Official Journal of the European Union

C 233

English edition

Information and Notices

Volume 61

4 July 2018

Contents

EN

[1] Text with EEA relevance.

[1] Text with EEA relevance.

II

(Information)

INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN COMMISSION

Communication from the Commission

The adaptation in line with inflation of minimum amounts of cover laid down in Directive 2009/103/EC of the European Parliament and of the Council relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability

(2018/C 233/01)

This Communication concerns the adaptation in line with inflation, for certain Member States, of minimum amounts laid down in Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability [1]. The Member States concerned are the thirteen Member States benefiting from a transitional period for the application of Directive 2009/103/EC.

In accordance with Article 9(2) of Directive 2009/103/EC, the amounts laid down in euro in Article 9(1) have been reviewed in order to take account of changes in the European index of consumer prices comprising all Member States, as published by Eurostat.

The Member States benefitting from a transitional period fall into three groups, with three different transitional periods, and therefore the calculation has been carried out separately for each group.

For the first group of Member States (Slovakia and Slovenia) the review period was from December 2011 to December 2016.

For the second group of Member States (Czech Republic, Greece and Latvia) the review period was from May 2012 to May 2017.

For the third group of Member States (Bulgaria, Estonia, Italy, Lithuania, Malta, Poland, Portugal and Romania) the review period was from June 2012 to June 2017.

As a result of the review, the amounts laid down in euro are as follows.

For the Member States for which the transition period ended in December 2011 (Slovakia and Slovenia):

— in case of personal injury, the minimum amount of cover is increased to EUR 1 050 000 per victim or EUR 5 240 000 per claim, whatever the number of victims;

— in case of material damage, the minimum amount is increased to EUR 1 050 000 per claim, whatever the number of victims.

For the Member States for which the transition period ended in May 2012 (Czech Republic, Greece and Latvia), and those for which the transition period ended in June 2012 (Bulgaria, Estonia, Italy, Lithuania, Malta, Poland, Portugal and Romania):

— in case of personal injury, the minimum amount of cover is increased to EUR 1 050 000 per victim or EUR 5 210 000 per claim, whatever the number of victims;

[1] OJ L 263, 7.10.2009, p. 11.

— in case of material damage, the minimum amount is increased to EUR 1 050 000 per claim, whatever the number of victims.

For other Member States, for which Directive 2009/103/EC entered into application with no transitional period, the minimum amounts were already revised in 2016 ([1]).

([1]) Commission Communication COM(2016) 246 of 10 May 2016.

Non-opposition to a notified concentration

(Case M.8416 — The Priceline Group/Momondo Group Holdings)

(Text with EEA relevance)

(2018/C 233/02)

On 17 July 2017, the Commission decided not to oppose the above notified concentration and to declare it compatible with the internal market. This decision is based on Article 6(1)(b) of Council Regulation (EC) No 139/2004 ([1]). The full text of the decision is available only in English and will be made public after it is cleared of any business secrets it may contain. It will be available:

— in the merger section of the Competition website of the Commission (http://ec.europa.eu/competition/mergers/cases/). This website provides various facilities to help locate individual merger decisions, including company, case number, date and sectoral indexes,

— in electronic form on the EUR-Lex website (http://eur-lex.europa.eu/homepage.html?locale=en) under document number 32017M8416. EUR-Lex is the online access to European law.

([1]) OJ L 24, 29.1.2004, p. 1.

IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN COMMISSION

Euro exchange rates ([1])

3 July 2018

(2018/C 233/03)

1 euro =

	Currency	Exchange rate		Currency	Exchange rate
USD	US dollar	1,1665	CAD	Canadian dollar	1,5344
JPY	Japanese yen	129,09	HKD	Hong Kong dollar	9,1506
DKK	Danish krone	7,4506	NZD	New Zealand dollar	1,7281
GBP	Pound sterling	0,88350	SGD	Singapore dollar	1,5921
SEK	Swedish krona	10,3123	KRW	South Korean won	1 298,07
CHF	Swiss franc	1,1573	ZAR	South African rand	15,9718
ISK	Iceland króna	124,60	CNY	Chinese yuan renminbi	7,7481
NOK	Norwegian krone	9,4655	HRK	Croatian kuna	7,3845
BGN	Bulgarian lev	1,9558	IDR	Indonesian rupiah	16 766,10
CZK	Czech koruna	26,073	MYR	Malaysian ringgit	4,7208
HUF	Hungarian forint	327,35	PHP	Philippine peso	62,249
PLN	Polish zloty	4,3915	RUB	Russian rouble	73,6468
RON	Romanian leu	4,6615	THB	Thai baht	38,681
TRY	Turkish lira	5,4444	BRL	Brazilian real	4,5429
AUD	Australian dollar	1,5761	MXN	Mexican peso	22,9451
			INR	Indian rupee	79,9310

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

Summary of European Commission Decisions on authorisations for the placing on the market for the use and/or for use of substances listed in Annex XIV to Regulation (EC) No 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)

(Published pursuant to Article 64(9) of Regulation (EC) No 1907/2006 [1])

(Text with EEA relevance)

(2018/C 233/04)

Decisions granting an authorisation

Reference of the decision [1]	Date of decision	Substance name	Holder of the authorisation	Authorisation numbers	Authorised use	Date of expiry of review period	Reasons for the decision
C(2018) 3702	27 June 2018	Bis(2-methoxyethyl) ether (diglyme) EC No: 203-924-4 CAS No 111-96-6	Merck KGaA, Frankfurter Straße 250, 64293 Darmstadt, Germany.	REACH/18/11/0	Industrial use of diglyme as solvent in the manufacturing process of cryptand intermediates for further conversion into cryptand 221 and cryptand 222.	27 June 2030	Risk is adequately controlled in accordance with Article 60(2) of Regulation (EC) No 1907/2006. There are no suitable alternatives before the sunset date.

[1] The decision is available on the European Commission website at: http://ec.europa.eu/growth/sectors/chemicals/reach/about/index_en.htm

[1] OJ L 396, 30.12.2006, p. 1.

Withdrawal of Commission proposals

(2018/C 233/05)

List of withdrawn proposals

Document	Interinstitutional procedure	Title
Agriculture and rural development		
COM/2017/0150	2017/068/COD	Proposal for a Regulation of the European Parliament and of the Council fixing the adjustment rate provided for in Regulation (EU) No 1306/2013 for direct payments in respect of the calendar year 2017
Economic and Financial Affairs, Taxation and Customs		
COM/2011/737	2011/333/CNS	Proposal for a Council Regulation on the methods and procedure for making available the own resource based on the value added tax
COM/2014/43	2014/0020/COD	Proposal for a Regulation of the European Parliament and of the Council on structural measures improving the resilience of EU credit institutions
Foreign Affairs and Security Policy		
COM/2003/695	CNS 2003/0268	Proposal for a Council Decision on the conclusion of a Political Dialogue and Cooperation Agreement between the European Community and its Member States, of the one part, and the Andean Community and its member countries, the Republics of Bolivia, Colombia, Ecuador, Peru and the Bolivarian Republic of Venezuela, of the other part
COM/2014/360	2014/0182/NLE	Proposal for a Council Decision on the Union position with the Cooperation Council established by the European Union –Georgia Partnership and Cooperation Agreement between the European Community and its Member States, of the one part, and Georgia, of the other part with regard to the adoption of a Recommendation on the implementation of the EU-Georgia Association Agenda
COM/2014/359	2014/0181/NLE	Proposal for a Council Decision on the Union's position in the Cooperation Council established by the Partnership and Cooperation Agreement between the European Community and its Member States on the one hand and the Republic of Moldova on the other, with regard to adopting a Recommendation on implementing the EU-Moldova Association Agenda
JOIN/2013/014	2013/0149/NLE	Joint Proposal for a Council Decision on the Union position within the Association Council established by the Euro-Mediterranean agreement establishing an Association between the European Community and its Member States, of the one part, and the Republic of Lebanon, of the other part with regard to the adoption of a Recommendation on the implementation of the second EU-Lebanon ENP Action Plan

Document	Interinstitutional procedure	Title
		Internal Market, Industry, Entrepreneurship and SMEs
COM/2012/164	2012/82/COD	Proposal for a Regulation of the European Parliament and of the Council simplifying the transfer of motor vehicles registered in another Member State within the Single Market
		International Cooperation and Development
COM/2011/0861	2011/0420/NLE	Proposal for a Council Decision on EU accession to the International Cotton Advisory Committee (ICAC)
		Justice, Consumers and Gender Equality
COM/2014/0212	2014/0120/COD	Proposal for a Directive of the European Parliament and of the Council on single-member private limited liability companies
		Maritime Affairs and Fisheries
COM/2011/0760	2011/0345/COD	Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1300/2008 of 18 December 2008 establishing a multi-annual plan for the stock of herring distributed to the west of Scotland and the fisheries
COM/2013/09	2013/0007/COD	Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1224/2009 establishing a Community control system for ensuring compliance with the rules of the Common Fisheries Policy
		Migration, Home Affairs and Citizenship
COM/2014/163	2014/0095/COD	Proposal for a Regulation of the European Parliament and of the Council establishing a touring visa and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 562/2006 and (EC) No 767/2008
COM/2014/164	2014/0094/COD	Proposal for a Regulation of the European Parliament and of the Council on the Union Code on Visas (Visa Code)
		Transport
COM/2013/409	2013/0187/COD	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 216/2008 in the field of aerodromes, air traffic management and air navigation services

EUROPEAN DATA PROTECTION SUPERVISOR

Summary of EDPS Opinion on online manipulation and personal data

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

(2018/C 233/06)

The digitisation of society and the economy is having a mixed impact on civic engagement in decision-making and on the barriers to public involvement in democratic processes.

Big data analytics and artificial intelligence systems have made it possible to gather, combine, analyse and indefinitely store massive volumes of data. Over the past two decades, a dominant business model for most web-based services has emerged which relies on tracking people online and gathering data on their character, health, relationships and thoughts and opinions with a view to generating digital advertising revenue. These digital markets have become concentrated around a few companies that act as effective gatekeepers to the internet and command higher inflation-adjusted market capitalisation values than any companies in recorded history.

This digital ecosystem has connected people across the world with over 50 % of the population on the internet, albeit very unevenly in terms of geography, wealth and gender. The initial optimism about the potential of internet tool and social media for civic engagement has given way to concern that people are being manipulated, first through the constant harvesting of often intimate information about them, second through the control over the information they see online according to the category they are put into. Viral outrage for many algorithm-driven services is a key driver of value, with products and applications that are designed to maximise attention and addiction. Connectedness, at least under the current model, has lead to division.

The ensuing debate has revolved around the misleading, false or scurrilous information ('content') served to people with the intention of influencing political discourse and elections, a phenomenon come to be labelled 'fake news' or 'online disinformation'. Solutions have focused on transparency measures, exposing the source of information while neglecting the accountability of players in the ecosystem who profit from harmful behaviour. Meanwhile market concentration and the rise of platform dominance present a new threat to media pluralism. For the EDPS, this crisis of confidence in the digital ecosystem illustrates the mutual dependency of privacy and freedom of expression. The diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy. This Opinion is therefore concerned with the way personal information is used in order to micro-target individuals and groups with specific content, the fundamental rights and values at stake, and relevant laws for mitigating the threats.

The EDPS has for several years argued for greater collaboration between data protection authorities and other regulators to safeguard the rights and interests of individuals in the digital society, the reason we launched in 2017 the Digital Clearinghouse. Given concerns that political campaigns may be exploiting digital space in order to circumvent existing laws ([1]), we believe that it is now time for this collaboration to be extended to electoral and audiovisual regulators.

1. WHY ARE WE PUBLISHING THIS OPINION

i. Intense ongoing public debate

There is currently an intense public debate about the impact of today's vast and complex ecosystem of digital information on not only the market economy but also on the political economy, how the political environment interacts with the economy. The major platforms sit at the centre of this ecosystem, gaining disproportionately from the growth in digital advertising, and are increasing their relative power as it evolves. Personal data is needed to segment, to target and to customise messages served to individuals, but most advertisers are unaware of how such decisions are taken and most individuals are unaware of how they are being used. The system rewards sensational and viral content and does

([1]) See, for instance, http://www.independent.co.uk/news/uk/politics/election-2017-facebook-ads-marginal-seats-tories-labour-outdated-election-spending-rules-a7733131.html [accessed 18.3.2018].

not in general distinguish between advertisers, whether commercial or political. Revelations of how deliberate disinformation ('fake news') has been propagated via this system have led to fears that the integrity of democracies may be under threat. Artificial Intelligence systems — the market for which is also characterised by concentration – are themselves powered by data and will — if unchecked — increase the remoteness and unaccountability of the decision-making in this environment.

ii. **Relevance of data protection law and political campaigns**

The fundamental rights to privacy and to data protection are clearly a crucial factor in remedying this situation, which makes this issue a strategic priority for all independent data protection authorities. In their 2005 *Resolution on the Use of Personal Data for Political Communication,* data protection regulators articulated worldwide key data protection concerns related to the increased processing of personal data by non-commercial actors. It referred specifically to the processing of 'sensitive data related to real or supposed moral and political convictions or activities, or to voting activities' and 'invasive profiling of various persons who are currently classified — sometimes inaccurately or on the basis of a superficial contact — as sympathizers, supporters, adherents or party' ([1]). The international Resolution called for data protection rules on data minimisation, lawful processing, consent, transparency, data subjects rights, purpose limitation and data security to be more rigorously enforced. It may now be time for this call to be renewed.

EU law on data protection and confidentiality of electronic communications apply to data collection, profiling and microtargeting, and if correctly enforced should help minimise harm from attempts to manipulate individuals and groups. Political parties processing voter data in the EU fall within the scope of the GDPR. The GDPR defines personal data revealing political opinions as special categories of data. Processing such data is generally prohibited unless one of the enumerated exemptions applies. In the context of political campaigning, the following two exemptions are particularly relevant and merit full citation:

'(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject; […].

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

Recital 56 clarifies para 9(2)(g): '[w]here in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established'.

Several data protection authorities have developed rules or guidelines on data processing for political purposes:

— In March 2014, the Italian Data Protection Authority adopted rules on processing of personal data by political parties. The rules highlighted the general prohibition to use personal data made public on the internet, such as on social networks or forums, for the purposes of political communication, if this data was collected for other purposes ([2]).

— In November 2016, the French National Data Protection Commission (CNIL) provided additional guidelines to its 2012 recommendations on political communication, specifying the rules for processing of personal data on social networks. In particular, CNIL underlined that aggregation of personal data of voters in order to profile and target them on social networks can only be lawful if based on the consent as a ground for data processing ([3]).

([1]) Resolution available here https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf [accessed 18.3.2018].

([2]) http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267 'Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale' published in the Official Gazette of the Italian Data Protection Authority number 71 on 26.3.2014 [doc. web n. 3013267].

([3]) https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux 'Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?' published by the Commission Nationale de l'informatique et des libertés (French National Commission of Informatics and Liberty) 8.11.2016.

— In April 2017, the UK Information Commissioner's Office (ICO) issued updated *Guidance on political campaigning*, which also included guidelines on the use of data analytics in political campaigning. ICO explained that when a political organization commissions a third party company to carry out analytics, then that company is likely to be a data processor, whereas the organization – a controller. Specific provisions of the data protection law governing controller-processor relationship have to be accounted for, in order for the processing to be lawful ([1]).

The guidelines of the national data protection authorities have a potential of providing additional authoritative interpretation of data protection and privacy law provisions, which account for the differences in the organisation of national political systems ([2]).

iii. **The purpose of this EDPS Opinion**

The EDPS vision is to help the EU lead by example in the global dialogue on data protection and privacy in the digital age by identifying cross-disciplinary policy solutions to the Big Data challenges and developing an ethical dimension to processing of personal information ([3]). We have called for the data subject to be treated 'as an individual not simply as a consumer or user' and highlighted ethical issues around the effects of predictive profiling and algorithm-determined personalisation ([4]). We have called for responsible and sustainable development of the digital society based on individual control over personal data concerning them, privacy-conscious engineering and accountability and coherent enforcement ([5]). The EDPS Ethics Advisory Group in its January 2018 report noted that 'microtargeting of electoral canvassing changes the rules of public speech, reducing the space for debate and interchange of ideas,' which 'urgently requires a democratic debate on the use and exploitation of data for political campaign and decision-making' ([6]).

This issue of using information and personal data to manipulate people and politics goes of course well beyond the right to data protection. A personalised, microtargeted online environment creates 'filter-bubbles' where people are exposed to 'more-of-the-same' information and encounter fewer opinions, resulting in increased political and ideological polarisation ([7]). It increases the pervasiveness and persuasiveness of false stories and conspiracies ([8]). Research suggests that the manipulation of people's newsfeed or search results could influence their voting behaviour ([9]).

The EDPS's concern is to help ensure the processing of personal data, in the words of the GDPR, serves mankind, and not vice versa ([10]). Technological progress should not be impeded but rather steered according to our values. Respect for fundamental rights, including a right to data protection, is crucial to ensure the fairness of the elections, particularly as we

([1]) https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office 'Guidance on political campaigning' [20170426].

([2]) According to Article 57(1)(d) of the GDPR, each supervisory authority shall on its territory […] promote the awareness of controllers and processors of their obligations under this Regulation.

([3]) See Leading by Example: The EDPS Strategy 2015-2019, p. 17. 'Big data', in our view, 'refers to the practice of combining huge volumes of diversely sourced information and analysing them, often using self-learning algorithms to inform decisions. One of the greatest values of big data for businesses and governments is derived from the monitoring of human behaviour, collectively and individually, and resides in its predictive potential; EDPS Opinion 4/2015, Towards a new digital ethics: Data, dignity and technology, 11.9.2015, p. 6.

([4]) Profiles used to predict people's behaviour risk stigmatisation, reinforcing existing stereotypes, social and cultural segregation and exclusion, with such 'collective intelligence' subverting individual choice and equal opportunities. Such 'filter bubbles' or 'personal echo-chambers' could end up stifling the very creativity, innovation and freedoms of expression and association which have enabled digital technologies to flourish; EDPS Opinion 4/2015, p. 13 (references omitted).

([5]) EDPS Opinion 7/2015 Meeting the challenges of big data, p. 9.

([6]) Report of the EDPS Ethics Advisory Group, January 2018, p. 28.

([7]) See for example The Economist, How the World Was Trolled (November 4-10, 2017), Vol. 425, No 9065, pp. 21-24.

([8]) Allcott H. and Gentzkow M., Social Media and Fake News in the 2016 Election (Spring 2017). Stanford University, Journal of Economic Perspectives, Vol. 31, No 2, pp. 211-236. https://web.stanford.edu/~gentzkow/research/fakenews.pdf, p. 219.

([9]) In one of the experiments, social platform users were told how their friends had said they had voted, which prompted statistically significant increase of segment of the population (0,14 % of the voting age population or about 340 000 voters) to vote in the congressional mid-term elections in 2010; Allcott H. and Gentzkow M., Social Media and Fake News in the 2016 Election (Spring 2017), Stanford University, Journal of Economic Perspectives, Vol. 31, No 2, pp. 211-236., p. 219) In another study, the researchers claimed that differences in Google search results were capable of shifting voting preferences of undecided voters by 20 %; Zuiderveen Borgesius, F. & Trilling, D. & Möller, J. & Bodó, B. & de Vreese, C. & Helberger, N. (2016). Should we worry about filter bubbles? Internet Policy Review, 5(1). DOI: 10.14763/2016.1.401, p. 9.

([10]) Recital 4 to 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, hereinafter 'GDPR'.

approach the European Parliament elections of 2019 ([1]). This Opinion is the latest in a series of broad engagements by EDPS on the question of how data protection should be applied to address the most pressing public policy concerns. It builds on the previous EDPS work on Big Data and digital ethics and the need to coordinate regulation of competitive and fair markets ([2]). The Opinion will first summarise the process whereby personal data fuels and determines the prevailing cycle of digital tracking, microtargeting and manipulation. It will then consider the roles of the various players in the digital information ecosystem. It will consider the fundamental rights at stake, the relevant data protection principles and other relevant legal obligations. It will conclude by recommending that the problem of online manipulation is only likely to worsen, that no single regulatory approach will be sufficient on its own, and that regulators therefore need to collaborate urgently to tackle not only localised abuses but also both the structural distortions caused by excessive market concentration.

7. **CONCLUSION**

Online manipulation poses a threat to society because filter bubbles and walled communities make it harder for people to understand each other and share experiences. The weakening of this 'social glue' may undermine democracy as well as several other fundamental rights and freedoms. Online manipulation is also a symptom of the opacity and lack of accountability in the digital ecosystem. The problem is real and urgent, and is likely to get worse as more people and things connect to the internet and the role of Artificial Intelligence systems increases. At the root of the problem is partly the irresponsible, illegal or unethical use of personal information. Transparency is necessary but not enough. Content management may be necessary but cannot be allowed to compromise fundamental rights. Part of the solution, therefore, is to enforce existing rules especially the GDPR with rigour and in tandem with other norms for elections and media pluralism.

As a contribution to advancing the debate, in spring 2019, EDPS will convene a workshop where national regulators in the area of data protection, electoral and audiovisual law will be able to explore these interplays further, discuss the challenges they are facing and consider opportunities for joint actions, also taking into consideration the upcoming European Parliament elections.

This Opinion has argued that technology and behaviour in the market is causing harm because of structural imbalances and distortions. We have called for adjusting the incentives to innovate. The tech giants and pioneers have benefited until now from operating in a relatively unregulated environment. Traditional industries and basic concepts of territorial jurisdiction, sovereignty and also social norms including democracy are affected. These values depend on a plurality of voices, and equilibrium between parties. No single player or sector can tackle this alone. Protection of data is part of the solution and perhaps a bigger part than expected. It is not enough to rely on the good will of ultimately unaccountable commercial players. We need now to intervene in the interests of spreading more fairly the benefits of digitisation.

Brussels, 19 March 2018.

Giovanni BUTTARELLI

European Data Protection Supervisor

([1]) As stated by the European Court of Human Rights in the case of Orlovskaya Iskra v. Russia, 'Free elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system. The two rights are inter-related and operate to reinforce each other: for example, freedom of expression is one of the "conditions" necessary to "ensure the free expression of the opinion of the people in the choice of the legislature". For this reason, it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely. In the context of election debates, the unhindered exercise of freedom of speech by candidates has particular significance' (references omitted from the text), para. 110. http://hudoc.echr.coe.int/eng?i=001-171525.

([2]) 2014 — Preliminary Opinion on 'Privacy and Competitiveness in the Age of Big Data'; 2015 — Opinion 4/2015 Towards a new digital ethics. Data, dignity and technology; 2015 — Opinion 7/2015 Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability; 2016 — Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data.

Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems

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

(2018/C 233/07)

Today's pressing challenges related to security and border management require smarter use of the information already available to competent public authorities. This has prompted the European Commission to launch a process towards the interoperability of (existing and future) EU large-scale information systems in the fields of migration, asylum and security. In December 2017, the Commission issued two Proposals for regulations that would establish a legal framework for interoperability between EU large-scale information systems.

Interoperability, provided that it is implemented in a well-thought manner and in full compliance with the fundamental rights, including the rights to privacy and to data protection may be a useful tool to address legitimate needs of competent authorities using large-scale information systems and to contribute to the development of effective and efficient information sharing. Interoperability is not only or primarily a technical choice but rather a political choice liable to have profound legal and societal consequences that cannot be hidden behind allegedly technical changes. The decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a 'point of no return'.

While interoperability might have been envisaged initially as a tool to only facilitate the use of the systems, the Proposals would introduce new possibilities to access and use the data stored in the various systems in order to combat identity fraud, facilitate identity checks, as well as streamline access to non-law information systems by law enforcement authorities.

In particular, the Proposals create a new centralised database that would contain information about millions of third-country nationals, including their biometric data. Due to its scale and the nature of the data to be stored in this database, the consequences of any data breach could seriously harm a potentially very large number of individuals. If such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights. It is therefore essential to build strong legal, technical and organizational safeguards. Special vigilance is also required both as regards the purposes of the database as well as its conditions and modalities of use.

In this context, the EDPS stresses the importance of further clarifying the extent of the problem of identity fraud among third-country nationals, in order to ensure that the measure proposed is appropriate and proportionate. The possibility to consult the centralized database to facilitate identity checks on the territory of the Member States should be framed more narrowly.

The EDPS understands the need for law enforcement authorities to benefit from the best possible tools to quickly identify the perpetrators of terrorist acts and other serious crimes. However, facilitating the access by law enforcement authorities to non-law enforcement systems (i.e. to information obtained by authorities for purposes other than law enforcement), even to a limited extent, is far from insignificant from a fundamental rights perspective. Routine access would indeed represent a serious violation of the principle of purpose limitation. The EDPS therefore calls for the maintenance of genuine safeguards to preserve fundamental rights of third country nationals.

Finally the EDPS would like to stress that both in legal and technical terms, the Proposals add another layer of complexity to the existing systems, as well as those that are still in the pipeline with precise implications that are difficult to assess at this stage. This complexity will have implications not only for data protection, but also for governance and supervision of the systems. The precise implications for the rights and freedoms which are at the core of the EU project are difficult to fully assess at this stage. For these reasons, the EDPS calls for a wider debate on the future of the EU information exchange, their governance and the ways to safeguard fundamental rights in this context.

1. INTRODUCTION

1.1. Background

1. In April 2016, the Commission adopted a Communication *Stronger and Smarter Information Systems for Borders and Security* ([1]) initiating a discussion on how information systems in the European Union could better enhance border management and internal security.

2. In June 2016, as a follow-up of the Communication, the Commission set up a high-level expert group on information systems and interoperability ('HLEG'). The HLEG was tasked to address legal, technical and operational challenges to achieving interoperability between central EU systems for borders and security ([2]).

3. The HLEG presented recommendations first in its interim report of December 2016 ([3]), and later in its final report of May 2017 ([4]). The EDPS was invited to take part in the works of the HLEG and issued a statement on the concept of interoperability in the field of migration, asylum and security which is included in the final report of the HLEG.

4. Building on the Communication of 2016 and the recommendations of the HLEG, the Commission proposed a new approach where all centralised EU information systems for security, border and migration management would be interoperable ([5]). The Commission announced its intention to work towards creating a European search portal, a shared biometric matching service and a common identity repository.

5. On 8 June 2017, the Council welcomed the Commission's view and the proposed way forward to achieve the interoperability of information systems by 2020 ([6]). On 27 July 2017, the Commission launched a public consultation on the interoperability of EU information systems for borders and security ([7]). The consultation was accompanied by an inception impact assessment.

6. On 17 November 2017, as an additional contribution, the EDPS issued a reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice ([8]). In this paper he recognised that interoperability, when implemented in a well thought-out-manner and in compliance with the core requirements of necessity and proportionality, may be a useful tool to address legitimate needs of competent authorities using large scale information systems including improve information sharing.

7. On 12 December 2017, the Commission published two legislative proposals ('the Proposals') for:

— a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226, hereinafter 'Proposal on borders and visa'.

— a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police, and judicial cooperation, asylum and migration) hereinafter 'Proposal police and judicial cooperation, asylum and migration'.

([1]) Communication from the Commission to the European Parliament and the Council on Stronger and Smarter Information Systems for Borders and Security, 6.4.2017, COM (2016) 205 final.
([2]) Idem, p. 15.
([3]) Interim report by the chair of the high-level expert group on information systems and interoperability set up by the European Commission, Interim report by the chair of the high-level expert group, December 2016, available at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435.
([4]) Final report of the high-level expert group on information systems and interoperability set up by the European Commission, 11 May 2017; available at http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435.
([5]) Communication of 16.5.2017 from the Commission to the European Parliament, the European Council and the Council, Seventh progress report towards an effective and genuine Security Union, COM(2017) 261 final.
([6]) Council conclusions on the way forward to improve information exchange and ensure the interoperability of EU information systems, 8 June 2017: http://data.consilium.europa.eu/doc/document/ST-10151-2017-INIT/en/pdf.
([7]) The public consultation and the impact assessment are available at: https://ec.europa.eu/home-affairs/content/consultation-interoperability-eu-information-systems-borders-and-security_en.
([8]) https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf.

1.2. **Objectives of the Proposals**

8. The Proposals aim in general at improving the management of the Schengen external borders and at contributing to the internal security of the European Union. To this end, they establish a framework to ensure the interoperability between existing and future EU large scale information systems in the areas of border checks, asylum and immigration, police cooperation and judicial cooperation in criminal matters.

9. The interoperability components established by the Proposals would cover:

— Three existing systems: the Schengen Information System (SIS), the Eurodac system and the Visa Information System (VIS);

— Three proposed systems that are still in preparation or development:

— one that has recently been agreed on by the EU legislators and needs to be developed: the Entry/Exit System (EES) ([1]) and,

— two that are still under negotiations: the proposed European Travel Information and Authorisation System (ETIAS) ([2]), and the proposed European Criminal Records Information System for third-country nationals (ECRIS-TCN) ([3]);

— the Interpol's Stolen and Lost Travel Documents (SLTD) database and

— Europol data ([4]).

10. The interoperability between these systems consists of four components:

— A European search portal ('ESP'),

— A shared biometric matching service ('shared BMS'),

— A common identity repository ('CIR') and,

— A multiple identity detector ('MID').

11. The ESP would work as a message broker. Its purpose is to provide a simple interface that would provide fast query results in a transparent way. It would enable the simultaneous query of the different systems using identity data (both biographical and biometric). In other words, the end-user would be able to carry out a single search and receive results from all the systems he/she is authorised to access rather than searching each system individually.

12. The shared BMS would be a technical tool to facilitate the identification of an individual who may be registered in different databases. It would store templates of the biometric data (fingerprints and facial images) contained in the EU centralised information systems (i.e. the SIS, the Eurodac system, the EES, the VIS and the ECRIS-TCN). It would enable on the one hand, to simultaneously search biometric data stored in the different systems and on the other hand, to compare these data.

13. The CIR would facilitate the identification of persons including on the territory of Member States and also help streamlining the access by law enforcement authorities to non-law information systems. The CIR would store biographical and biometric data recorded in the VIS, the ECRIS-TCN, the EES, the Eurodac system and the ETIAS). It would store the data — logically separated — according to the system from which the data was originated.

([1]) Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

([2]) Proposal for a Regulation of the European parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, COM(2016) 731 final, 16.11.2016.

([3]) Proposal for a Regulation of the European Parliament and of the Council establishing a centralized system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRIS-TCN system) and amending Regulation (EU) No 1077/2011, COM(2017) 344 final, 29.6.2017.

([4]) 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 (OJ L 135, 24.5.2016, p. 53).

14. The MID would be a tool that would allow to link identities within the CIR and the SIS and would store links between records. It would store links providing information when one or more definite or possible match(es) is(are) detected and/or when a fraud identity is used. It would check whether queried or input data exists in more than one of the systems to detect multiple identities (e.g. same biometric data linked to different biographical data or same/similar biographical data linked to different biometric data). The MID would show the biographical identity records that have a link in the different systems.

15. Through the four interoperability components, the Proposals aim at:

— providing authorised users with fast, seamless, systematic and controlled access to relevant information systems,

— facilitating identity checks of third country nationals on the territory of Member States,

— detect multiple identities linked to the same set of data and,

— streamline the access of law enforcement authorities to non-law enforcement information systems.

16. In addition, the Proposals would establish a central repository for reporting and statistics ('CRRS'), the Universal Message Format ('UMF') and would introduce automated data quality control mechanisms.

17. The publication of two legislative proposals instead of one results from the need to respect the distinction between systems that concern:

— the Schengen *acquis* regarding borders and visas (i.e. the VIS, the EES, the ETIAS and the SIS as regulated by Regulation (EC) No 1987/2006),

— the Schengen *acquis* on police cooperation or that are not related to the Schengen *acquis* (the Eurodac system, the ECRIS-TCN and the SIS as regulated by Council Decision 2007/533/JHA).

18. The two Proposals are 'sister proposals' that have to be read together. The numbering of the Articles is mainly similar in both proposals as is their content. Therefore, unless otherwise specified, when we mention a specific Article, this Article is referring to the one of both proposals.

5. **CONCLUSIONS**

142. The EDPS recognises that interoperability, when implemented in a well thought-out manner and in compliance with the core requirements of necessity and proportionality, may be a useful tool to address legitimate needs of competent authorities using large scale information systems including improve information sharing.

143. He stresses that interoperability is not primarily a technical choice, it is first and foremost a political choice to be made, with significant legal and societal implications in the years to come. Against the backdrop of the clear trend to mix distinct EU law and policy objectives (i.e. border checks, asylum and immigration, police cooperation and now also judicial cooperation in criminal matters), as well as granting law enforcement routine access to non-law enforcement databases, the decision of the EU legislator to make large-scale IT systems interoperable would not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a 'point of no return'. For these reasons, the EDPS calls for a wider debate on the future of the EU information exchange, their governance and the ways to safeguard fundamental rights in this context.

144. Although the Proposals as presented could give the impression of interoperability as the final component of already fully functioning information systems (or at least systems the legal founding acts of which are already 'stable' and in the final stages of the legislative process), the EDPS wishes to recall that this is not the case. In reality, three of the six EU information systems the Proposals seek to interconnect do not exist at the moment (ETIAS, ECRIS-TCN and EES), two are currently under revision (SIS and Eurodac) and one is to be revised later this year (VIS). Assessing the precise implications for privacy and data protection of a very complex system with so many 'moving parts' is all but impossible. The EDPS recalls the importance to ensure consistency between the legal texts already under negotiation (or upcoming) and the Proposals in order to ensure a unified legal, organizational and technical environment for all data processing activities within the Union. In this context, he would like to stress that this Opinion is without prejudice to further interventions that may follow as the various interlinked legal instruments progress through the legislative process.

145. The EDPS notes that while interoperability might have been envisaged initially as a tool to only facilitate the use of the systems, the Proposals introduce new possibilities to access and use the data stored in the various systems in order to combat identity fraud, facilitate identity checks and streamline access by law enforcement authorities to non-law information systems.

146. As already stressed in his reflection paper, the EDPS stresses the importance of first further clarifying the extent of the problem of identity fraud among third-country nationals so as to ensure that the measure proposed is appropriate and proportionate.

147. As regards the use of the data stored in the various systems to facilitate identity checks on the territories of the Member States, the EDPS highlights that the purposes of such use, i.e. combating irregular migration and contributing to a high level of security are formulated too broadly and should be 'strictly restricted' and 'precisely defined' in the Proposals so as to comply with the case law of the Court of Justice of the European Union. He considers in particular that access to the CIR to establish the identity of a third country national for purposes of ensuring a high level of security should only be allowed where access for the same purposes to similar national databases (e.g. register of nationals/residents etc.) exist and under the same conditions. He recommends to make this clear in the Proposals. Otherwise, the Proposals would appear to establish a presumption that third country nationals constitute by definition a security threat. He also recommends to ensure that access to the data to identify a person during an identity check would be allowed:

— in principle, in the presence of the person and,

— where he or she is unable to cooperate and does not have document establishing his/her identity or,

— refuses to cooperate or,

where there are justified or well-founded grounds to believe that documents presented are false or that the person is not telling the truth about his/her identity.

148. The EDPS understands the need for law enforcement authorities to benefit from the best possible tools to quickly identify the perpetrators of terrorist acts as other serious crimes. However, removing genuine safeguards introduced to preserve fundamental rights mainly in the interest of speeding up a procedure would not be acceptable. He therefore recommends to add in Article 22(1) of the Proposals the conditions related to the existence of reasonable grounds, the carrying out of a prior search in national databases and the launching of a query of the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA, prior to any search in the common repository for identity. In addition, he considers that the compliance with the conditions of access to even limited information such as a hit/no hit should always be verified, independently of further access to the data stored in the system that triggered the hit.

149. The EDPS considers that the necessity and the proportionality of the use of the data stored in the ECRIS-TCN to detect multiple identities and to facilitate identity checks should be more clearly demonstrated, and require clarification also with regard to its compatibility with the purpose limitation principle. He therefore recommends to ensure in the Proposals that the data stored in the ECRIS- TCN could be accessed and used solely for the purposes of the ECRIS TCN as defined in its legal instrument.

150. The EDPS welcomes that the Proposals aim at the creation of a harmonized technical environment of systems that will work together to provide fast, seamless, controlled, and systematic access to the information the various stakeholders need to perform their tasks. He recalls that the fundamental data protection principles should be taken into account during all stages of the implementation of the Proposals and consequently recommends to include in the Proposals the obligation for eu-LISA and the Member States to follow the principles of data protection by design and by default.

151. Beyond the general comments and key issues identified above, the EDPS has additional recommendations related to the following aspects of the Proposals:

— the functionality of the ESP, the shared BMS, the CIR and the MID,

— the data retention periods in the CIR and the MID,

— the manual verification of links,

— the central repository for reporting and statistics,

— the division of roles and responsibility between eu-LISA and the Member States,

— the security of the interoperability components,

— the data subjects' rights,

— the access by eu-LISA staff

— the transitional period,

— the logs and

— the role of the national supervisory authorities and the EDPS.

152. The EDPS remains available to provide further advice on the Proposals, also in relation to any delegated or implementing act adopted pursuant to the proposed Regulations which might have an impact on the processing of personal data.

Brussels, 19 March 2018.

Giovanni BUTTARELLI

European Data Protection Supervisor

NOTICES FROM MEMBER STATES

Commission notice pursuant to Article 17(5) of Regulation (EC) No 1008/2008 of the European Parliament and of the Council on common rules for the operation of air services in the Community

Invitation to tender in respect of the operation of scheduled air services in accordance with public service obligations

(Text with EEA relevance)

(2018/C 233/08)

Member State	France
Route concerned	Agen-Paris (Orly)
Period of validity of the contract	From 7 January 2019 to 6 January 2023
Deadline for the submission of applications and tenders	10 September 2018 (12.00, local time)
Address where the text of the invitation to tender and any relevant information and/or documentation relating to the public tender and the public service obligation can be obtained	Syndicat Mixte pour l'Aérodrome Départemental (SMAD) Aéroport d'Agen La Garenne 47520 Le Passage FRANCE Tel. +33 553770083 Email: m.bertaud@aeroport-agen.fr Or on the platform containing SMAD's buyer profile: https://www.e-marchespublics.fr

V

(Announcements)

PROCEDURES RELATING TO THE IMPLEMENTATION OF COMPETITION POLICY

EUROPEAN COMMISSION

Prior notification of a concentration

(Case M.8891 — Puig/BSH/Noustique)

Candidate case for simplified procedure

(Text with EEA relevance)

(2018/C 233/09)

1. On 26 June 2018, the Commission received notification of a proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004 ([1]).

This notification concerns the following undertakings:

— Puig International, S.A. ('Puig International', Switzerland), controlled by Puig, S.L.,

— BSH Hausgeräte GmbH ('BSH', Germany), controlled by Robert Bosch GmbH ('Bosch'),

— Noustique Perfumes, S.L. ('Noustique', Spain).

Puig International and BSH acquire within the meaning of Article 3(1)(b) and 3(4) of the Merger Regulation joint control of Noustique.

The concentration is accomplished by way of a purchase of shares in a newly created company constituting a joint venture.

2. The business activities of the undertakings concerned are:

— for Puig International: manufacturing and distribution of fragrances and cosmetics including owned brands, such as Carolina Herrera or Nina Ricci; licenses and celebrity fragrances,

— for BSH: manufacturing and distribution of home appliances via its global brands Bosch, Siemens, Gaggenau and Neff and different local brands. Bosch supplies technology and services for the automotive, industrial technology, consumer goods (e.g. home appliances) and energy and building technology industries on a worldwide basis,

— for Noustique: joint venture for the development and promotion of a new product in the perfume sector.

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 ([2]) 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:

M.8891 — Puig/BSH/Noustique

([1]) OJ L 24, 29.1.2004, p. 1 (the 'Merger Regulation').
([2]) 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

Prior notification of a concentration

(Case M.8939 — Liberty House Group/Aluminium Dunkerque)

Candidate case for simplified procedure

(Text with EEA relevance)

(2018/C 233/10)

1. On 26 June 2018, the Commission received notification of a proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004 ([1]).

This notification concerns the following undertakings:

— Liberty Industries France (France), controlled by Liberty House Group (UK),

— Aluminium Dunkerque (France).

Liberty Industries France acquires within the meaning of Article 3(1)(b) of the Merger Regulation control of the whole of Aluminium Dunkerque.

The concentration is accomplished by way of purchase of shares.

2. The business activities of the undertakings concerned are:

— for Liberty House Group: production, trading and recycling of steel and aluminium and manufacture value added engineering products worldwide,

— for Aluminium Dunkerque: manufacture of primary aluminium in France.

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 ([2]) 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:

M.8939 — Liberty House Group/Aluminium Dunkerque

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

([1]) OJ L 24, 29.1.2004, p. 1 (the 'Merger Regulation').
([2]) OJ C 366, 14.12.2013, p. 5.

OTHER ACTS

EUROPEAN COMMISSION

Notice concerning a request pursuant to Article 35 of Directive 2014/25/EU

End of the suspension of the period for adoption of implementing acts

(2018/C 233/11)

On 2 November 2016 the Commission received a request in accordance with Article 35 of Directive 2014/25/EU of the European Parliament and of the Council [1].

This request, made by the Czech Republic, concerns certain activities in the markets for retail of electricity and gas in the Czech Republic. The relevant notices were published in OJ C 23, 24.1.2017, p. 10, in OJ C 167, 25.5.2017, p. 10, in OJ C 276, 19.8.2017, p. 4, in OJ C 396, 23.11.2017, p. 18 and in OJ C 439, 20.12.2017, p. 12.

On 21 December 2017, the Commission asked the Applicant to provide additional information by 10 January 2018 the latest. As announced in the notice published in OJ C 114, 28.3.2018, p. 20, the final deadline was prolonged by 55 working days after the receipt of complete and correct information. Complete and correct information was received on 12 April 2018.

The final deadline therefore expires on **5 July 2018**.

[1] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).

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

Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN