notes to the Combined Nomenclature of the European Union ⁽²⁾ are hereby amended as follows:

On page 412:

9503 00 70 Other toys, put up in sets or outfits

The following text is inserted in the 4th paragraph, as a second hyphen (after the text 'chalks,'):

— creativity kits/sets designed for children to make mosaics. They consist of pre-printed cardboard papers/cards and various self-adhesive ornaments to be attached to the cards (for example, small coloured pieces of foam and colourful plastic sequins). They may also contain other small articles, such as a stand. They are designed for the amusement of children and also for developing their colour and shape perception and their fine motor skills.

Examples of products:



⁽¹⁾ Council Regulation (EEC) No 2658/87 of 23 July 1987 on the tariff and statistical nomenclature and on the Common Customs Tariff (OJ L 256, 7.9.1987, p. 1).

⁽²⁾ OJ C 119, 29.3.2019, p. 1.



EUROPEAN EXTERNAL ACTION SERVICE

Decision of the High Representative of the Union for Foreign Affairs and Security Policy

of 1 October 2019

on implementing rules relating to the protection of personal data by the European External Action Service and the application of Regulation (EU) 2018/1725 of the European Parliament and of the Council

(2019/C 370/05)

THE HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY,

Having regard to the Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service ⁽¹⁾ ('the EEAS Council Decision'), and in particular Article 11(3) thereof,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 ⁽²⁾ ('the Regulation'), and in particular Articles 43, 44 and 45 thereof,

Whereas:

- (1) The enhanced accountability of the data controllers established in the Regulation requires the adoption of a new implementing decision replacing the Decision PROC HR(2011) 016 of the High Representative of the Union for Foreign Affairs and Security Policy of 8 December 2011 on the rules regarding data protection in the EEAS.
- (2) The role of the data protection officer and the responsibilities of the data controller within the European External Action Service need to be clearly established and adapted to the requirements of the Regulation,

HAS DECIDED AS FOLLOWS:

SECTION 1

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. In accordance with Article 45(3) of the Regulation, this Decision sets out the tasks, duties and powers of the data protection officer (hereinafter referred to as the 'DPO') within the EEAS.
2. This Decision also further specifies internal procedures and the responsibilities of data controllers and processors as well as the role, tasks and duties of data protection coordinators and correspondents, in particular pursuant to Article 26 and 29 of the Regulation.

Article 2

Definitions

For the purpose of this Decision and without prejudice to the definitions provided by the Regulation:

- (a) 'data controller' shall mean the EEAS or its organisational entities, including EU Delegations that, alone or jointly with others, determine the purposes and means of processing personal data;

⁽¹⁾ OJ L 201, 3.8.2010, p. 30.

⁽²⁾ OJ L 295, 21.11.2018, p. 39.

- (b) 'representative of the data controller' shall mean members of the EEAS management or heads of organisational entities who supervise the data controller entities referred to in point (a) above and who are responsible and accountable for the processing of personal data;
- (c) 'delegated controller' shall mean a service or staff within the data controller organisational entity which is entrusted with managing the personal data processing activity;
- (d) 'joint controllers' shall mean two or more organisational entities who determine together the purposes and means of the processing of personal data, and the roles and responsibilities of the controllers, including their duties in relation to exercising the rights of the data subject, in particular when the EEAS jointly controls the processing with other EU institutions, bodies, agencies, offices, or any other entities;
- (e) 'data protection officer ("DPO")' shall mean the EEAS staff member designated by the EEAS, in accordance with Article 43 of the Regulation, to support, inform and advise the data controllers;
- (f) 'data protection coordinator and correspondent ("DPC")' shall respectively mean EEAS staff members in Headquarters and in EU Delegations, designated to assist their data controllers in data protection matters;
- (g) 'processor' shall mean an entity, inside or outside the EEAS, which processes personal data on behalf of the data controller;
- (h) 'data protection notices' are notices, such as privacy statements, by which the data controller provides information to data subjects under Article 15 and 16 of the Regulation;
- (i) 'EEAS staff' shall mean, in accordance with Article 6 of the EEAS Council Decision, officials and other servants of the EU working for the EEAS, including personnel from the diplomatic services of EU Member States, seconded national experts and trainees.

SECTION 2

THE DATA PROTECTION OFFICER

Article 3

Designation of the data protection officer

1. The Secretary-General of the EEAS shall designate the DPO from the EEAS staff, in accordance with Article 43 of the Regulation, and register him or her with the European Data Protection Supervisor (hereinafter referred to as the 'EDPS').
2. In addition to the requirements of Article 43(3) of the Regulation, the DPO shall have a sound knowledge of the EEAS services, their structure, information systems, administrative rules and procedures. The DPO shall have expertise in data protection, sound judgement and the ability to maintain an impartial and objective stance in accordance with the Staff Regulations.
3. The DPO shall be designated for a term of five years and shall be eligible for reappointment.
4. The DPO may be dismissed from the post only with the consent of the EDPS if he or she no longer fulfils the conditions required for the performance of his or her duties.
5. The DPO shall be administratively attached to the Secretary-General.
6. The DPO contact details shall be published on the EEAS intranet and on the EEAS external website and communicated to the EDPS.

Article 4

Position of the data protection officer

1. The DPO shall act independently and in cooperation with the EDPS. The EEAS shall not issue any instructions to the DPO with regard to the exercise of his or her tasks.
2. The DPO shall not be dismissed or penalised for performing his or her tasks.
3. The DPO shall be informed of all contacts with external parties concerning the application of the Regulation and this Decision, in particular, of any interaction with the EDPS and the members of the DPO network in EU institutions, bodies, offices and agencies.

4. Data subjects may contact the DPO on any issue related to processing of their personal data or the exercise of their rights under the Regulation.

5. The DPO may be consulted by the data controller or by his or her representative, by the Staff Committee and by any staff member on any matter concerning the interpretation or application of the Regulation, without the need for them to go through official channels. No one shall suffer prejudice as a result of bringing a matter to the attention of the DPO.

Article 5

Tasks of the data protection officer

The DPO shall:

- (a) be consulted on all issues which relate to the protection of personal data;
- (b) provide guidance and pro-actively advise EEAS entities and their contractors who carry out personal data processing activities, on how to implement the Regulation and this Decision, including consultation on data breach notifications, impact assessments and the necessity of prior consultation with the EDPS;
- (c) keep regular contact with the data controllers to monitor data protection compliance, and support them in their tasks, in particular to contribute to preparing and publishing data protection notices and replying to the requests from data subjects;
- (d) maintain regular contact with the DPCs of the EEAS Headquarters and EU Delegations and manage the DPC Network within the EEAS;
- (e) raise general data protection awareness, organise trainings and information sessions;
- (f) cooperate with DPOs of other EU institutions, bodies, offices and agencies, in particular by exchanging experience and best practices;
- (g) keep a central register of processing activities carried out by the EEAS based on the records prepared by the data controllers in accordance with Article 31 of the Regulation and making the register publicly available;
- (h) assist in ensuring the representation of the High Representative or the EEAS at international level on all data protection related issues.

Article 6

Powers

In performing his or her tasks the DPO:

- (a) shall have access at all times to the data processed by EEAS entities and their contractors and to all offices, data processing centres and data carriers;
- (b) shall provide his or her opinion to the Appointing Authority prior to any decision is taken on matters relating to the application of data protection provisions;
- (c) may propose administrative measures and issue general recommendations on the appropriate application of the Regulation and of this Decision;
- (d) may make recommendations for the practical improvement of data protection to the EEAS management, staff and any relevant external party;
- (e) may investigate data protection matters and, in addition to the person who requested the investigation or lodged the complaint, may report the result of the investigation to the data controller, and to any relevant member of the EEAS management;
- (f) may develop templates and internal procedures, instructions or policies to provide guidance to data controllers and processors;
- (g) may use the services of external experts, including IT specialists;
- (h) may bring to the attention of the EEAS Appointing Authority any failure by a staff member to comply with the obligations under the Regulation and this Decision and suggest the launch of an administrative investigation;
- (i) may issue internal guidelines on data protection (DPO Guidance Notes) that shall be taken into account when processing personal data.

*Article 7***Resources**

1. The DPO shall be provided with adequate staff and resources necessary to carry out the tasks referred to in Article 5 of this Decision.
2. All EEAS staff shall support the DPO in carrying out the tasks referred to in Article 5 of this Decision, in particular the data controllers and processors shall provide requested information about data processing activities, access to personal data and prepare draft replies to the requests of the data subjects exercising their right of access, modification and deletion received by the DPO but related to the processing activities for which the data controller is responsible.
3. The DPO may have a deputy or an assistant DPO as well as administrative staff and secretarial support, as required. The DPO may also use other EEAS or contracted entities and external experts.
4. When designated, the deputy or assistant DPO shall support the DPO in carrying out his or her tasks and may represent the DPO in the event of his or her absence. Article 4, 5 and 6 of this Decision shall also apply to the deputy or assistant DPO.
5. The DPO shall have appropriate premises where the security and confidentiality of information, including personal data, can be guaranteed and where adequate storage and archiving of data and documents can be ensured.
6. The DPO shall have at their disposal an electronic tool which can (i) manage the records of personal data processing activities in accordance with Article 31 of the Regulation and (ii) store data protection notices, data breach notifications, data protection impact assessments, data subject requests and records of data transfers.
7. The EEAS shall support the DPO in maintaining and expanding their expert knowledge, among others, by facilitating participation in inter-institutional or external training courses, conferences or events related to data protection and in meetings and trainings organised by the EDPS and the DPO Network of EU institutions, bodies, offices and agencies.

SECTION 3

ACTORS INVOLVED IN PROCEDURES IN RELATION TO DATA PROTECTION*Article 8***Data controllers and processors**

1. The delegated controllers, the representatives of the controllers and of the processors are responsible, on behalf of the data controller, for ensuring that all processing activities under their control comply with the Regulation, in particular Article 26 thereof, and with the provisions of this Decision. They may, as required, entrust data processing tasks to EEAS staff working under their responsibility or to contracted entities, in accordance with Article 29 of the Regulation.
2. In particular, data controllers shall:
 - (a) be accountable, ensure and demonstrate that processing is carried out in compliance with the Regulation and this Decision;
 - (b) record any processing activity and any substantial changes to an existing processing activity;
 - (c) ensure that the data subjects are informed about the processing of their data in accordance with Articles 15 and 16 of the Regulation by making the data protection notices available;
 - (d) cooperate with the DPO and the EDPS, in particular by providing information in reply to their requests within 14 calendar days of the date of the request;

- (e) inform the DPO when a contractor is used to process personal data on behalf of the data controller;
- (f) appoint a DPC, support them in fulfilling their duties and inform the DPO about any change of the person or function of the DPC;
- (g) consult the DPO on whether processing activities comply with the Regulation and this Decision. They may consult the DPO or other experts on issues relating to the confidentiality, availability and integrity of the processing activities and on the security measures taken pursuant to Article 33 of the Regulation.

3. Data controllers may use other entities in the EEAS or contracted entities as processors in compliance with the provisions of the Regulation, as long as they document in their records who the processor is, specify the tasks entrusted to them and the security measures taken.

4. The data controller shall ensure that the DPO is informed without delay:

- (a) of all issues that have, or might have, data protection implications;
- (b) of all EEAS management communication and decisions in relation to the application of the Regulation, in particular any interaction with the EDPS.

Article 9

Data protection coordinator and correspondent

1. Depending on their size and on the type of personal data processed, EEAS organisational entities shall have a DPC who would act as a focal point for data protection. Each managing directorate or directorate in the EEAS Headquarters and each EU Delegation shall designate a data protection coordinator or a data protection correspondent. All divisions that regularly process a large quantity of personal data, special categories of data or sensitive personal data, the processing of which presents high risk, shall also designate their own DPC. The DPC function shall be assigned to a position that has an overview on the activities of the entity.

2. The DPC shall have the necessary skills and acquire knowledge about data protection. They shall receive a data protection induction training and may attend information sessions and DPC Network meetings.

3. The DPC shall:

- (a) without prejudice to the responsibilities of the DPO, assist the data controllers in complying with their obligations;
- (b) facilitate communication between the DPO and the data controllers.
- (c) be a focal point for data protection matters in their service and liaise with the DPO;
- (d) inform and support their colleagues on matters related to the processing of personal data;
- (e) forward information to staff on awareness-raising events and training sessions;
- (f) work with the DPO to create and update an inventory of existing and new processing activities of personal data;
- (g) contact and notify the DPO regarding any personal data processed within the service;
- (h) assist in identifying the relevant delegated data controllers and processors;
- (i) develop records in their area of expertise;
- (j) support data controllers in establishing and reviewing records and creating data protection notices;
- (k) to contribute to compliance verifications and impact assessments;
- (l) ensure that the relevant data protection notices are published and correctly used by their service;

- (m) notify the DPO of any data breaches;
 - (n) prepare, in cooperation with the DPO, the reply to requests from data subjects exercising their rights, handle complaints and questions relating to the data processing activities in their service.
4. The DPC has the right to obtain necessary information required to identify personal data processing activities and consult the DPO on behalf of their service. This does not include the right to access personal data processed under the responsibility of the data controller.

Article 10

Appointing Authority

The Appointing Authority shall consult the DPO on any request or complaint pursuant to Article 90 of the Staff Regulations in relation to the application of the Regulation.

Article 11

EEAS staff

1. All EEAS staff shall apply the confidentiality and security rules for the processing of personal data as set out in Articles 33, 34 and 35 of the Regulation. No EEAS staff member with access to personal data shall process the data other than on instructions from the data controllers.
2. All EEAS staff members shall indicate to their line manager when they need to process personal data in order for data controllers to document the processing in their data protection records and to prepare the necessary data protection notices.
3. Any EEAS staff member may submit a request or raise a concern, including an alleged data breach, to the DPO, or may lodge a complaint with the EDPS regarding an alleged breach of the Regulation or of this Decision, without the necessity to inform its hierarchical superiors.
4. If any staff member considers that a third country, a territory or one or more specified sectors within a third country, or an international organisation does not ensure an adequate level of protection within the meaning of Article 45(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council ⁽³⁾ or to Article 36(3) of Directive (EU) 2016/680 of the European Parliament and of the Council ⁽⁴⁾, they shall notify the DPO.

SECTION 4

MEASURES AND PROCEDURES

Article 12

Security measures and data protection by design and by default

1. The safeguards, technical and organisational measures to avoid data breaches, leakages or unauthorised disclosure shall include:
 - (a) an adequate definition of roles, responsibilities and procedural steps;
 - (b) a secure electronic environment which prevents unlawful or accidental access or transfer of electronic data to unauthorised persons with safety measures built in the various IT applications used;

⁽³⁾ 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

⁽⁴⁾ 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).

- (c) secure processing and storage of paper-based documents;
- (d) electronic and physical access only to authorised staff with access rights to be granted individually;

2. Before designing data processing activities, data controllers shall implement data protection by design and by default as referred to in Article 27 of the Regulation. In order to implement data protection by design and default, the data controller may consult the DPO and other relevant services, including IT and IT security.

Article 13

Data breach notifications

After becoming aware of any incident, in particular a breach of security, leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transferred, stored, or otherwise processed ('personal data breach'), the data controller or processor shall immediately notify the DPO and within 72 hours the EDPS and shall appropriately document the incident.

Article 14

Investigations and handling requests and complaints by the DPO

1. The DPO may open an investigation concerning an alleged breach of the obligations under the Regulation on his or her own initiative or upon request. Requests shall be addressed to the DPO in writing.
2. The DPO may request a written statement on the matter from the data controller responsible for the relevant data processing activity. The data controller shall provide the response to the DPO within 14 calendar days of receiving this request. The DPO may request access to complementary information, documents, data carriers, data centres, premises and systems from other EEAS services, in particular the IT division, the security directorate, and the directorate-general dealing with administrative inquiries and disciplinary procedures. The DPO shall be provided with the information or opinion within 14 calendar days.
3. In the case of manifestly unfounded, abusive and excessive requests, in particular where requests of repetitive character have been made by the same data subject, the DPO may refuse to act on the request pursuant to Article 14 of the Regulation. The requestor shall be informed accordingly.

SECTION 5

PROCEDURE FOR DATA SUBJECTS TO EXERCISE THEIR RIGHTS

Article 15

General provisions

1. Data subjects may contact the data controller or the DPO to exercise their rights in accordance with Articles 14 to 24 of the Regulation.
2. Requests to exercise data subjects' rights shall be made in writing. If necessary, the DPO shall assist the data subject in identifying the relevant data controller. The DPO shall forward any requests received to the relevant data controller who may consult the DPO.
3. The data controllers shall process the request and reply directly to the data subject.

*Article 16***Processing requests for exercising data subject rights**

1. Data controllers shall act on the request only after the requestor's identity has been verified or in case of a request by a representative of the data subject, the authorisation from the data subject has been provided.
2. The data controller responsible for the data processing activity shall send to the requestor an acknowledgement of receipt within 14 calendar days of the receipt of the request by the EEAS. Unless otherwise provided, the data controller shall reply to the request within 1 month of the registration of the request. The data controller shall either give a positive reply to the request or state in writing the reasons for a complete or partial refusal. The period for reply may be extended by up to 2 further months, taking into account the complexity of the matter and the number of requests made, in accordance with Article 14(3) of the Regulation.
3. The data subject's request can be refused, if
 - (a) the request is not justified;
 - (b) an exception established in the Regulation applies;
 - (c) a restriction applies in accordance with the internal rules ⁽⁵⁾ adopted on the basis of Article 25 of the Regulation.
4. In the case of manifestly unfounded, abusive and excessive requests, in particular where requests of repetitive character have been made by the same data subject, the data controller, after having consulted the DPO, may refuse to act on the request pursuant to Article 14 of the Regulation. The requestor shall be informed accordingly.

*Article 17***Exceptions and restrictions**

Restrictions in accordance with the internal rules adopted on the basis of Article 25 of the Regulation and exceptions established in Articles 15-19 and 21-24 of the Regulation shall be applied only after having consulted the DPO.

SECTION 6

FINAL PROVISIONS*Article 18***Communication about this Decision**

1. In accordance with Article 41 of the regulation, the EDPS shall be informed about this Decision.
2. This decision shall be made available to the EEAS staff through appropriate means, in particular by publishing it on the internal website of the EEAS.

*Article 19***Repeal**

Decision PROC HR(2011) 016 of the High Representative of the Union for Foreign Affairs and Security Policy of 8 December 2011 on the rules regarding data protection is hereby repealed.

⁽⁵⁾ Decision of the High Representative of the Union for Foreign Affairs and Security Policy on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the European External Action Service (ADMIN(2019) 10).

*Article 20***Effect**

This Decision shall take effect on the day following its adoption.

Done at Brussels, 1 October 2019.

Federica MOGHERINI
The High Representative

Decision of the High Representative of the Union for Foreign Affairs and Security Policy
of 1 October 2019
on internal rules concerning restrictions of certain rights of data subjects in relation to processing of
personal data in the framework of the functioning of the European External Action Service
(2019/C 370/06)

THE HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to the Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service ⁽¹⁾,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 ⁽²⁾ ('Regulation (EU) 2018/1725'), and in particular Article 25 thereof,

Having regard to the opinion of the European Data Protection Supervisor in accordance with Article 41(2) of the Regulation (EU) 2018/1725, delivered on 28 June 2019,

Whereas:

- (1) The European External Action Service (EEAS) carries out its activities in accordance with Decision 2010/427/EU.
- (2) In accordance with Article 25(1) of Regulation (EU) 2018/1725, restrictions of the application of Articles 14 to 21, 35 and 36, as well as Article 4 of Regulation (EU) 2018/1725 insofar as its provisions correspond to the rights and obligations provided for in Articles 14 to 21, shall be laid down by the EEAS in internal rules, where they are not based on legal acts adopted on the basis of the Treaties.
- (3) These internal rules, including its provisions on the assessment of the necessity and proportionality of a restriction, should not apply where a legal act adopted on the basis of the Treaties provides for a restriction of data subject rights.
- (4) Where the EEAS performs its duties with respect to data subject's rights under Regulation (EU) 2018/1725, it shall consider whether any of the exemptions laid down in that Regulation apply.
- (5) Such restrictions may apply to different data subject rights, including the provision of information to data subjects, right of access, rectification, erasure, restriction of processing, communication of a personal data breach to the data subject or confidentiality of communication.
- (6) Within the framework of its organisation and functioning the EEAS carries out activities involving personal data wherein it may be necessary and proportionate in a democratic society to impose a restriction in accordance with Article 25(1) of Regulation (EU) 2018/1725 in order to safeguard a legitimate interest, while respecting the essence of the fundamental rights and freedoms of data subjects.
- (7) Such restrictions may apply to several categories of personal data, including factual data and assessment data.
- (8) Assessments, observations and opinions are considered personal data in the meaning of Article 3(1) of Regulation (EU) 2018/1725. Limitations, in particular to the access, rectification and erasure of such assessments, observations or opinions in the context of staff selection and evaluation procedures, and in the context of activities of the Medical Service, the Mediation Service and the internal audit and inspection services for Union Delegations and Offices, are foreseen in these specific administrative procedures.

⁽¹⁾ OJ L 201, 3.8.2010, p. 30.

⁽²⁾ OJ L 295, 21.11.2018, p. 39.

- (9) In relation to selection and recruitment procedures, staff evaluation and public procurement procedures the right to access, rectification, erasure and restriction can be exercised only at certain points in time as foreseen in the relevant procedure in order to safeguard the rights of other data subjects and to respect the principles of equal treatment and the secrecy of deliberations.
- (10) The data subject may exercise the right to rectification of assessments or opinions of EEAS medical officers and advisers by providing their comments or a report of a medical practitioner of their choice.
- (11) In relation to the selection and recruitment procedures, it is not possible to modify the opinion or the assessment of the selection board. This right may be exercised through an appeal of the decision of the selection board. The assessments made by individual members of the selection board and the internal discussions of the selection board are covered by the secrecy of deliberations.
- (12) In relation to the staff evaluations, including appraisal procedures, it is not possible to modify the opinion or the assessment of the different actors intervening in the appraisal procedure. Data subjects may exercise the right to rectification by providing their comments or by making an appeal as foreseen by the staff appraisal procedure.
- (13) Restrictions to personal data rights and obligations shall be applied on a case-by-case basis and maintained for no longer than necessary for the fulfilment of the purpose of the restriction.
- (14) The EEAS is committed to respecting, to the maximum extent possible, the fundamental rights of the data subjects, including the right of provision of information, access and rectification, right to erasure, restriction of processing, right of communication of a personal data breach to the data subject or confidentiality of communication, as enshrined in Regulation (EU) 2018/1725. However, the EEAS may also be required to restrict the rights and obligations for the purpose of protecting its activities and the fundamental rights and freedoms of others,

HAS DECIDED AS FOLLOWS:

Article 1

Subject-matter and scope

1. In accordance with Article 25 of Regulation (EU) 2018/1725 (the 'Regulation'), this Decision lays down rules relating to the conditions under which the EEAS, in the framework of its activities referred to in paragraph 2, may restrict the application of the rights and obligations under the Regulation Articles 14 to 21, 35 and 36, as well as Article 4 of the Regulation insofar as its provisions correspond to the rights and obligations provided for in the same Articles 14 to 21.
2. This Decision applies to the processing of personal data by the EEAS for the purposes of the following activities:
 - (i) internal investigations, including security investigations, administrative enquiries including on harassment or reported irregularities, disciplinary and suspension proceedings;
 - (ii) notifying and referring cases to the Investigation and Disciplinary Office of the Commission (IDOC) and the European Anti-Fraud Office (OLAF);
 - (iii) security analyses related to cyber security incidents or IT system abuse, including external involvement of CERT-EU, ensuring internal security by means of video surveillance, access control and investigation purposes, securing communication and information systems and carrying out technical security counter-measures;
 - (iv) investigating matters directly relating to the tasks of the Data Protection Officer of the EEAS (hereinafter 'DPO');
 - (v) internal audits;
 - (vi) inspections of EU Delegations and offices;
 - (vii) activities of the Medical Service and of medical advisers engaged by the EEAS;
 - (viii) activities of the Mediation Service;
 - (ix) public procurement procedures;
 - (x) staff selection procedures and staff evaluations;

- (xi) collecting data for intelligence purposes, including situational awareness, counter-intelligence, early warning and intelligence analysis supporting the various EU decision-making bodies in the fields of the Common Foreign and Security Policy (CFSP), the Common Security and Defence Policy (CSDP), Counter-terrorism and Hybrid threats;
- (xii) procedures on restrictive measures (sanctions) in pursuit of specific foreign and security policy objectives of the Union;
- (xiii) activities to protect other important objectives of general public interest of the Union or of a Member State, in particular the objectives of the CFSP.

For the purposes of this Decision, the above activities shall include preparatory and follow-up actions directly related to the same activities.

3. The categories of personal data processed related to the above activities may contain factual data and assessment data. Factual data include data related to personal identification and other administrative details, metadata related to electronic communications and traffic data. Assessment data include the description and assessment of situations and circumstances, opinions, observations related to data subjects, evaluation of the conduct or performance of data subjects and reasoning underpinning individual decisions in connection with the administrative functioning of the EEAS.

Article 2

Specification of the controller and safeguards

1. The EEAS shall put in place specific safeguards to avoid data breaches, leakages or unauthorised disclosure of data under a restriction, such as
 - (a) enhanced security measures for storing physical supports with personal data;
 - (b) specific security measures for electronic databases and tools;
 - (c) restrictions on access and log files.
2. The data controller for the data processing activities is the EEAS. The organisational entities that may restrict rights and obligations referred to in Article 1(1) are the services that are in charge of the activities described under Article 1(2).
3. Restrictions to personal data rights and obligations should be maintained for no longer than necessary for the fulfilment of the purpose of the restriction. The retention period for personal data under a restriction shall be defined taking into account the purpose of the processing and shall include the timeframe necessary for administrative and judicial review.

Article 3

Restrictions

1. A restriction under this Decision may be applied by the EEAS on a case-by-case basis to safeguard:
 - (a) national security, public security or defence of Member States, including, but not limited to surveillance and processing of data for intelligence purposes or for the protection of human life, especially in response to natural or manmade disasters and terrorist attacks;
 - (b) the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including, but not limited to preventing threats to public security; such investigations may include administrative inquiries, disciplinary proceedings or OLAF investigations to the extent that there is a connection with the prevention or investigation of criminal offences;
 - (c) important objectives of general public interest of the Union or of a Member State, in particular CFSP objectives or important economic or financial interests of the Union or of a Member State, including, but not limited to monetary, budgetary and taxation matters, public health and social security, and procurement procedures and investigations serving important objectives of public interest of the Union;
 - (d) the internal security of Union institutions and bodies, including, but not limited to the electronic communications and information networks;
 - (e) the protection of judicial independence and judicial proceedings, including legal advice;

- (f) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions or violations of obligations in the Staff Regulations ⁽³⁾ and the Financial Regulation ⁽⁴⁾, including cases with no connection to criminal offences;
- (g) monitoring, inspection or regulatory functions connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c), including, but not limited to the case of a targeted audit, an inspection or an investigation;
- (h) the protection of the data subject or the rights and freedoms of others, including, but not limited to the protection of witnesses, interviewed persons in the context of security investigations, administrative inquiries, inspections and audits, whistleblowers and alleged victims of harassment;
- (i) the enforcement of civil law claims.

2. Subject to Articles 4 to 8, the EEAS may restrict the rights and obligations referred to in Article 1(1) in relation to personal data obtained from another Union institution, body, agency or office, competent authorities of a Member State or third country or from an international organisation, in the following cases:

- (a) where the exercise of those rights and obligations could be restricted by the other Union institution, body, agency or office on the basis of their relevant legal acts adopted in accordance with Article 25 or Chapter IX of the Regulation or their founding acts;
- (b) where exercise of those rights and obligations could be restricted by the competent authorities of a Member State on the basis of legal acts adopted in accordance with Article 23 of Regulation (EU) 2016/679 ⁽⁵⁾ of the European Parliament and of the Council or under national measures transposing Articles 13(3), 15(3) or 16(3) of Directive (EU) 2016/680 ⁽⁶⁾ of the European Parliament and of the Council;
- (c) where the exercise of those rights and obligations could jeopardise the EEAS cooperation with third countries or international organisations in the conduct of its activities, unless this need to cooperate is overridden by the interests or fundamental rights and freedoms of the data subjects.

Before applying a restriction under this paragraph, the EEAS shall consult the relevant Union institution, body, agency, office, international organisation or the competent authorities of a Member State unless it is patently clear that the restriction is provided for by a legal act referred to under this paragraph or such a consultation would jeopardise the EEAS activities.

3. Before applying a restriction, the EEAS shall consider if it is necessary and proportionate in a democratic society and that it respects the essence of the fundamental rights and freedoms of data subjects.

In making the necessity and proportionality assessment for each case, the EEAS shall:

- i. weigh the risk to the rights and freedoms of the data subject against the risk to the rights and freedoms of others. The risks to the rights and freedoms of the data subject concern primarily their privacy, their reputation and the moment in time when they can start to exercise their rights of defence; and
- ii. consider the need to safeguard the objective of the EEAS activities under Article 1(2), in particular the risk of destroying or hiding evidence.

This necessity and proportionality assessment, as well as the reasons for a restriction, shall be documented. To that end, every restriction shall be specifically recorded in the inventory managed by the data controller and shall state how the exercise of the restricted rights and obligations referred to in Article 1(1) would jeopardise the purpose of the activities referred to in Article 1(2), or would adversely affect the rights and freedoms of others. The documents containing the underlying factual and legal elements of the restriction shall be also registered. The records shall be made available to the European Data Protection Supervisor on request.

⁽³⁾ Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union (OJ 45, 14.6.1962, p. 1385 in its consolidated version).

⁽⁴⁾ Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

⁽⁵⁾ 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

⁽⁶⁾ 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).

Access to the records in the inventory, including the assessment note, shall be restricted for as long as the restriction it justifies remains valid in accordance with paragraph 4 and 5.

4. A restriction shall be lifted as soon as the reasons, that justify it, no longer exist.
5. The need to maintain a restriction shall be reviewed at appropriate intervals, at least every six months from its adoption, and in any case at the closure of the relevant procedure in relation to the activities referred to in Article 1(2).

Article 4

Review by the Data Protection Officer

1. Each organisational entity shall, without undue delay, inform the DPO in writing when it restricts the exercise of the rights and obligations referred to in Article 1(1), when it performs the review of the restriction and when it extends or lifts the restriction. The DPO shall have access to the records established in accordance with Article 3(3).
2. The DPO may request the data controller in writing to review the application of the restriction. The data controller shall inform the DPO in writing about the outcome of the requested review.
3. Documents under this article shall be made available to the EDPS on request.

Article 5

Provision of information to data subjects and information on restrictions

1. The EEAS shall publish on its website or intranet its privacy statements and data protection notices that inform data subjects of its activities involving processing of personal data, of their rights and their potential restrictions.
2. The right to information may be restricted by the data controller with regards to activities under Article 1(2) (i), (ii), (iii), (iv), (v), (vi), (viii), (xi), (xii) and (xiii). Without prejudice to paragraph 4, the EEAS, where proportionate, shall inform individually the concerned data subjects of the application of the restriction without undue delay and in a written form. If a request from a data subject is rejected due to a restriction, data subjects shall be informed of the principal reasons on which a restriction is based and of their right to lodge a complaint with the European Data Protection Supervisor.
3. A restriction under this article shall be applied in accordance with Articles 3 and 4.
4. The provision of information about a restriction under this Decision may be deferred, omitted or denied if it would cancel the effect of the restriction. This deferral, omission or denial shall be applied in accordance with the provisions of Article 3 and 4.

Article 6

Right of access

1. The right of access under Article 17 of the Regulation may be restricted with regards to activities under Article 1(2) (i), (ii), (iii), (iv), (v), (vi), (vii), (viii), (x), (xi), (xii) and (xiii).
2. Where data subjects request access to their personal data processed in the context of a specific activity referred to in Article 1(2), the EEAS shall limit its response to the personal data processed for that activity.
3. Where the EEAS restricts, wholly or partly, the right of access to personal data by data subjects, as referred to in Article 17 of Regulation (EU) 2018/1725, it shall inform the data subject concerned, in writing, in its reply to the request for access without undue delay of the restriction applied and of the principal reasons thereof. The provision of information concerning the reasons for the restriction may be deferred, omitted or denied for as long as it would undermine the purpose of the restriction.
4. The EEAS may restrict, on a case-by-case basis, data subjects' right to access directly medical data of a psychological or psychiatric nature, where access to such data is likely to represent a risk for the data subject's health. This restriction shall be proportionate to what is strictly necessary to protect the data subject. In such cases, access to the information shall be given to a medical practitioner of the data subject's choice.

5. A restriction under this article shall be applied in accordance with Articles 3, 4 and 5.

Article 7

Right of rectification, erasure and restriction of processing

1. The right to rectification, erasure and restriction of processing under Articles 18, 19(1) and 20(1) of the Regulation may be restricted with regards to activities under Article 1(2) (i), (ii), (iii), (iv), (v), (vi), (vii), (viii), (ix), (x), (xi), (xii) and (xiii).
2. In relation to medical data, data subjects may exercise the right to rectification of the assessments or opinions of EEAS medical officers or advisors by providing their comments or a report of a medical practitioner of their choice.
3. A restriction under this article shall be applied in accordance with Articles 3, 4 and 5.

Article 8

Communication of a personal data breach to data subjects

1. The right to the communication of a personal data breach to the data subject under Article 35 of the Regulation may be restricted with regards to activities under Article 1(2) (i), (ii), (iii), (iv), (v), (vi), (viii), (xi), (xii) and (xiii).
2. A restriction under this article shall be applied in accordance with Articles 3, 4 and 5.

Article 9

Confidentiality of electronic communications

1. The obligation of ensuring the confidentiality of electronic communications may only be restricted with regards to activities under Article 1(2) (i), (ii), (iii), (iv), (xi), (xii) and (xiii) in the following exceptional cases:
 - (a) if the restriction to the obligation of ensuring the confidentiality of the calling line identification is necessary to trace nuisance calls;
 - (b) if the restriction to the obligation of ensuring the confidentiality of the calling line identification and location data is necessary to allow emergency services to carry out their tasks effectively;
 - (c) if the restriction to the obligation of ensuring the confidentiality of the communications, traffic data and location data is necessary to safeguard national security, public security or defence of the Member States, internal security of Union institutions and bodies, the prevention, investigation, detection and prosecution of criminal offences, violations of the Staff Regulations and the Financial Regulation or of unauthorised use of the electronic communication system, as referred to in Article 25 of the Regulation.
2. A restriction under this article shall be applied in accordance with Articles 3, 4 and 5.

Article 10

Entry into force

This Decision shall enter into force on the day following its publication in the *Official Journal of the European Union*.

Done at Brussels, 1 October 2019.

Federica MOGHERINI
The High Representative

EUROPEAN DATA PROTECTION SUPERVISOR

Summary of the Opinion of the European Data Protection Supervisor on the revision of the EU Regulations on service of documents and taking of evidence in civil or commercial matters

(The full text of this Opinion can be found in English, French and German on the EDPS website www.edps.europa.eu)

(2019/C 370/07)

On 31 May 2018, the European Commission issued two proposals for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters ⁽¹⁾, on the one hand and a Regulation amending Regulation (EC) No 1393/2007 of the European Parliament and of the Council of 13 November 2001 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters ⁽²⁾, on the other hand. The proposals mainly aim at improving the smooth functioning of judicial cooperation in these areas, by, inter alia, providing for transmission of documents and taking of evidence requests through a decentralised IT system.

The EDPS acknowledges that exchanges of personal data are necessary elements of the creation of an area of Freedom, Security and Justice. Therefore he welcomes the overall objectives of the proposals to improve the efficiency of judicial cooperation in civil or commercial matters in relation to the taking of evidence and the service of documents, in particular through digitalisation and the use of IT technology. He shares the view that the proposed legislation could have a real impact on the everyday lives of EU citizens.

This Opinion makes three main recommendations in order to constructively assist the legislators in achieving this very important objective while ensuring compliance with the Charter and the GDPR:

- providing a clear legal basis for the IT system which would be used for the transmission of documents, requests and communications for the purposes of these Regulations. In particular, in case the IT system would entail the involvement of an EU institution, body, agency or office, this legal basis should in principle be provided in an EU legislative act. Also, even in case the processing of personal data would take place in the framework of an existing IT system, the EDPS recommends providing for the use of such system in the legislative act itself. However, the existing system envisaged to be used should itself be duly established on the basis of a legal act adopted at EU level, which is currently not the case of e-CODEX. Should the EU legislator choose the e-CODEX solution, the lack of a legal instrument at EU level establishing and regulating the system should be remedied without delay,
- including in the legislative acts themselves a high level description of the IT system aspects, such as data protection responsibilities or relevant applicable safeguards, to be further defined in implementing acts. In particular, to the extent the Commission or another EU institution, body, agency or office would be implicated in the operation of the new system, the legal act should ideally define its responsibilities as a (joint) controller or a processor,
- conducting an impact assessment on data protection when preparing the implementing acts.

Further detailed recommendations are provided by the EDPS in this Opinion.

The EDPS remains at the disposal of the institutions for further advice during the legislative process and at the implementing phase of the Regulations once adopted.

⁽¹⁾ OJ L 174, 27.6.2001, p. 1.

⁽²⁾ OJ L 324, 10.12.2007, p. 79.

1. Introduction and background

1. On 31 May 2018, the Commission adopted two proposals ⁽³⁾ for a Regulation of the European Parliament and the Council that would amend:
 - Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (hereinafter the ‘taking of evidence Regulation’),
 - Regulation (EC) No 1393/2007 of the European Parliament and of the Council on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (hereinafter the ‘service of documents Regulation’).
2. The taking of evidence Regulation, which has applied since 2004, provides for two ways of taking of evidence between Member States: taking of evidence through the requested court and the direct taking of evidence by the requesting court.
3. The service of documents Regulation, which has applied since 2008, provides for different ways of transmitting documents from one Member State to another, for purposes of service in the latter, through transmitting and receiving agencies or through transmission by consular or diplomatic channels. It also sets uniform legal conditions for serving a document by post directly across borders and provides for a direct service through the competent person of the Member State addressed where permitted under the law of that Member State. It includes certain minimum standards on the protection of the rights of defence. The application of the Regulation ‘is not restricted to proceedings before civil tribunals, because its scope covers also ‘extrajudicial’ documents, the service of which may arise in various out-of-court proceedings (e.g. in succession cases before a public notary, or in family law cases before a public authority), or even in the absence of any underlying judicial proceedings’ ⁽⁴⁾.
4. The proposals are included in the Commission’s 2018 work programme under REFIT initiatives in the area of justice and fundamental rights based on mutual trust ⁽⁵⁾. The proposals are accompanied by an impact assessment ⁽⁶⁾.
5. Both proposals provide for the transmission of documents, requests and communications through a mandatory decentralised IT system composed of national IT systems interconnected by a communication infrastructure enabling the secure and reliable cross-border exchange of information between the national IT systems. They also provide for the application of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market ⁽⁷⁾.
6. On 13 February 2019, the European Parliament adopted its legislative resolutions on both proposals at first reading ⁽⁸⁾, *inter alia* agreeing on the establishment of a decentralised IT system, providing that such system be based on e-CODEX and that the implementation of such system be ensured via delegated acts.
7. On 6 June 2019, a policy debate took place in Council. The presidency concluded that ‘the Council confirmed the need to modernise our processes when it comes to judicial cooperation in civil and commercial matters. The presidency noted the preference expressed for a decentralised and secured IT system. It added that ministers could accept mandatory use of the system only with certain conditions, including a longer transition period and with a

⁽³⁾ Proposal COM(2018)378 final (hereinafter the ‘taking of evidence proposal’) and proposal COM (2018)379 final (hereinafter the ‘service of documents proposal’).

⁽⁴⁾ Explanatory memorandum, p. 2.

⁽⁵⁾ Commission work programme 2018: an agenda for a more united, stronger and more democratic Europe (COM(2017) 650 final, 24.10.2017), Annex II, points 10 and 11.

⁽⁶⁾ Commission Staff working documents SWD(2018) 285 and SWD(2018) 287.

⁽⁷⁾ Explanatory memorandum of the taking of evidence proposal, p. 3 and of the service of documents proposal, p. 4: ‘[w]hile in principle nothing prevents Member States from digitalising the way they communicate, past experience and projections of what will happen without EU action show that progress would be very slow and that, even where Member States take action, interoperability cannot be ensured without a framework under EU law. The objective of the proposal cannot be sufficiently achieved by the Member States themselves and can be achieved only at Union level’.

⁽⁸⁾ P8_TA(2019)0103 and P8_TA(2019)0104.

backendreference system to be provided by the Commission. A list of necessary exceptions will also have to be considered. Finally, the presidency noted that e-CODEX could be the software solution to be used for that purpose. Further work will have to be conducted at technical level' ⁽⁹⁾.

8. On 23 April 2019, the Commission has submitted a request for consultation to the European Data Protection Supervisor (hereinafter the 'EDPS') in order to assess the conformity of both proposals with the General Data Protection Regulation (hereinafter the 'GDPR'). The EDPS welcomes the consultation by the Commission.

3. Conclusions

24. The EDPS welcomes the overall objectives of the proposals to improve the efficiency of judicial cooperation, in particular through digitalisation and the use of IT technology, in relation to the taking of evidence and the service of documents in civil or commercial matters. Therefore, this Opinion aims at providing constructive and objective advice to the EU institutions.
25. The EDPS welcomes the identification of a high-level architecture of the system in the legislative act itself and the obligation of a reliable exchange of information as well as the need to use trust services as defined in Regulation (EU) No 910/2014.
26. There are three major recommendations the EDPS makes to ensure compliance with the Charter and the GDPR:
- providing a clear legal basis for the IT system which would be used for the transmission of documents, requests and communications for the purposes of these Regulations. In particular, in case the IT system would entail the involvement of an EU institution, body, agency or office, this legal basis should in principle be provided in an EU legislative act. Also, even in case the processing of personal data would take place in the framework of an existing IT system, the EDPS recommends providing for the use of such system in the legislative act itself. However, the existing system envisaged to be used should itself be duly established on the basis of a legal act adopted at EU level, which is currently not the case of e-CODEX. Should the EU legislator choose the e-CODEX solution, the lack of a legal instrument at EU level establishing and regulating the system should be remedied without delay,
 - including in the legislative acts themselves a high level description of the IT system aspects, such as data protection responsibilities or relevant applicable safeguards, to be further defined in implementing acts. In particular, to the extent the Commission or another EU institution, body, agency or office would be implicated in the operation of the system, the legal act should ideally define its responsibilities as a (joint) controller or a processor,
 - conducting an impact assessment on data protection when preparing the implementing acts.
27. The EDPS also recommends:
- providing in both legislative acts for an implementing act to further detail the IT system and that the implementing acts cover the new provisions on electronic service and on direct taking of evidence by videoconference so as to include specific safeguards also on these processing operations,

⁽⁹⁾ Outcome of the Council meeting (9970/19), p. 7, provisional version available at: <https://www.consilium.europa.eu/media/39709/st09970-en19.pdf>

According to the Presidency Paper (9566/19), par. 8 and 13, 'in the Commission Impact Assessments accompanying both proposals, e-CODEX is considered the most suitable and only readily available IT system. The development of another decentralised system would mean that the same challenges already addressed in the context of the development of the e-CODEX would be addressed once again'. 'One of the existing solutions is e-CODEX, a system developed with EU financial support by a consortium of Member States over a period of almost 10 years. E-CODEX is currently used for the following: Business Registers Interconnection System (BRIS); the interconnection of national insolvency registers; the e-Evidence Digital Exchange System. However, insofar as use cases based on voluntary cooperation are concerned, e-CODEX is not yet implemented and used by all the Member States. In this context, during the discussions in the Working Party, for the Member States where there are currently no IT systems that support electronic procedures, the Commission could consider the development of a reference implementation solution for a back-end system at national level, provided that there is sufficiently strong and broad delegations' support for mandatory electronic communication. All systems would have to be technically interoperable and compliant with the same set of technical specifications (protocols, standards, XML schemas and workflows).'

- in case of joint controllership, defining in the implementing acts the relationship among joint controllers and the content of the mandatory arrangements among them,
 - specifying in the implementing acts safeguards ensuring an access to a limited number of authorised users,
 - defining in further detail as far as possible the statistical elements to be collected in the implementing acts.
28. Finally, the EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide advice at further stages of this process. The recommendations made in this Opinion are without prejudice to any additional comments that the EDPS could make as further issues may arise. He recalls that, in accordance with Article 42(1) of Regulation (EU) 2018/1725, the Commission has the obligation to consult the EDPS when preparing implementing or delegated acts having an impact on the protection of individual's rights and freedoms with regard to the processing of personal data. The EDPS expects therefore to be consulted later on the provisions of the draft implementing or delegated acts in this respect.

Brussels, 13 September 2019.

Wojciech Rafał WIEWIÓROWSKI
European Data Protection Supervisor

NOTICES CONCERNING THE EUROPEAN ECONOMIC AREA

EFTA SURVEILLANCE AUTHORITY

EFTA Surveillance Authority notice on State aid recovery interest rates and reference/discount rates for the EFTA States applicable as from 1 October 2019

(Published in accordance with the rules on reference and discount rates set out in Part VII of the Authority's State Aid Guidelines and Article 10 of the Authority's Decision No 195/04/COL of 14 July 2004 ⁽¹⁾)

(2019/C 370/08)

Base rates are calculated in accordance with the Chapter on the method for setting reference and discount rates of the Authority's State Aid Guidelines as amended by the Authority's Decision No 788/08/COL of 17 December 2008. To obtain the applicable reference rates, appropriate margins shall be added to the base rate in accordance with the State Aid Guidelines.

Base rates have been determined as follows:

	Iceland	Liechtenstein	Norway
1.10.2019 –	4,93	–0,66	1,72

⁽¹⁾ OJ L 139, 25.5.2006, p. 37 and EEA Supplement No 26, 25.5.2006, p. 1.

V

(Announcements)

ADMINISTRATIVE PROCEDURES

EUROPEAN COMMISSION

**Call for proposals for support for information measures relating to the common agricultural policy
(CAP) for 2020**

(2019/C 370/09)

Notice is hereby given of the launch of a call for proposals for information measures relating to the CAP for the 2020 financial year.

Proposals are invited for the following call: IMCAP — Support for information measures relating to the common agricultural policy (CAP) for 2020

This call for proposals, including deadlines and budgets for the different activities, is available on the *Funding & Tenders* portal (<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home>), along with information on the related activities and instructions for applicants on how to submit proposals. All this information will be updated as necessary on the same portal.

PROCEDURES RELATING TO THE IMPLEMENTATION OF COMPETITION POLICY

EUROPEAN COMMISSION

Prior notification of a concentration **(Case M.9568 — Marcegaglia Plates/Evraz Palini Bertoli)**

Candidate case for simplified procedure

(Text with EEA relevance)

(2019/C 370/10)

1. On 24 October 2019, the Commission received notification of a proposed concentration pursuant to Article 4 and following a referral pursuant to Article 4(5) of Council Regulation (EC) No 139/2004 ⁽¹⁾.

This notification concerns the following undertakings:

- Marcegaglia Plates S.p.A. ('Marcegaglia Plates', Italy). Marcegaglia Plates is a wholly owned subsidiary of the Marcegaglia Group (Italy).
- Evraz Palini & Bertoli S.r.l. ('Evraz Palini', Italy).

Marcegaglia Plates acquires within the meaning of Article 3(1)(b) of the Merger Regulation sole control of the whole of Evraz Palini.

The concentration is accomplished by way of purchase of shares.

2. The business activities of the undertakings concerned are:

- for Marcegaglia Plates: rolling of heavy quarto plates;
- for the Marcegaglia Group: steel processing ⁽²⁾;
- for Evraz Palini: rolling of heavy quarto plates.

3. On preliminary examination, the Commission finds that the notified transaction could fall within the scope of the Merger Regulation. However, the final decision on this point is reserved.

Pursuant to the Commission Notice on a simplified procedure for treatment of certain concentrations under the Council Regulation (EC) No 139/2004 ⁽³⁾ it should be noted that this case is a candidate for treatment under the procedure set out in the Notice.

4. The Commission invites interested third parties to submit their possible observations on the proposed operation to the Commission.

Observations must reach the Commission not later than 10 days following the date of this publication. The following reference should always be specified:

Case M.9568 — Marcegaglia Plates/Evraz Palini Bertoli

⁽¹⁾ OJ L 24, 29.1.2004, p. 1 (the 'Merger Regulation').

⁽²⁾ Marcegaglia Group is Europe's largest non-integrated steel supplier, processing mainly carbon steel but also stainless steel in its rolling mills and SSCs.

⁽³⁾ OJ C 366, 14.12.2013, p. 5.

Observations can be sent to the Commission by email, by fax, or by post. Please use the contact details below:

Email: COMP-MERGER-REGISTRY@ec.europa.eu

Fax +32 22964301

Postal address:

European Commission
Directorate-General for Competition
Merger Registry
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

OTHER ACTS

EUROPEAN COMMISSION

**Publication of a communication of approval of a standard amendment to the product specification
for a name in the wine sector referred to in Article 17(2) and (3) of Commission Delegated
Regulation (EU) 2019/33**

(2019/C 370/11)

This notice is published in accordance with Article 17(5) of Commission Delegated Regulation (EU) 2019/33 ⁽¹⁾.

COMMUNICATION OF APPROVAL OF A STANDARD AMENDMENT

PAUILLAC

PDO-FR-A0713-AM03

Date of communication: 9.8.2019

DESCRIPTION OF AND REASONS FOR THE APPROVED AMENDMENT

1. Demarcated parcel area

The date of 6 September 2018 is added to the 2nd indent of point 2 of Chapter I of the specification.

2. Geographical area

Point IV(1) of the specification:

- the phrase ‘on the basis of the Official Geographic Code in force on 27 April 2018’ is added after the word ‘aged’;
- the municipality of Cissac-Médoc has been deleted.

This amendment follows on from the demarcation work which established that there was no claim for designations for the plots located in the municipality of Cissac-Médoc, which is now removed from the geographical area.

Point 1.6 of the Single Document on the geographical area has been amended accordingly.

3. Link with the geographical area

In point 1(a) of section X of the specification, the words ‘Cissac-Médoc’ have been removed.

This amendment follows the change in the geographical area.

The Single Document is not affected by this amendment.

⁽¹⁾ Commission Delegated Regulation (EU) 2019/33 of 17 October 2018 supplementing Regulation (EU) No 1308/2013 of the European Parliament and of the Council as regards applications for protection of designations of origin, geographical indications and traditional terms in the wine sector, the objection procedure, restrictions of use, amendments to product specifications, cancellation of protection, and labelling and presentation (OJ L 9, 11.1.2019, p. 2).

4. **Parcels outside the municipality of Pauillac**

The annex setting out the list of parcels located outside the municipality of Pauillac and eligible to use the 'Pauillac' designation has been updated following the work on boundary setting.

The Single Document is not affected by this amendment.

SINGLE DOCUMENT

1. **Name of product**

Pauillac

2. **Geographical indication type**

PDO — Protected Designation of Origin

3. **Categories of grapevine products**

1. Wine

4. **Description of the wine(s)**

The name 'Pauillac' is can only be used for still red wines.

These wines have:

- a minimum natural alcoholic strength by volume of 11 %
- a total alcoholic strength by volume after enrichment of 13,5 %
- a malic acid content of $\leq 0,30$ g/l.
- a fermentable sugar content of ≤ 2 g/l.
- for wines sold in bulk, a volatile acidity content of $\leq 13,26$ meq/l until 31 July of the year following that of the harvest, and $\leq 16,33$ meq/l thereafter.

'Pauillac' wines are intense in colour. The wines are powerful and robust, notably due to the blending where Cabernet Sauvignon N is particularly dominant. The resulting tannic structure gives these wines excellent ageing capacity. Merlot N is nonetheless present, making for round, fruity wines. The structure and complexity are boosted by Cabernet Franc N and, to a lesser extent, Petit Verdot N. After long ageing, these wines develop a very complex bouquet.

The other criteria are in line with the applicable rules.

General analytical characteristics	
Maximum total alcoholic strength (in % volume)	
Minimum actual alcoholic strength (in % volume)	
Minimum total acidity	
Maximum volatile acidity (in milliequivalents per litre)	
Maximum total sulphur dioxide (in milligrams per litre)	

5. **Wine-making practices**

a. *Essential oenological practices*

Specific oenological practice

- Reductive methods of enrichment are permitted with a limit of a 15 % concentration rate.
- After enrichment, the wines' total alcoholic strength by volume must not exceed 13,5 %.

Growing method

The minimum vine planting density is 7 000 plants per hectare.

The spacing between the rows of the vines must not exceed 1,5 metres, and the spacing between plants in the same row must be at least 0,80 metres.

Pruning is carried out at the unfolded leaves stage (Lorenz stage 9) at the latest.

Vines are pruned with a maximum of 12 buds per plant, using the following techniques:

- the so-called Médoc long pruning, or short and 'shoot' pruning, with two canes per plant and a maximum of four buds per cane for the Cot N, Cabernet Sauvignon N, Merlot N and Petit Verdot N varieties, and a maximum of five buds per cane for the Cabernet Franc N and Carmenère N varieties. Repeat short pruning has two buds;
- short pruning to two cordons, or fan pruning to four arms.

Irrigation during the growing season of the vine may be authorised in accordance with the provisions of Article D. 645-5 of the Rural and Maritime Fishing Code.

b. *Maximum yields*

63 hectolitres per hectare

6. **Demarcated geographical area**

The grapes are harvested and the wines made, developed, and aged in the territory of the municipality of Pauillac in the department of Gironde, and on the parcels listed in the Annex to the specification for the following municipalities: Saint-Estèphe, Saint-Julien Beychevelle and Saint-Sauveur.

7. **Main wine grapes**

Petit Verdot N

Cabernet Franc N

Merlot N

Carmenère N

Cot N — Malbec N

Cabernet Sauvignon N

8. **Description of the link(s)**

The geographical area of production for the 'Pauillac' protected designation of origin is located in the department of Gironde in the central part of the Médoc peninsula, 50 km north of Bordeaux on the left bank of the estuary. It covers the territory of the municipality of Pauillac and part of the municipalities of Saint-Estèphe, Saint-Julien-Beychevelle and Saint-Sauveur.

This designation is produced in an area with a temperate oceanic climate and various climatic factors conducive to the establishment of a fine vineyard, thanks to the effect which the Atlantic Ocean and the Gironde have on regulating temperatures. The oceanic climate, in some years combined with periods of rain and low pressure in autumn, or, conversely, hot and very sunny late seasons, creates a notable 'vintage effect'. The area's main characteristics are, however, linked above all to the geology typical of this sedimentary basin, the specific geological history of its soils, its landscape and topography, and the current soil composition of its vineyards.

The parcel production area defines the plots whose soils are gravelly or gravelly with sand, on condition that the content of fine sand, usually windblown, is fairly low and the soil permeability is correct. The soils of Pauillac are among those best suited to Cabernet Sauvignon N, and Merlot N also thrives there. However, the parcels located on modern alluvial deposits, on large layers of windblown or poorly drained sandbanks, are excluded from the parcel production area because they are located on impermeable subsoil. The same applies to parcels which comprise artificial land, have been built on or used as gravel pits. The vineyard is managed very selectively, with limits on the distance between rows and monitoring of maximum load per parcel and per plant.

The quality and typical characteristics of the wines with the 'Pauillac' controlled designation of origin are based on the soil type and their topography in the vicinity of the estuary which protects the vineyard from climatic extremes.

Even more than in the other wine designations of the Médoc peninsula, the vintages of the municipality of Pauillac have been widely acknowledged by the various ownership classifications undertaken since the end of the 17th century. With currently 18 classified vintages (of which the leading ones were Lafite-Rothschild and Latour in 1855 and Mouton-Rothschild in 1973), this municipality has the largest number of classified vintages.

'Pauillac' wines are intense in colour. The wines are powerful and robust, notably due to the blending where Cabernet Sauvignon N is particularly dominant. The resulting tannic structure gives these wines excellent ageing capacity. Merlot N is nonetheless present, making for round, fruity wines. The structure and complexity are boosted by Cabernet Franc N and, to a lesser extent, Petit Verdot N. After long ageing, these wines develop a very complex bouquet.

Actual vine density is well above the 7 000 plants per hectare required by the specification for the designation of origin and the controlled yield means grapes are very ripe, healthy and concentrated. Very long macerations and large extractions are thus possible to obtain the necessary structure for ageing. Consequently, an ageing time of at least six months is essential to encourage the tannin-anthocyanin combinations needed to stabilise the colour and for the tannins to become coated and, therefore, softer.

9. Essential further conditions (packaging, labelling, other requirements)

Legal framework:

EU legislation

Type of further condition:

Derogation concerning production in the demarcated geographical area

Description of the condition:

The area in immediate proximity, defined by derogation for the processing and ageing of the wines, comprises the territory of the following municipalities in the department of Gironde beyond the plots listed in annex: Cissac-Médoc, Saint-Estèphe, Saint-Julien-Beychevelle, Saint-Laurent-Médoc, Saint-Sauveur, Saint-Seurin-de-Cadourne and Vertheuil.

Legal framework:

National legislation

Type of further condition:

Additional provisions relating to labelling

Description of the condition:

The broader geographical unit 'Bordeaux-Médoc', 'Vin de Bordeaux-Médoc' or 'Grand Vin de Bordeaux-Médoc' may be indicated on the label.

The size of the letters used must not be larger, either in height or in width, than two thirds of the size of the letters denoting the name of the registered designation of origin.

Link to the product specification

https://info.agriculture.gouv.fr/gedei/site/bo-agri/document_administratif-6d2525a4-0869-49f7-97bf-4a489bee5499

ISSN 1977-091X (electronic edition)
ISSN 1725-2423 (paper edition)



Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN