FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

European Union data protection reform: new fundamental rights guarantees

3rd Annual FRA Symposium
Vienna, 10 May 2012

FRA SYMPOSIUM REPORT

FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Schwarzenbergplatz 11 – 1040 Wien – Austria
Tel: +43 (1) 580 30 - 0 – Fax: +43 (1) 580 30 - 699
fra.europa.eu – information@fra.europa.eu
facebook.com/fundamentalrights
twitter.com/EURightsAgency

Contents

The 3rd annual symposium – an introduction

The 2012 Symposium of the European Union Agency for Fundamental Rights (FRA) focused on the fundamental rights dimension of the Data Protection Reform package, which the European Commission proposed on 25 January 2012.

The proposals for the data protection reform comprise three components: a Communication on Safeguarding Privacy in a Connected World: a European Data Protection Framework for the 21st century,[1] a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[2] and a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.[3]

The symposium brought together about 50 key experts from national government agencies and specialised bodies, international and non-governmental organisations, data protection authorities, universities and companies. They discussed how and to what extent the Data Protection Reform package is likely to impact on the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union (EU). Two fundamental rights of the Charter, namely Article 7 (respect for private and family life) and Article 8 (protection of personal data), were largely left aside in the symposium discussions, given that the European Data Protection Supervisor (EDPS) and the Article 29 Data Protection Working Party have already analysed the impact on these fundamental rights in their respective opinions on the data protection reform.[4] The discussions focused instead on the key topics of the proposed reform.

After welcoming remarks by FRA Director Morten Kjaerum, the keynote speeches were delivered by Marie-Helene Boulanger, Head of the European Commission's Data Protection Unit; Dimitrios Droutsas, Member of the European Parliament and European Parliament

---

1 European Commission (2012), COM(2012) 9 final, Brussels.

2 European Commission (2012), COM(2012) 11 final, Brussels.

3 European Commission (2012), COM(2012) 10 final, Brussels. For all related documents, see the Europa website: Commission proposes a comprehensive reform of the data protection rules.

4 EPDS (2012), *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7 March 2012; Article 29 Data Protection Working Group (2012), *Opinion 01/2012 on the data protection reform proposals*, 00530/12/EN WP191, 23 March 2012.

Rapporteur on the proposed Data Protection Directive; and Christian Wiese Svanberg, the Deputy Chair of the Council of the European Union Working Party on Information Exchange and Data Protection (Dapix) and member of the Danish Presidency of the EU Council. The speeches set the scene for the discussions on the three themes contained in the proposed reform:

1. the right to be forgotten and the right to data portability;
2. enhancement of the independence and powers of national data protection authorities;
3. profiling – aims, modalities and safeguards.

Each of the themes was discussed in a working group and also in the plenary concluding session. Each working group session was introduced by speakers whose presentations served to frame the group's discussions. The report will summarise the main discussion points for each of these themes.

The discussions held at the 3rd Annual FRA Symposium aimed to identify a core list of fundamental rights which are likely to be affected, either positively or negatively, by the proposed data protection rules. Awareness of the relationship between fundamental rights and these new data protection rules should help give European lawmakers a deeper understanding of the sensitivities that exist in the field of data protection. The discussion results aim at assisting both the European Parliament and the Council of the European Union as they decide on the final shape of the Data Protection Reform package. In this context, this meeting report will be communicated to relevant committees of the European Parliament, including the Civil Liberties, Justice and Home Affairs (LIBE) Committee and to the Dapix Working Party of the Council of the European Union.

The symposium programme and a list of participants are included in this report's annex.

More information about the symposium can also be found at FRA's website: http://fra.europa.eu/fraWebsite/symposium2012/.

1. The right to be forgotten and the right to data portability

- Wojciech Wiewiórowski, Inspector General for Personal Data Protection, Poland: *The right to be forgotten, the fundamental right of the person and the danger of the 'ministry of truth'*
- Vagelis Papakonstantinou, researcher, Vrije Universiteit Brussel, Belgium: *The right to data portability in the draft General Data Protection Regulation: The social networks' provision*

Summary of symposium discussions

1.1 The right to be forgotten

The first working group speaker, Mr Wiewiórowski, focused on the right to be forgotten, in other words the right to have personal data deleted, and commented on the right to data portability. Article 17 of the General Data Protection Regulation lays out the data subject's right to have his or her data forgotten and to data erasure. According to the speaker, the right to be forgotten not only relates to Article 17, but also to recitals 53 and 54. With the aim of reconciling the right to data protection and the right to freedom of expression, however, Article 80 of the Regulation provides for exemptions or derogations where the data are used solely for journalistic purposes or the purpose of artistic or literary expression. The speaker also mentioned promising practices such as the Norwegian internet site: slettmeg.no ('deleteme.no').

Promising practice

Advising on online information deletions

The Norwegian Centre for Information Security offers a web-based service called 'deleteme.no' that aims to help people who experience privacy violations online. The service, a two-year trial project launched in March 2010, offers advice and guidance via its website, telephone, email and chat services. The trial ended on 1 January 2012, with authorities concluding that there was considerable need for such services in Norway.

The service is available in Norwegian at: www.slettmeg.no.

The right to be forgotten, as enshrined in Article 17 of the draft General Data Protection Regulation, was discussed both in plenaries and during the dedicated working group session. Such a right would enjoy broad popular support. An overwhelming majority of EU citizens, 75% according to the Special Eurobarometer 359, called for this right. Since national laws cannot affect parties operating internationally, an EU-level approach is welcome. Closer cooperation between Data Protection Authorities (DPAs) and those who can erase data is needed.

Effective implementation of this right, however, raises some issues. The right to be forgotten affects several fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union.

The working group raised several challenges linked to the future implementation of the right to be forgotten. Given it is a new concept, the right to be forgotten needs to be clearly defined and its scope delineated so as not to raise false expectations. Misunderstandings have already led to lawsuits and complaints to regulators and could continue to produce ill-founded complaints.

Further, due to the nature of the internet, particularly the worldwide availability of information and its translation into different languages, the implementation of the right to be forgotten is difficult to achieve despite the best efforts of all the actors involved. This international dimension raises the question of whether the right to be forgotten should be dealt with at the national domain level or at the global, worldwide web level.

Example: An individual had asked that information be removed from a German Wikipedia page. The information was deleted from the German page, but was kept in all other language versions of the same Wikipedia page despite the individual's removal request.

Similarly, the cultural differences reflected in the diverse regulatory frameworks for freedom of expression found at the EU Member State level raise additional challenges for the uniform implementation of the right to be forgotten.

The concept of journalistic purpose, as used in Article 17 of the regulation, might also need revisiting. It needs to take into account proper guarantees of the freedom of expression, especially regarding new forms of journalism, such as blogs and social media.

The right to be forgotten, as a right attached to data protection, may also affect other fundamental rights that fall outside EU competence.

Impact on fundamental rights

The right to be forgotten is not an absolute right; Article 17 of the draft General Data Protection Regulation prescribes permissible limitations. The right to be forgotten also impacts on a variety of fundamental rights guaranteed under the EU Charter of Fundamental Rights, including, among others, the freedom of expression and information and freedom of the arts and sciences.

Possible undue censorship or revisionism raises concerns, for example, with a number of Charter rights. Article 11 of the Charter, which protects freedom of expression and information, is affected not only by the implicit link between media and the right to be forgotten, but also by the risk of individuals rewriting their own and others' histories. The freedom of arts and sciences, guaranteed in Article 13, is, for example, also relevant in this regard. National supervisory authorities could face difficult decisions when attempting to strike a balance between freedom of expression and privacy.

Potential clashes also loom between the right to be forgotten and Article 10, protecting freedom of thought, conscience and religion. Some religious communities worry that this right would enable individuals to delete or rewrite religious history.

Article 15, which protects the freedom to choose an occupation and the right to engage in work, is also relevant, particularly with regard to social networking sites. Looking at profiles job applicants may have made public is one thing, but discriminating on the grounds of gender or race – information they are likely to find on such profiles – is another matter. Therefore, job applicants want to be able to use the right to be forgotten to protect information from, and prevent potential discrimination by, future employers.

With regard to the freedom to conduct business, Article 16 raises the question of who is responsible for guaranteeing these rights: is the internet platform or the user considered the responsible party as far as putting information online is concerned? Do data controllers have the obligation to check or monitor the data? If so, how is this to be done?

Furthermore, Article 3 of the Charter, the right to personal integrity, may be affected, particularly in the case of journalists. Journalists who consider their physical safety under threat may need to exercise the right to be forgotten for their own protection.

Lastly, the rights of the child as outlined in Article 24 are also relevant, as Article 17 of the draft General Data Protection Regulation includes an emphasis on information provided by children.

1.2 The right to data portability

The second working group speaker, Mr Papakonstantinou, presented the right to data portability. This right contains two elements: the right to take your personal data elsewhere, moving it from one electronic processing system to another, and the right to get your personal data in a common electronic format. The former has been viewed as more of a consumer rights issue, and the latter can be seen as a further specification of the right to access information in the online world. Under this portability right, the data subject has the right to obtain from a controller a copy of his or her data undergoing processing, which raises several further issues: the ownership of personal data and the movement of profiles across platforms. The speaker suggested that the intent of this provision could have been achieved through a general obligation to interoperability, which refers to the ability of diverse systems to work together, and would facilitate movement across platforms. The speaker noted that the legal obligation to system interoperability is not, however, a general principle. He commented on the World Economic Forum's 'Rethinking Personal Data', which focused on functional portability.

Some question whether data protection legislation is the right vehicle for addressing consumer rights and their associated issues. The right to data portability is applicable only to data held electronically, while data protection covers information held both electronically and non-electronically. The electronic data covered by the right to data portability can, however, be delivered either in hard copy or with the use of common formats. Given the years of unresolved discussions on common formats in the EU, it is difficult to see how the legislator can address this issue. Some suggest the focus should be placed more squarely on interoperability.

Questions have also been raised about the regulation and its use of terms. If the regulation is attempting to be technology neutral, for example, then it may not be logical to include specific technological examples. Is an explicit mention of social networks meaningful? Similarly, a clarification of data ownership is needed: who exactly should be considered in control of the data – the platform or the individual user?

Impact on fundamental rights

The right to data portability impacts the freedom to conduct a business, Article 16, since it affects competition. Businesses do not want to make it easy for customers to leave and take their data with them. It is also costly for businesses, especially start-ups, to deliver interoperability and common formats.

Data portability also impacts Article 7, the respect for private and family life, and Article 8, the protection of personal data. Decisions to move one's own personal data elsewhere can, for example, affect the privacy of others whose personal data are part of the information one is moving.

In the broader context of fundamental rights, the right to data portability may be seen as a specification of the right to access information, whereas the right to be forgotten may be seen as a specification of the rights to delete and object.

Concluding remarks

Participants representing businesses, national authorities and the academic field contributed to a lively discussion on the topics of the right to be forgotten and the right to data portability. The aim of this working group session was to identify which fundamental rights, as guaranteed by the Charter of Fundamental Rights of the EU, are affected by these two rights. During the lively discussions after the presentations, the working group outlined which fundamental rights the European Commission should pay special attention to when adopting the new Data Protection Reform package, and indeed any other relevant future legislation, bearing in mind that the right to be forgotten and the right to data portability impact several fundamental rights. In addition, the European Commission should take into account the different interpretations of the right to be forgotten and the necessity of introducing the right to data portability.

2. Independence and powers of independent supervisory authorities

- Eva Souhrada-Kirchmayer, Executive Member of Data Protection Commission, Austria: *The Austrian data protection authority*
- Andrej Tomšič, Deputy Information Commissioner, Slovenia: *The Slovenian data protection authority*

Summary of symposium discussions

Keynote speakers during the plenary session underlined that a key objective of the EU Data Protection Reform package is to increase the effectiveness of data protection law in the EU and its Member States – effectiveness which is closely linked to those institutions promoting and enforcing data protection law, the national data protection supervisory authorities. This is borne out by completed FRA research on *Data Protection in the European Union: the role of national Data Protection Authorities*, as well as on-going FRA research on 'Data protection: redress mechanisms and their use'. Both show that national data protection supervisory authorities play a crucial role in the effectiveness of EU data protection law. Ms Souhrada-Kirchmayer and Mr Tomšič presented the examples of the Austrian and Slovenian authorities, drawing on examples of practice from these two EU Member States to furnish a basis for the working group's discussions.

This effectiveness depends on the public visibility, independence and the powers of the independent supervisory authorities, all of which are key issues in the EU Data Protection Reform package. In this respect, the findings of the Special Eurobarometer 359, published in June 2011, are relevant. The majority of the Europeans surveyed (63%) have not heard of any public authority responsible for protecting their rights regarding their personal data, but nine out of 10 of the Europeans surveyed (90%) think it is important for them to have common rights and protections over their personal information, regardless of the EU Member State in which it is collected and processed. As symposium participants observed, independence and the powers of national data protection supervisory authorities are also key fundamental rights issues, with particular reference to Article 8 on the protection of personal data of the EU Charter of Fundamental Rights. The working group discussed the independence of national supervisory authorities extensively during its session.

2.1 Independence and data protection authorities: case law

Case law has important ramifications for the effectiveness of data protection supervisory authorities. It has particularly addressed the issue of independence. The working group session began with introductory presentations focusing, among others, on the Austrian and Slovenian data protection supervisory authorities, in light of the Court of Justice of the European Union's (CJEU) judgment in the *European Commission v. Germany* case C-518/07. This judgment focused on German state scrutiny of regional authorities responsible for supervising the processing of data by non-public bodies. The CJEU considered this scrutiny to be incompatible with the 'complete independence' required by Directive 95/46. Similarly, the European Commission initiated a court procedure against Austria in 2010, case C-614/10, in connection with the perceived lack of independence of the Austrian federal data protection authority. As a speaker at the working group observed the Austrian case differs from the German case: while the German case covered state scrutiny, the Austrian case concerns the Federal Chancellery's administrative supervision of the Data Protection Commission. The judgment, expected in autumn/winter 2012, is being closely observed elsewhere in Europe because similar forms of administrative supervision exist in other EU Member States. Finally, participants in the working group also mentioned the infringement procedure on the independence of the Hungarian data protection authority as another case dealing with the independence of data protection authorities.

2.2 Independence and appointment procedures

The working group discussed at length the methods used for appointing chairpersons of national data protection authorities, as these have implications for the independence of the authorities. The members of the Austrian data protection commission are, for example, appointed by the federal president based on a government proposal; in Slovenia, the president appoints the head of the data protection authority based on a parliamentary proposal. Article 48 of the Draft Regulation COM(2012) 11 speaks of appointment by either parliament or by government. Within the working group, Slovenia was discussed as a potential 'promising practice' with respect to independence. The Slovenian data protection authority inspectors are independent public servants, which means that not even the head of the supervisory authority can instruct them on how to proceed with inspections. The inspectors have the authority to enter premises, demand documents and issue administrative orders and fines. The accountability of Slovenian inspectors is ensured by recourse to courts.

To reduce government influence, participants suggested involving the parliamentary opposition, since, typically, the government already reflects the parliamentary majority. Participants also suggested setting up appointment procedures on the basis of fair and transparent competition, with candidates proposing their candidacies based on clear criteria. They pointed out, however, that the EU cannot regulate the appointment in too much detail without impinging on national sovereignty. With the suggested new responsibilities for matters related to police and criminal justice under the proposal for a new Directive COM(2012) 10, the link between the supervisory authority's appointment procedure and its independence becomes even more important. Participants also suggested another mechanism for enhancing independence: establishing a one-term maximum excluding the possibility of reappointment.

Participants remarked that the issue of independence at data supervisory authorities could be compared to the experience of independence at other similar bodies, such as national human rights institutions (NHRIs) under the Paris Principles and NHRI accreditation by the International Coordinating Committee. NHRIs share many features with data protection supervisory authorities and can therefore be a good source of knowledge on the topic of independence.

2.3 Independence and resources

The link between the resources of a data protection supervisory authority and its independence stimulated considerable debate during the working group session. As with appointment procedures, EU Member States use a wide variety of methods for financing and staffing these authorities, which reflect, in part, the different constitutional and institutional positions of public administrations in different national jurisdictions. In Slovenia, for example, the supervisory authority itself proposes the budget, which the parliament then decides upon. In this context, participants stressed the importance of an independent budgetary chapter of the supervisory authority, noting that Austria had one of the smallest supervisory authorities relative to the size of its population. Participants agreed that the most crucial share of the budget goes to employee salaries to ensure sufficient human resources to carry out all the tasks entrusted to the authority, and suggested that perhaps this human resources component could be benchmarked across the EU. One proposal was to link the amount of human resources allocated to the supervisory authority to the population of the Member State. Another idea would be to tie the authority's budget to a multi-annual plan agreed upon with the government. The European Commission has launched work on guidelines on

adequate resources for supervisory authorities, but it is a difficult process as Member States may reject any strong EU intervention in their budgetary planning.

2.4 Powers in the field of the former third pillar

Participants also discussed the power of these authorities in the former third pillar of the EU and the justification for limiting their powers in relation to this area of police and judicial co-operation in criminal matters. The supervisory authorities in Austria and Slovenia already deal with the third pillar, especially police investigations. Two speakers concurred that there is little justification for any distinction of powers between the proposed Regulation COM(2012) 11 and the proposed Directive COM(2012) 10.

Concluding remarks

The working group focused on what it considered the most crucial issue of data supervisory authorities' effectiveness – their 'functional' independence, in other words, their ability to act independently. The working group considered such independence as compatible with reporting requirements, accountability and transparency, as well as with the inevitable involvement of political institutions in the appointment process. It noted that not only is the independence of regulatory bodies of all kinds pertinent to data protection supervisory authorities, but such questions of independence are a common feature of the public administration of the modern state.

Laws and resources may govern the distance between governments or parliaments and independent regulators, such as supervisory authorities, but there are other factors that influence the distance and independence a data protection authority might enjoy. The working group highlighted one important factor: the internal organisation, procedures, and professionalism of the authority, which equip it to exercise its functions effectively, consistently and in an independent manner. Another factor reflects the way in which a supervisory authority relates to 'strategic partners' in state or civil society. By forming networks of relationships with these strategic bodies, the supervisory authority would not be a lone voice in the regulation of personal data practices.

Time constraints meant that the working group could not fully explore some important matters. Perhaps the most relevant of these was the question of the effects on independence of mechanisms to enhance co-operation and consistency across EU Member States' supervisory authorities, particularly the proposed role of the European Commission within the

European Data Protection Board. Consistency and co-operation require a degree of negotiation and compromise, which would suggest possible influences that could impinge upon an authority's independence. This matter, as well as others, requires further investigation as the European Commission's new data protection package is debated and modified in the months to come.

3. Profiling – aims, modalities, safeguards

- Jörg Polakiewicz, Head of the Human Rights Policy and Development Department, Council of Europe: *Profiling – aims, modalities, safeguards*

Summary of symposium discussions

This working group brainstormed a series of ideas for further consideration with respect to profiling and the EU's data protection reform. The working group speaker focused on profiling techniques used in online advertising, where individual browsing habits are often tracked and collected without notice or permission. The participants also discussed the aims, modalities and safeguards of profiling as performed in various fields of activity.

Different features and characteristics of profiling can provide a methodology for analysis. From this framework, the working group extracted six elements as areas for discussion:

- definition of profiling;
- the subjection of profiling practices on a natural person;
- the range of data on which profiling practises are based;
- quality and effect of information provided to natural persons subjected to profiling;
- legal effects of profiling activities; and
- legal remedies available to persons being subjected to profiling.

3.1 Profiling – aims, modalities, safeguards

Within this working group, and also later in the plenary, participants agreed that profiling, for the purposes of the new data protection framework, could not be viewed as a bad practice in and of itself. Instead, to tease out the key fundamental rights issues, various participants brought up aspects worthy of further consideration, such as the varied purposes profiling is put to, specific points on the reform package and issues surrounding information technology solutions. They also pointed out that each step of the profiling process – from data collection and data mining, data computer analysis, to correlation and identification of the individual – needs to be assessed separately.

With regard to profiling's purpose, participants emphasised the importance of determining its necessity and/or proportionality, which would need to take place on a case-by-case basis for law enforcement. In contrast, representatives from the business sector underscored the need for a comprehensive approach to profiled customer data. They added that this issue should be

a priority as data-matching – the process whereby data are brought together from different sources and compared – takes place constantly and plays a crucial commercial role in many companies. Within the business sector, participants also noted that profiling serves different purposes for small- and medium-sized enterprises than for other businesses.

In addition to the many differences between the purposes of public (such as for law enforcement) and commercial data processing, participants said one also needs to distinguish between a situation in which a natural person is acting on behalf of a legal person rather than on behalf of him- or herself. In such cases, the person subjected to profiling must be provided with all information relevant to the profiling process.

With reference to the EU's proposed reform, participants underlined that the issue of profiling must be considered within the context of EU citizenship rights such as the free movement of persons. Given the relevant United Nations (UN) human rights treaties, the data protection package might need to refer to the non-discrimination principle in a wider context than in its present form.

Participants also shared the view that the definitions of profiling, as worded in the legislation, must be as clear and sound as possible. Furthermore, they agreed that the lack of specifics on the scope of the delegated acts made the European Commission's package less transparent.

The experts noted that, under the European Commission's proposals, the essential prerequisite for implementing profiling techniques and the information technology (IT) solutions supporting this implementation was the adoption of high-level safeguards against fraudulent profiling-related activities.

Participants emphasised that IT solutions should not be implemented simply because they are feasible, nor should possible IT solutions dictate policy. Furthermore, they should be applied only for the purposes for which they were designed, avoiding so-called 'function-creep'.

On the other hand, IT solutions can help to achieve desired outcomes. Data masking, for example, can ensure better proportionality of proposed measures, because it provides a higher level of personal data protection but does not pose a hurdle to those accessing the data.

Both before and after the adoption of the new data protection package, EU institutions and EU Member States authorities should invest in public awareness raising to avoid misconceptions arising concerning the use of profiling. The dissemination of public information, training and targeted education activities should help citizens to learn about profiling's characteristics as well as the scope of this package.

The financial resources stakeholders (both public and private) devote to profiling techniques was another issue thought to merit further attention. Profiling can be an expensive solution.

Concluding remarks

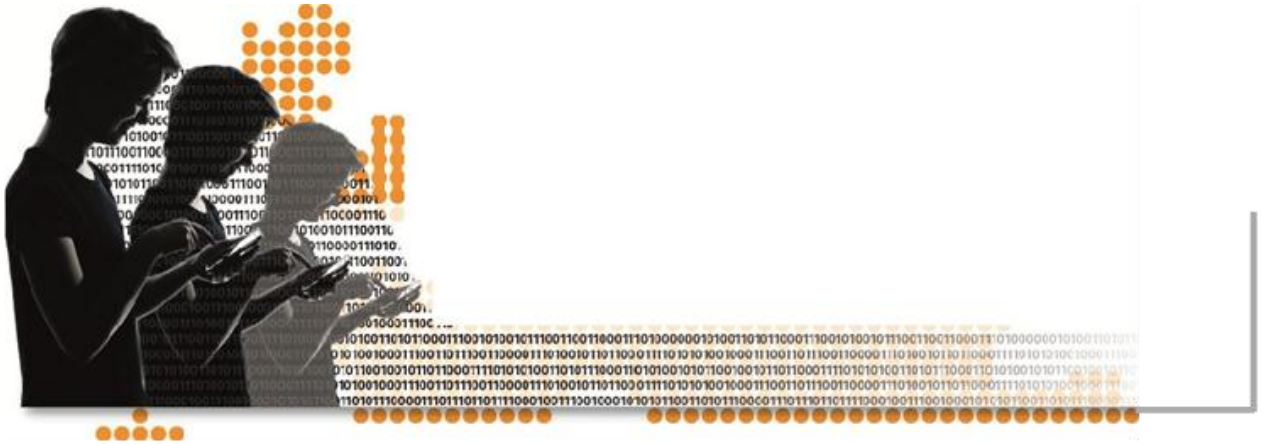
The working group came to the conclusion that profiling could not be considered a 'bad practice' in and of itself. Participants agreed that when assessing the admissibility of a given profiling technique it is important to identify what information is processed, how it is processed and how the results of that processing are used.

Time constraints prevented the experts from further in-depth exploration of the ideas considered deserving of further consideration. The working group voiced their expectation that EU decision makers would reflect further on these issues when developing legislation on the new data protection instruments.

Working group participants agreed that the right of individuals to have their personal data protected should be appropriately balanced with other rights guaranteed by the EU Charter of Fundamental Rights, on which the legislation under discussion will impact considerably, most notably on: Article 1 (human dignity); Article 10 (freedom of thought, conscience and religion); Article 11 (freedom of expression and information); Article 12 (freedom of assembly and association); Article 15 (freedom to choose an occupation and engage in work); Article 16 (freedom to conduct a business); Article 21 (non-discrimination); Article 24 (the rights of the child); Article 36 (access to services of general economic interest); Article 38 (consumer protection); Article 47 (right to an effective remedy and to a fair trial); and Article 48 (presumption of innocence and right of defence).

Annexes

Annex I – Programme



The EU data protection reform: new fundamental rights guarantees

3rd Annual FRA Symposium
Vienna, 10 May 2012

Day 1	WEDNESDAY, 9 MAY
18.00	Reception at the FRA premises
19.30	Dinner
Day 2	**THURSDAY, 10 MAY**
08.00 – 09.00	Registration
09.00 – 09.10	Welcome note by: • Morten Kjaerum, Director, FRA
09.10 – 10.00	Keynote addresses by: • Marie-Helene Boulanger, Head of Data Protection Unit, European Commission • Dimitrios Droutsas, Member of the European Parliament and its Rapporteur on the proposed Data Protection Directive • Christian Wiese Svanberg, Deputy Chair of the DAPIX Working Party, Danish Presidency of the EU Council

10.00 – 13.00	3 parallel working groups: **1. The right to be forgotten and the right of portability** Speakers: • Wojciech Wiewiórowski, Inspector General for Personal Data Protection, Poland • Vagelis Papakonstantinou, Researcher, Vrije Universiteit Brussel, Belgium Rapporteur: • Emma Butler, Senior Policy Officer, Information Commissioner's Office, United Kingdom **2. Independence and powers of independent supervisory authorities** Speakers: • Eva Souhrada-Kirchmayer, Executive Member of Data Protection Commission, Austria • Andrej Tomšič, Deputy Information Commissioner, Slovenia Rapporteur: • Charles Raab, Professor, University of Edinburgh, United Kingdom **3. Profiling – aims, modalities, safeguards** Speaker: • Jörg Polakiewicz, Head of the Human Rights Policy and Development Department, Council of Europe Rapporteur: • Filip Jasinski, Polish Representation to the EU
13.00 – 14.00	Lunch
14.00 – 15.40	Plenary: Working group presentations by rapporteurs followed by discussion
15.40 – 16.00	Concluding remarks: • Peter Hustinx, European Data Protection Supervisor

Annex II – List of participants

No	Title	Surname	Name	Institution
EU INSTITUTIONS AND BODIES				
1	Ms	Boulanger	Marie-Helene	European Commission, Directorate- General Justice, Data Protection Unit
2	Mr	Hustinx	Peter	EDPS
3	Ms	Grzybowska-Cuadrat	Katarzyna	EDPS
4	Mr	Kranenborg	Herke	EDPS
5	Ms	Kilg	Leelo	Cepol
6	Mr	Vuorensola	Sakkari	Frontex
EUROPEAN PARLIAMENT				
7	Mr	Droutsas	Dimitrios	European Parliament
8	Mr	van Ballegooij	Wouter	Greens/EFA
COUNCIL OF EUROPE				
9	Mr	Polakiewicz	Jörg	Council of Europe

MANAGEMENT BOARD				
10	Ms	Horuczi	Szilvia	National Authority for Data Protection and Freedom of Information, Hungary
11	Mr	Tretter	Hannes	Boltzmann Institut für Menschenrechte, Austria
SCIENTIFIC COMMITTEE				
12	Ms	Mustola	Kati	FRA Scientific Committee, Finland
13	Mr	McBride	Jeremy	FRA Scientific Committee, United Kingdom
MEMBER STATES (including Council negotiators)				
14	Mr	Jasinski	Filip	Polish Representation to the EU
15	Mr	Wiese Svanberg	Christian	Ministry of Justice, Denmark
16	Ms	Kisné dr. Szabó	Adrienn	Ministry of Interior, Hungary
17	Ms	Janssen	Heleen	Ministry of the Interior, Netherlands
18	Mr	Pavlin	Peter	Ministry of Justice, Slovenia
EQUALITY BODIES & NHRIs				
19	Mr	Töpfer	Eric	Deutsches Institut für Menschenrechte

CIVIL SOCIETY				
20	Mr	Schulte in den Bãumen	Tobias	European Law Institute
21	Ms	Waloszczyk	Alina	European Law Institute
22	Ms	Fiedler	Kirsten	European Digital Rights
23	Ms	Sloetjes	Janneke	Bits of Freedom
24	Ms	Szymielewicz	Katarzyna	Panotykon Foundation
25	Ms	Giraudy	Martine	REGES-FORUM
DATA PROTECTION AUTHORITIES (DPA)				
26	Mr	Tomšič	Andrej	DPA Slovenia
27	Ms	Souhrada-Kirchmayer	Eva	DPA Austria
28	Mr	Wiewiorowski	Wojciech	DPA Poland
29	Ms	Butler	Emma	DPA UK
30	Ms	de Sousa-Pereira	Sonia Cristina	DPA Portugal
31	Ms	Lankinen	Hanna	DPA Finland
32	Mr	Niederer	Stefan	DPA Germany

33	Ms	Žuffová-Kunčová	Veronika	DPA Slovakia
ACADEMIA				
34	Mr	Raab	Charles	University of Edinburgh
35	Mr	Bernal	Paul	University of East Anglia
36	Ms	Boni	Delfina	University of Milano-Bicocca
37	Mr	Schweighofer	Erich	Vienna University
38	Mr	Korff	Douwe	London Metropolitan University
39	Mr	Kloza	Dariusz	Vrije Universiteit Brussel
40	Ms	Kosta	Vasiliki	The European University Institute
BUSINESS				
41	Mr	Papakonstantinou	Vagelis	Vrije Universiteit Brussel/partner in PKpartners Law Firm in Athens
42	Ms	ChlebowskaVan Loon	Monika	Visa Europe
43	Mr.	Scheuer	Alexander	Institute of European Media Law
44	Mr.	Fleischer	Peter	Google
45	Mrs	Cseh	Gabriella	Facebook

46	Ms	Bellamy	Bojana	Accenture
47	Mr	Chappelle	Kasey	Vodafone
FRANET				
48	Mr	Meyer	Antoine	CEDRA, FRANET Partner France
49	Ms	Romanova-Bosac	Maria	CEDRA, FRANET Partner France