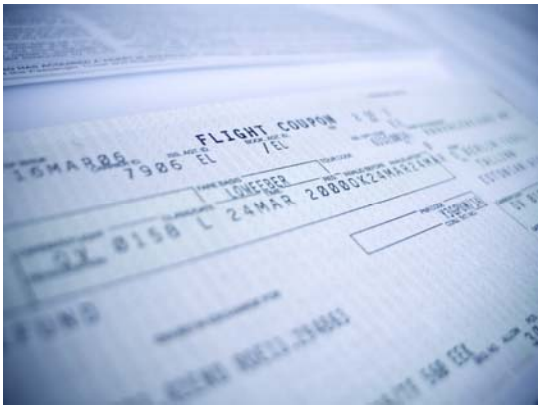
EDPS Newsletter

European Data Protection Supervisor

N° 26 | NOVEMBER 2010

CONSULTATION

> EDPS opinion on EU external strategy on Passenger Name Record



On 19 October 2010, the EDPS adopted an opinion on the Commission's communication on the transfer of Passenger Name Record (PNR) data to third countries. The Communication sets out the EU external strategy on PNR and puts forward the general principles, including a set of data protection standards, on which any PNR agreement with a third country should be based.

The EDPS welcomes the horizontal approach followed by the Commission and strongly supports the objective of achieving a high and harmonised level of data protection applicable to all existing and foreseen PNR schemes. He however expresses major concerns as regards the **necessity and legitimacy** of some important aspects of the proposed schemes. He considers in particular that the proactive use of PNR data of all passengers for risk assessment purposes requires more explicit justification and safeguards.

> ***"I welcome the horizontal approach presented by the Commission as an essential step in the direction of a comprehensive framework for the exchange of PNR data. However, to be admissible, the conditions for collection and processing of PNR***

data should be considerably restricted. I am particularly concerned about the use of PNR schemes for risk assessment or profiling. ***Peter Hustinx, EDPS***

The EDPS also underlines the need to ensure **consistency** between the various initiatives directly or indirectly related to the processing of PNR data, including the EU general framework for data protection currently under revision, the initiative to set up a PNR system for the EU, and the negotiations for an EU-US agreement on data sharing for law enforcement.

As regards the content of proposed data protection standards, the EDPS calls for **more precision** with regards to the **minimal safeguards** applicable to all PNR agreements. Stricter conditions should apply in particular to the processing of sensitive data, the conditions of onwards transfers, and the retention of data.

The EDPS also emphasises the need for any PNR agreement to explicitly provide for **directly enforceable rights** to concerned individuals.

☞ EDPS opinion (pdf)

> EDPS opinion on Information management in the area of freedom, security and justice

The opinion, adopted on 30 September 2010, relates to the Commission's communication of 20 July 2010 providing a comprehensive overview of EU instruments that regulate the collection, storage or cross-border exchange of personal data for law enforcement or migration management purposes (e.g. Schengen Information System, EURODAC and Prüm Decision on DNA data exchange). The Communication also sets out the core principles that the Commission intends to use as a benchmark for the initiation and evaluation of future policy proposals.

While welcoming and fully supporting the objectives and the main content of the Communication, the EDPS draws attention to the fact that this initiative should only be considered as a **first step** in the evaluation process. Such an exercise should be followed by further concrete measures, the outcome of which should be a well-structured, **integrated and comprehensive EU policy** on information exchange and management.

There is a need for a comprehensive policy based on a real and in-depth assessment of this area. I consider this Communication as an important first step in that direction and will follow closely further developments in this field. ***Peter Hustinx, EDPS***

The opinion also includes the following main recommendations:

- **objective and balanced assessment**: assessment of information management should not only focus on successful aspects, but also report on deficiencies and weaknesses of the systems (e.g. number of people wrongly arrested or inconvenienced following a false hit in the system);
- **alignment of data subjects' rights**: it should be ensured that citizens benefit from similar data protection rights across all different EU systems and instruments dealing with information exchange;

- **privacy and data protection assessment**: the Communication provides a good opportunity to better analyse what is meant by a "privacy and data protection assessment". Specific indicators and features should be developed to that end;

- **biometrics and system interoperability**: the EDPS invites the Commission to develop a more coherent and consistent policy on the prerequisites for use of biometrics and a policy on systems interoperability.

☞ EDPS opinion (pdf)

> EDPS opinion on the European Protection Order and European Investigation Order in criminal matters

The opinion, adopted on 5 October 2010, relates to the initiatives of a number of Member States for a Directive on the European Protection Order (EPO) (pdf) and for a Directive regarding the European Investigation Order (EIO) (pdf) in criminal matters. The aim is to improve within the EU protection of victims of criminal acts (particularly women) and cross-border cooperation in criminal matters creating a single, efficient and flexible instrument - the EIO - for obtaining evidence located in another Member State. The initiatives, both based on the principle of mutual recognition of judgments and judicial decisions, are rooted in the Stockholm Programme and provide for the exchange of personal data between Member States.

The EDPS is aware of the importance of enhancing the effectiveness of judicial cooperation between Member States, in particular the fields covered by the EPO and the EIO initiatives. He however underlines that the processing of personal data, particularly in the sensitive area of freedom, security and justice (AFSJ), must be in conformity with the EU rules on data protection.

> ***"Effective protection of personal data is not only important for the data subjects but also contributes to the success of the judicial cooperation itself."***
> ***Peter Hustinx, EDPS***

With regard to both the EPO and the EIO initiatives, the EDPS recommends:

- the inclusion of specific provisions stating that the instruments apply without prejudice to the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Decision 2008/977/JHA);

- the inclusion of provisions requiring the Member States to ensure that:
  - competent authorities have the **resources** necessary for the application of the proposed directives;
  - competent officials observe **professional standards** and are subject to appropriate internal procedures that ensure the proper observance of the **confidentiality** and **professional secrecy** provisions;
  - **authentication systems** allow only authorised access to either databases containing personal data or premises where evidence is located;
  - **tracking of accesses and operations** are performed.

From a more general perspective, the EDPS reiterates the need for a **comprehensive data protection legal framework** covering all areas of EU competence, including police and justice, to be applied both to

personal data transmitted or made available by competent authorities of other Member States and to domestic processing in AFSJ.

☞ EDPS opinion (pdf)

> EDPS opinion on Deposit Guarantee Schemes

Deposit Guarantee Schemes reimburse deposits to depositors up to a maximum of € 100 000 in case a credit institution goes bankrupt. European rules on such schemes have existed since 1994. Shortly after the outbreak of the financial crisis in 2008, this instrument was reinforced. This summer, in July 2010, the Commission put forward another proposal to simplify and harmonise the relevant national rules on the matter.

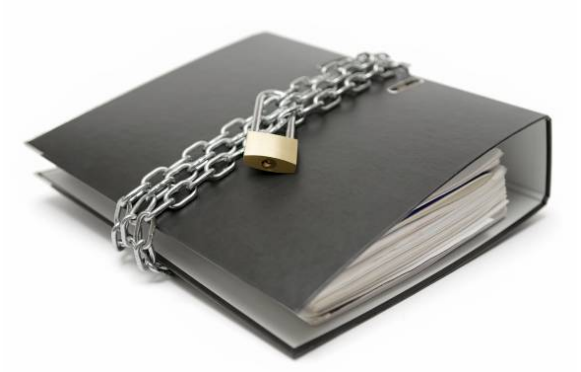
The reimbursement of deposits through such Guarantee Schemes requires the processing of data of depositors. The data protection rules are therefore applicable, as long as these depositors are natural persons. The data is exchanged between a credit institution and a Deposit Guarantee Scheme, but also between Deposit Guarantee Schemes themselves either within a Member State or between different Member States.

On 9 September 2010, the EDPS issued a brief opinion on this proposal and stated that he was generally satisfied with the way in which the data protection aspects were addressed in the proposal. It is for instance assured in the proposal that the relevant personal data are used only for the purposes for which they are exchanged, namely the reimbursement of deposits.

The EDPS was particularly pleased to see that data can only be used for performing so-called 'stress tests' in an anonymous format. During the drafting stage of the proposal, the EDPS had questioned the necessity of using personal data for performing such tests.

☞ EDPS opinion (pdf)

> Additional EDPS paper on public access to documents and data protection after the Bavarian Lager judgment



On 29 June 2010, the European Court of Justice issued its ruling in the Bavarian Lager case, a key case on the question of how best to reconcile the fundamental right to the protection of personal data with the fundamental right of public access to documents (see the previous newsletter (pdf)).

In 2005, the EDPS published a background paper on the matter titled "Public access to documents and data protection" (pdf), which contained guidelines for the EU institutions and bodies. Part of the analysis presented in that Background paper is no longer valid in the light

of the Court's judgment. The EDPS is therefore preparing a short additional paper on this subject which is expected to be ready for publication end of 2010.

In this additional paper, the EDPS will put emphasis on the need for a "proactive approach" on the matter. In brief, this means that institutions should make clear to data subjects - before or at least at the moment they collect their personal data - the extent to which the processing of such data includes or might include its public disclosure. The EDPS takes the position that institutions are obliged to do so as a matter of good practice.

A proactive approach will reduce the number of situations in which institutions have to decide upon public disclosure upon a request for public access, such as in the Bavarian Lager case. The paper will advise on how to strike a fair balance, both in proactive and reactive situations.

SUPERVISION

> News on EDPS prior checking of personal data processing

Processing of personal data by the EU administration that is likely to result in specific risks for the people concerned is subject to a prior check by the EDPS. This procedure serves to establish whether the processing is in compliance with the Data Protection Regulation (EC) No 45/2001, which lays down the data protection obligations of Community institutions and bodies.

>> Fraud investigation - European Investment Bank

On 14 October 2010, the European Data Protection Supervisor issued a prior check opinion regarding the data processing operations that take place in the context of procedures related to fraud investigations at the European Investment Bank (EIB) on credible allegations of fraudulent practices in EIB-financed operations.

In order to conduct investigations the Bank's Fraud Investigation Division of the EIB (IG/IN) has full access to all relevant personnel information, documents and data, including electronic data within the EIB. At the term of the investigation, the Head of IG/IN will determine if a complaint or allegation has been substantiated and will refer the case to the relevant authorities within and/or outside the EIB for appropriate action. If, after reasonable investigation, IG/IN determines that a complaint or allegation has not been substantiated, it shall document the findings in a note to the file and close the case.

After closely examining the processing operation, the EDPS made a number of recommendations. Amongst other things, the EDPS recommended the adoption of a formal protocol for conducting computer forensics investigations by the EIB; recommended the harmonisation of the conservation periods; and recommended the provision of information to data subjects in compliance with the Data Protection Regulation.

☞ EDPS opinion (pdf)

>> Processing of strike related data - European Central Bank

On 28 September 2010 the EDPS issued a prior checking opinion on the issue of processing of personal data in the frame of deductions from salary in the event of a strike at the European Central Bank (ECB).

According to the ECB Staff Rules, staff members have a right to strike and, unless the Executive Board decides otherwise, the total period of the strike shall be deducted from the salary related payments of the member of staff taking part in the strike. To the extent that the participation to a strike automatically entails a deduction from salary and other allowances, the processing of personal data related to that deduction is subject to prior checking by the EDPS as it entails a processing operation excluding individuals from a right, benefit or contract.

After examination of the notification, the EDPS made recommendations notably as concerns the conservation periods of any documentation stored in the electronic document and records management system of the ECB, and the information to be provided to the data subjects

☞ EDPS opinion (pdf)

>> European Surveillance System (TESSy) - European Centre of Disease Prevention and Control

On 3 September 2010, the EDPS issued a prior checking opinion on the data protection aspects of TESSy. TESSy is a communication tool designed to ensure a rapid and effective exchange of epidemiological surveillance data among EU Member States.

The EDPS opinion explains that statistical data continue to be considered as "personal data", and thus, subject to the Data Protection Regulation, so long as the individuals can be at least indirectly identified. The fact that certain "anonymisation techniques have been used", does not mean that the data are considered as "anonymised" in the meaning of recital 8 of the Regulation, and thus, cease to be considered "personal data".

In his opinion, the EDPS also recommends that controllers and processors must be clearly indicated in a way which corresponds to the effective role as well as the legal status of the organisations involved. It must be specified who is responsible for what, and how data subjects can exercise their rights. The EDPS also calls for the adoption of a set of data protection guidelines for TESSy. Other recommendations include the provision of comprehensive and user-friendly information to data subjects on the operator's website which should be complemented by notice provided by Member State contact points in accordance with national data protection laws. A dedicated security policy should also be adopted as soon as possible to help ensure the security of TESSy, and to verify and document good administration.

☞ EDPS opinion (pdf)

>> Safety Inspections - European Commission (JRC Ispra)

On 6 September 2010, the EDPS adopted a prior-check opinion on safety inspections at the Joint Research Centre in Ispra. It addresses the data processing operations carried out for the purpose of maintaining and improving the applicable safety standards.

The EDPS acknowledged that the 'Procedura in caso d'infortunio" involves the processing of health related data by several parties with the aim of minimising the consequences of and preventing similar safety incidents at, the Ispra site.

Consequently, the EDPS issued recommendations in order to guarantee purpose limitation of data transfers, as well as compliance with the data quality principles applicable to the storage and further processing of personal data processed in this context.

A corresponding revision of the existing privacy statement was also suggested.

☞ EDPS opinion (pdf)

> Enforcement

>> Compliance monitoring and enforcement policy

The EDPS is currently developing a Compliance Monitoring and Enforcement Policy which should be available by the end of 2010.

The policy will elaborate how the EDPS intends to monitor, measure and ensure compliance with the Data Protection Regulation (EC) 45/2001. It will also explain the nature of the various enforcement powers available to the EDPS, and outline the drivers and triggers for any formal action that might be taken. By encouraging responsibility, voluntary compliance and the adoption of best practice, the policy will place a strong emphasis on accountability, and will seek to target those agencies and institutions with the poorest compliance record. Finally, the policy will also outline the EDPS' approach to transparency and publicity in relation to his enforcement activities.

> Administrative measures

The Data Protection Regulation (45/2001) provides for the right of the EDPS to be informed about administrative measures which relate to the processing of personal data. The EDPS may issue his opinion either following a request from the Community institution or body concerned or on his own initiative. The term "administrative measure" has to be understood as a decision of the administration of general application relating to the processing of personal data done by the institution or body concerned.

>> Request for access to the identity of an informant - European Ombudsman

The European Ombudsman consulted the EDPS on an issue raised in a complaint lodged against OLAF. The consultation included a number of questions, mainly referring to the following:

- whether it is the case that the identity of the persons who provide OLAF with information, as informants or whistleblowers, should not be disclosed to anyone other than the judicial authorities;
- whether the protection of informants and whistleblowers also has to be guaranteed after the closure of an investigation where there is no follow-up and, if so, in what way and to what extent.

The EDPS has provided comments at rule or policy level, rather than at case level. From this perspective, the EDPS has taken the position that, as a general rule, the identity of a whistleblower or informant should not be disclosed, except when this would contravene national rules on judicial procedures and/or where they maliciously make a false statement. In such cases, these personal data could only be disclosed to judicial authorities.

As to the second question, it has been considered that there are good reasons to believe that the protection of whistleblowers and informants should be the same after the closure of an investigation, regardless of whether there is a follow-up or not. The vulnerability of the whistleblower's or

informant's role and, therefore, the risks to their privacy and integrity do not change depending on whether the investigation is opened or closed with no follow-up.

This approach would of course not exclude that, in practice, there may be situations where the protection of whistleblowers or informants should be superseded by the legitimate claims of others. The passage of time may be a relevant factor here, but it is obviously difficult to speculate about this in the abstract.

☞ EDPS opinion (pdf)

>> International transfers of personal data - European Aviation Safety Agency

The European Aviation Safety Agency (EASA) performs some activities (e.g. services in the field of certification) that give rise to the payment of fees and charges by applicants. Part of these certification activities may be conducted fully or partly outside the territory of the Member States. In some cases the Agency has been asked by the applicants to provide them with the names and date of travelling of the experts in order to allow them to proceed with the payment of the invoice.

The DPO of EASA has asked the advice of the EDPS on the application of Article 9 of the Data Protection Regulation (i.e. transfer of personal data to recipients, other than Community institutions and bodies, which are not subject to the Data Protection Directive 95/46/EC) to the case under consideration.

According to Article 9.1 of the Regulation personal data shall only be transferred to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC, if an adequate level of protection is ensured in the country of the recipient.

In his opinion, the EDPS underlines that, if the third country in question – outside the EEA – does not ensure an adequate level of protection, other conditions mentioned in Article 9 should be taken into account. Article 9.6 indeed stipulates that "by way of derogation from paragraphs 1 and 2, the Community institution or body may transfer personal data if: (...) (d) the transfer is necessary or legally required on important public interest grounds (...)".

Since the performance of the services described above is one of the core activities of EASA, the transfers conducted for the payment of those services could be considered, in principle, as necessary for the functioning of this body, so as to qualify for a derogation under Article 9.6 (d).

The EDPS also notes that, in the present case, it seems that transfers would not be "repeated, mass or structural", but that they would take place as a "one off" transfer to different recipients in different countries. As to the risks to the data subjects, no specific risks have been mentioned in the DPO's letter. The categories of data to be transferred (the name and travel date of the given experts) do not seem to give rise to particular concerns either.

The EDPS however points out that no safeguards are ensured in those cases where an exception is applied. For this reason, he recommends the inclusion of a clause that should specify that the recipient is legally authorised to request this data, and limit the use of the data to the sole purposes motivating the transfer.

☞ EDPS opinion (pdf)

EVENTS

> Forthcoming events

>> EDPS press conference on the future of the EU legal framework for data protection (Brussels, 15 November 2010)

The EDPS will hold a press conference on Monday 15 November 2010 on the future of the EU legal framework for data protection. The press conference will provide an opportunity to hear the EDPS' perspective on the imminent wide-ranging revision of EU rules on data protection and privacy, and on some topical issues in related areas.

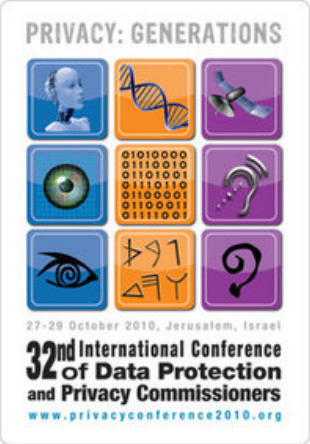
Peter Hustinx, EDPS, and Giovanni Buttarelli, Assistant Supervisor, will in particular address the Commission's recent communication on a strategy to strengthen EU data protection rules. They will run through the implications of a reform that will shape the development of an Information Society where the citizens' fundamental right to data protection should be effectively ensured.

The press conference will also provide the opportunity to present the EDPS Annual Report 2009 and outline the main features of the activities in 2009 with regard to the EDPS' supervisory, consultative and cooperative tasks.

☞ For more information, please send an email to: press@edps.europa.eu

> Outcome of past events

>> OECD event and 32nd International Conference of Data Protection and Privacy Commissioners (Jerusalem, 26-29 October 2010)



In the last week of October 2010, two major data protection events took place in Jerusalem as part of a Privacy week, organised by the Organisation for Economic Co-operation and Development (OECD) and by ILITA, the Israeli Data Protection Authority.

The OECD event, organised to mark the 30th anniversary of the OECD Privacy Guidelines, focused on the evolving role of the individual in privacy protection. Individuals are no longer simply data subjects but now actively process personal data themselves, for instance when they participate in social networks. Moreover, current technology allows all human behaviour to be recorded and ensures that nothing will be forgotten. These are just two reasons why the OECD is considering revising its Privacy Guidelines that are now 30 years old.

The 32nd International Conference of Data Protection and Privacy Commissioners, organised by ILITA, further elaborated on these developments and on the perspectives of different generations on privacy and data protection. A major subject of the conference was how laws and self regulatory mechanisms influence technology and vice versa. Once again, the emerging use of social networks played a central role in this conference.

On behalf of the EDPS, Supervisor Peter Hustinx, Assistant Supervisor Giovanni Buttarelli, and legal advisor Rosa Barcelo gave presentations and chaired different sessions of the Conference.

The closed session of the Commissioners adopted various resolutions, the most important being a call for the organisation of an intergovernmental conference with a view to developing a binding international instrument on privacy and the protection of personal data.

The 33rd International Conference will take place in Mexico in November 2011.

☞ More information on the Conference website

>> Data Protection Officers meeting (London, 15 October 2010)

On 15 October 2010 the EDPS held a biannual meeting with the Data Protection Officers of the European Union institutions and bodies at the European Medicines Agency in London.

After a general presentation on recent developments in data protection, the EDPS presented a new structure and organisation chart. He further outlined the compliance and enforcement policy which he aims to finalise before the end of the year (see Enforcement section of this newsletter). He also took this occasion to highlight the main points of his imminent joint opinion on the processing of health-related data in the agencies.

SPEECHES AND PUBLICATIONS

- Statement (pdf) of Peter Hustinx on the Reform of Regulation 1049/2001 on public access to documents, Committee on Petitions, European Parliament (Brussels, 9 November 2010)
- "Government access to private sector data", speaking points (pdf) of Giovanni Buttarelli at the 32nd International Conference on Data Protection and Privacy Commissioners (Jerusalem, 28 October 2010)
- "Promoting Dialogue Between NGOs and DPAs" speaking note (pdf) of Giovanni Buttarelli at the Public Voice Civil Society Meeting: “Next Generation Privacy Challenges and Opportunities” held in conjunction with the 32nd International Conference on Data Protection and Privacy Commissioners (Jerusalem, 25 October 2010)
- Speaking points (pdf) of Giovanni Buttarelli at the conference on "Criminal Justice in Europe: Challenges, Principles and Perspectives" (Luxembourg, 22 October 2010)
- Speaking points (pdf) of Peter Hustinx at the High-level Roundtable Discussion on the "Future of Personal Data Protection", European Commission (Brussels, 5 October 2010)
- Speaking points (pdf) of Giovanni Buttarelli at the Monthly Roundtable of the Security & Defence Agenda on "Fine-tuning EU border security" (Brussels, 29 September 2010)
- Speaking points (pdf) of Giovanni Buttarelli at the LIBE Hearing on combating sexual abuse, sexual exploitation of children and child pornography, European Parliament (Brussels, 28 September 2010)
- "Protection of children on the Internet", article (pdf) by Peter Hustinx published in Information Bulletin of Czech Office for Personal Data Protection, nr 1/2010, p. 1-2 (2 September 2010)
- "Privacy and data protection - legal lessons?", EDPS Contribution (pdf) ("Expert Think Piece") to HiiL Law of the Future Conference 2011 (30 July 2010)

NEW DATA PROTECTION OFFICERS

Each Community institution and body has to appoint at least one person as a Data Protection Officer (DPO). These officers have the task of ensuring the application of the data protection obligations laid down in Regulation (EC) No 45/2001 in their institution or body in an independent manner.

> Recent appointments:

- Mr Alfonso **SCIROCCO**, DPO, and Mrs Sylvie **PICARD**, Assistant DPO - European Data Protection Supervisor
- Mr Alain **LEFÈBVRE**, European Chemicals Agency

☞ See full list of DPOs.

> EDPS appoints new DPO team

On 1 September 2010, the EDPS appointed a new DPO team, composed of Alfonso Scirocco, DPO, and Sylvie Picard, Assistant DPO. Both of them have substantial experience in data protection: Alfonso in the EDPS policy and consultation team, and Sylvie in the supervision team.

These appointments show that the EDPS is eager to invest new resources and energy in this area, in order to advance quickly towards a better level of compliance.

The role of the DPO at the EDPS presents many challenges: being independent within an independent institution, meeting the high expectations of colleagues who are particularly well-informed and sensitive about data protection issues, and delivering solutions that can serve as benchmarks for other institutions.

The implementing rules (pdf) reflect these specificities, while taking into account both the EDPS position paper (pdf) and the DPO Network's Paper on Professional Standards for Data Protection Officers (pdf).

A DPO page is now available on the EDPS website, and will be developed to include new features over the coming months.

About this newsletter

This newsletter is issued by the European Data Protection Supervisor – an independent EU authority established in 2004 to:

- monitor the EU administration's processing of personal data;
- give advice on data protection legislation;
- co-operate with similar authorities to ensure consistent data protection.

☞ **You can subscribe / unsubscribe to this newsletter via our website**

CONTACTS

www.edps.europa.eu
Tel: +32 (0)2 283 19 00
Fax: +32 (0)2 283 19 50
E-mail:
NewsletterEDPS@edps.europa.eu

POSTAL ADDRESS

EDPS – CEDP
Rue Wiertz 60 – MO 63
B-1047 Brussels
BELGIUM

OFFICE

Rue Montoyer 63
Brussels
BELGIUM

EDPS – The European guardian of personal data protection