



EUROPEAN DATA
PROTECTION SUPERVISOR



CONSULTATION

- > eHealth Action Plan needs a data protection boost.....2
- > Insolvency proceedings need more concrete data protection safeguards3
- > Privacy by design should be included on the Digital Agenda3
- > Minimisation of personal data will help occurrence reporting in civil aviation.....4
- > Radio equipment proposal needs fine tuning4
- > Balancing investor privacy and regulatory transparency5



SUPERVISION

- > Tighter safeguards can help secure JRC6
- > EACI: Analysis and transfer of fraud information to OLAF6
- > Compliance controls in anti-money laundering and combating the financing of terrorism must be strengthened.....7
- > Scheduled works down the line: ERA should make significant changes to its email policy7
- > Helping to get internet monitoring policy back on track.....7



EVENTS

- > ICO: The UK's Information Commissioner welcomes progress on the planned EU reforms8
- > DPO training, Brussels9
- > DPO Meeting, Lisbon9
- > EDPS round table: the smart borders package and its data protection implications.....9
- > VIS Supervision Coordination meeting.....10
- > EURODAC Supervision Coordination meeting.....11



SPEECHES AND PUBLICATIONS



NEW DATA PROTECTION OFFICERS

- HIGHLIGHTS -

Data Protection Reform Package - an update

On 15 March 2013, the EDPS sent additional comments on the reform of the EU data protection rules to the European Parliament, the Commission and the Council. Our comments related to specific areas that required clarification and reacted to the amendments proposed by the relevant committees of the European Parliament.

In our comments, we reiterated that pseudonymised data remains personal data (or personal information) and as such should be protected. Any definition of anonymous data or pseudonymous data should, therefore, be fully consistent with the definition of personal data and should not lead to unduly removing certain categories of personal data from the scope of the data protection framework. We also advised against excluding specific sectors from the scope of application of the EU data protection framework and against limiting the territorial scope of the proposed general Data Protection Regulation. We support the amendments eliminating the general possibility of further processing for incompatible purposes and stressed that the definition of explicit consent should be maintained.

We also support the definition and responsibilities of controllers and processors as proposed by the Commission, as well as the principle of accountability, which should apply to the whole package. We support some of the elements of the so called 'risk-based approach' but pointed out that full protection as provided for in the Regulation should apply to all processing operations, not only to the most risky ones. We also called for more incentives for the use of data protection officers. As regards international transfers, we recommend clarifying the rules and welcome the amendments introducing a new article on transfers not authorised under EU law.

As regards the proposed Data Protection Directive on criminal law enforcement, we support the amendments that further align the Directive with the Regulation to ensure consistency. We also welcome the amendments introducing specific conditions and safeguards for the access by law enforcement authorities to data initially processed for other purposes and highlighted that any transfer to non law enforcement authorities or private parties should be strictly limited.

🔗 EDPS Press release ([pdf](#)) and Comments ([pdf](#))

Tailor-made training at the ETF

Promoting a data protection culture within the EU institutions and bodies is a strategic objective at the EDPS. To this end we have coordinated several training and other outreach activities; we continued our cooperation with the data protection officer (DPO) network with a training session in our offices on 17 April 2013 and participated in the biannual EDPS-DPO Network meeting at EMCDDA in Lisbon. Read more about these in our events section.



On 25 February 2013, as part of our outreach activities to raise awareness, Supervision and Enforcement and IT Policy colleagues from the EDPS gave a one day data protection training in-situ at the European Training Foundation (ETF) in Turin, Italy.

As well as an overview of the role of the EDPS, we presented a case study and, at the request of the ETF, we devoted sessions to specific issues such as data subjects' rights, HR matters and public procurement issues.

The training was an excellent forum to exchange views, for example, on the practical implementation of our Guidelines and an opportunity for EDPS staff to learn from the experiences of an agency.

We are delighted that this training was well received by the ETF and in our efforts to combine efficiency and effectiveness, we will consider similarly original formats for other agencies, with the possible inclusion of video conferences.



CONSULTATION

> eHealth Action Plan needs a data protection boost



In our opinion of 27 March 2013, on the Commission Communication for an *eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century*, we welcomed the attention paid to data protection in the Communication. However, the personal information processed in the context of eHealth and well-being through information communication technology (ICT) applications and solutions, often relates to health data, which requires a higher level of data protection. We urge

industry, Member States and the Commission to carefully consider the data protection implications when implementing initiatives within the eHealth area. Furthermore, we recommend that the Commission consult the EDPS before it takes further legislative and non-legislative action as described in the Communication.

☞ EDPS Opinion ([pdf](#))

> Insolvency proceedings need more concrete data protection safeguards

In our opinion of 27 March 2013 on the Commission proposal for a Regulation amending Council Regulation (EC) No 1346/2000 on insolvency proceedings, we welcomed the references made to the applicability of EU data protection legislation.

However, we recommend that the substantive provisions should be clearer on how the data protection principles referred to concretely apply to insolvency proceedings, in particular to the information exchanged between stakeholders that is also sometimes published.

We expressed concerns about the publication of information relating to the opening and closing of insolvency proceedings in insolvency registers which are accessible to the public, on the internet, free of charge.

We acknowledge that the aim of encouraging transparency and communication between stakeholders is legitimate. However, we consider that this particular method of publication raises specific risks and is privacy intrusive. We pointed out that the proportionality of this measure was not proven since, contrary to what is advised in the *Schecke* ruling, no alternative option, i.e. a different method of publication that would cause less interference with the beneficiaries' right to private life, has been considered.

Among other things, we advise that data controllers are designated, updates of the data exchanged or published is organised, the retention period of the data processed is specified and procedures are set up to inform data subjects of the processing of their personal information.

☞ EDPS Opinion ([pdf](#))

> Privacy by design should be included on the Digital Agenda

In its Communication on *The Digital Agenda for Europe - Driving European growth digitally*, the Commission has identified various policy areas on which it will focus its efforts to enable and stimulate the development of the digital economy, such as the Digital Single Market, very fast internet supply and demand, cloud computing and trust and security.

In our opinion of 10 April 2013, we emphasise that any design and deployment of new information communication technology (ICT) applications and solutions for the digital environment must respect data protection principles, especially since the principle of *privacy by design*, will become a legal obligation under the proposed Data Protection Regulation. We also reminded the Commission that there should be an appropriate legal basis for the use of



interoperability as a means to facilitate data sharing among databases, together with appropriate data protection safeguards.

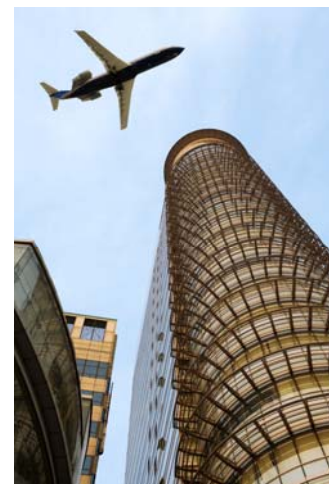
In the area of cloud computing, we referred to the extensive guidance on the application of current data protection law and on the impact of the proposed Data Protection Regulation that has been provided by data protection authorities as well as the EDPS. We urge the Commission to act upon this guidance to help foster trust from individuals and customers in these new technologies, which in turn will ensure their successful deployment.

↪ EDPS Opinion ([pdf](#))

> Minimisation of personal data will help occurrence reporting in civil aviation

The Commission Proposal for a Regulation on occurrence reporting in civil aviation aims to improve the existing occurrence reporting systems in civil aviation both at national and European level. An occurrence is any event that could affect aviation safety, including accidents, defects, faults and other problems associated with the operation of aircrafts. To ensure more comprehensive and high quality reporting the proposal outlines, among other things, a voluntary reporting system to supplement the mandatory system and encourages organisations - and not only Member States - to report occurrences. The proposal also offers harmonised protection from hierarchical punishment or the prosecution of individuals reporting occurrences and aims to ensure adequate access to information contained in the European Central Repository.

In our opinion of 10 April 2013, we welcomed the attention paid to the protection of personal data in the proposal, particularly through the engagement taken to *unidentify* a major part of the data processed. However, we pointed out that what is provided for, at best, amounts to partial anonymisation and thus data processed would still be personal data subject to the applicability of EU data protection legislation. We recommend clarifying several points in the text to better protect the data and fully anonymise them where possible. We also advise that the controller of every database is clearly identified, the period(s) for which the data is to be stored in databases is specified, the rights of data subjects and the security measures to be implemented are highlighted. Furthermore, we recommend additional safeguards for the transfer of data to third countries and to the processing of sensitive data.



↪ EDPS Opinion ([pdf](#))

> Radio equipment proposal needs fine tuning

The Commission proposal for a Directive harmonising the laws of Member States that relate to the availability of radio equipment on the market will replace Directive 1999/5/EC on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (the so-called R&TTE Directive).

With some exceptions, any equipment that makes use of radio waves or telecommunication frequencies would fall within the scope of these rules, for example, cars equipped with SIM cards (such as the integrated [eCall](#), reported on in our last newsletter), which make use of radio equipment. As the use of such technology allows for the tracking of the location of a vehicle (and thereby of a person), its use has implications for the privacy of individuals.

In our formal comments of 27 February 2013, we noted that the R&TTE Directive incentivised manufacturers of such equipment to apply privacy by design. We are, therefore, pleased that the proposal builds on the approach of the R&TTE Directive in privacy and data protection terms as they remain essential requirements for the design of radio equipment. We also welcome that the proposal clearly imposes responsibility on manufacturers for ensuring that radio equipment placed on the market has been designed and manufactured so that it incorporates, among other things, safeguards to ensure the protection of personal data and privacy of consumers.

However, we regret that fixed terminal equipment has been removed from the scope of the Directive, which reduces the incentive for building in privacy by design in such equipment. This is particularly regrettable since terminal equipment plays an increasingly important role for the protection of privacy and there is no equivalent rule on the protection of personal data and privacy in other legislative instruments that apply to terminal equipment not using radio. We, therefore, recommend that the proposal includes a commitment from the Commission to monitor the compliance of terminal equipment with data protection and privacy requirements and to consider appropriate measures should the need arise.

↪ EDPS Comments ([pdf](#))

> Balancing investor privacy and regulatory transparency

In its Action plan on European company law and corporate governance: balancing investor privacy and the need for regulatory oversight and transparency, the Commission outlines its initiatives to modernise the company law and corporate governance framework in Europe.

In our letter of 27 March 2013, we reminded the Commission that any legislative proposals aimed at *increasing visibility* of shareholdings must take due account of shareholders' rights to protect their personal information. Policy makers need to carefully assess and clearly articulate the public policy objectives that increase this visibility and balance them against the risks to shareholders' rights to protect their privacy.



Better shareholder oversight of remuneration policy is another area in the proposal where transparency needs to be balanced with the rights of individuals to their privacy and protection of their data. We encourage the exploration of different methods, modalities and granularities of making personal data publicly available to ensure that the measures adopted are proportionate for any scenario that allows access to information on the remuneration of individual members of management and/or supervisory boards to the public.

↪ EDPS Letter ([pdf](#))



SUPERVISION

> Tighter safeguards can help secure JRC

On 19 March 2013, we adopted an opinion on processing operations carried out in the context of security investigations at the Joint Research Centre (JRC) in Petten.

We approached this notification in light of the revision of the Commission Security Decision which defines the general tasks of the Security Service and the upcoming adoption of a Memorandum of Understanding between the Directorate General Human Resources & Security Directorate of the European Commission and the JRC to conduct certain types of security investigations.

The purpose of the processing operation is to obtain information associated with security related incidents such as traffic accidents, parking violations and vandalism that have occurred in JRC Petten premises, ultimately resulting in a report describing the occurrence.

Our main concerns over this processing, related to the use of the transferred data by recipients such as EU institutions or bodies or national authorities (police and judicial, for instance). We, therefore, suggested that a notice on purpose limitation be provided to the recipients. We also insisted that the necessity of any potential transfers of information be duly assessed and documented before an actual transfer takes places.

↪ EDPS Opinion ([pdf](#))

> EACI: Analysis and transfer of fraud information to OLAF



The purpose of the processing carried out by the European Agency for Competitiveness and Innovation (EACI) is to analyse and transfer information to the European Anti-Fraud Office (OLAF) on cases of alleged fraud and financial irregularities in the management of EU funds. EACI was the first agency to submit a notification in this field to the EDPS.

In our prior-check opinion we insisted on a proportionate retention period for the personal information in cases which are not transferred to OLAF; that only data that is strictly necessary should be transferred to the appropriate recipients on the basis of the legitimate performance of their tasks and that EACI guarantees the rights of access and rectification of those whose information is retained, including whistleblowers, informants or witnesses specifying the restrictions under Article 20 of the Regulation.

↪ EDPS Opinion ([pdf](#))

> Compliance controls in anti-money laundering and combating the financing of terrorism must be strengthened

The aim of the European Investment Bank's proposal to implement anti-money laundering (AML) and combating the financing of terrorism (CFT) controls is to apply best banking practices in these fields and to minimise the risks to integrity and reputation.



In our prior-check opinion, we urged the EIB to reinforce the existing legal basis. We further stressed the need to introduce a number of safeguards to enhance the quality of the personal data processed. Personal information which has no relevance for the underlying objective should not be processed. Unverified rumours, press reports, or other allegations should be treated with care. Ultimately, the EIB should put in place procedures to ensure that the information used is accurate and up-to-date.

↪ EDPS Opinion ([pdf](#))

> Scheduled works down the line: ERA should make significant changes to its email policy



In reply to a notification for prior-checking from the European Railway Agency (ERA), we thoroughly reviewed their email monitoring policy, which was drawn up to help prevent disruption and misuse by staff and urged amendments in a number of areas.

We warned that any email monitoring must be necessary and proportionate; it should be performed first by automated means and on a no-name basis. The examination of individual emails with the identification of the user must only be performed when there is reasonable suspicion of wrongdoing, corroborated by concrete initial evidence and in the framework of an administrative investigation.

Among other things, we also invited ERA to exclude the applicability of the email policy to personal webmail accounts and to exclude, or significantly limit, ERA's power to interfere with personal communications.

↪ EDPS Opinion ([pdf](#))

> Helping to get internet monitoring policy back on track

The purpose of e-monitoring at the European Railway Agency (ERA) is to verify whether internet use is in conformity with that permitted in its internal policy documents.

In our prior-check opinion, we applied the analysis and guidelines outlined in our previous opinions.

We warned that general monitoring of individual internet use in the absence of suspicion is excessive. We recommended that a policy that allows a gradual increase in monitoring depending on concrete needs and circumstances be implemented. Monitoring internet use of identified, individual users

should only take place if there is reasonable suspicion, corroborated by evidence and in the framework of an administrative inquiry. Before engaging in individual monitoring, other less intrusive measures (such as general reminders or warnings) should be considered where possible.

↪ EDPS Opinion ([pdf](#))



EVENTS

> ICO: The UK's Information Commissioner welcomes progress on the planned EU reforms



In the UK, 2013 has been the year when business has truly started to realise the importance of the planned EU data protection reforms, and the direct impact the changes to the law will have.

That awareness has come with a level of concern, but the UK Information Commissioner's Office (ICO) is working hard to show that there is much to be welcomed

in the content of the proposals. The current law needs modernisation, and these reforms should bring that about, particularly in enhancing individuals' rights.

Much of the concern has been around suggestions the new Regulation could bring increased red-tape, particularly for smaller businesses. Against that backdrop, it was good to hear the comments of Françoise Le Bail, Director General of the Commission's DG Justice, when she spoke at the ICO's Data Protection Officer's Conference last month.

Ms Le Bail dispelled concerns that the new legal framework would be too prescriptive, reassuring the audience that the Commission is willing to adopt a more risk-based approach and take into account the position of SMEs in particular. It's an approach that should reduce any disproportionate impact on business, and one the ICO welcomes.

There's much work left to do to shape the proposals into a law which should be applicable to both the public and private sectors and that will prove fit for the next decade and beyond, but we believe real progress is being made.

You can read more about the ICO's views on the proposals [here](#) and also through their latest blog posts [here](#).

> DPO training, Brussels

At the EDPS, we believe that the role of the DPO is pivotal in ensuring that data protection rules and principles are applied within the EU administration. So we were delighted to host a training session at our offices on 17 April 2013. The day was an opportunity to recap on:

- the basic principles of the existing Data Protection Regulation (lawfulness of processing, sensitive data and exceptions, quality of data);
- the duties of the DPOs (inventory, register and notifications to the EDPS);
- the prior-checking procedure (deadlines, procedural phases, follow up of recommendations made in opinions);
- the guidance available on the EDPS website (DPO corner, thematic guidelines);
- the tools to measure compliance (such as surveys);
- what to expect in case of non-compliance (visit with roadmap and/or use of the EDPS enforcement powers).

The questions and practical examples that accompanied the presentations gave rise to useful exchanges between EDPS colleagues and the DPOs. The event was received positively and feedback indicates that DPOs appreciated the event and the opportunity to interact with EDPS staff.

> DPO Meeting, Lisbon

On 1 March 2013, the first of our bi-annual meetings with Data Protection Officers took place at the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA).

As well as an exchange of views between the EDPS and DPOs on the processing of personal information related to the use of internet and communications networks, there were

discussions on data protection developments at European and International level; recent EDPS activities such as our report on Data Protection Coordinators at the European Commission, developments in prior-checking opinions and consultations, and the EDPS strategic review.

The meeting once again proved to be an excellent opportunity to exchange views on shared issues.



33rd Meeting of the Data Protection Officers and the European Data Protection Supervisor - Lisbon 1st March 2013

> EDPS round table: the smart borders package and its data protection implications

On 28 February 2013, the Commission adopted a smart border package. In it, the Commission proposes an entry/exit system (EES) that will record the time and place of entry and exit of third country nationals travelling to the EU. The system will calculate the length of the authorised short stay electronically, replacing the current manual system, and will issue an alert to national authorities when there is no exit record by the expiry date. In order to complement this system, a Registered Traveller Programme (RTP) is proposed to allow frequent travellers from third countries to enter the EU using simplified border checks, subject to pre-screening and vetting.

On 10 April 2013, as part of our 2013-2014 Strategy, we organised a workshop for experts, including those from countries that have implemented similar systems to share their experiences and debate the data protection implications.

Participants were welcomed to the workshop by Peter Hustinx, EDPS and Giovanni Buttarelli, Assistant EDPS. They included experts from the European Commission, the European Parliament (EP), the Irish Presidency, the USA Mission to the EU, EU Member States, the Article 29 Working Party, data protection authorities, academics, NGOs including the Meijers Committee and CEPS.



Moderated by Mr. Hielke Hijmans, head of the Policy and Consultation unit at the EDPS, a number of questions and concerns were raised in the forum about the practical implications on data protection of the EES, the compatibility with other systems such as VIS and SIS, the role of biometrics, possible access of law enforcement authorities and transfer of data to third countries. The experiences of the USA and EU Member States that have implemented similar systems were of particular interest to the group.

Following the presentation of our initial reaction on the package before the EP Civil Liberties (LIBE) committee on 21 March 2013, we are working on an opinion on the package to be published in the coming months.

> VIS Supervision Coordination meeting

The Visa Information System (VIS) became operational in North Africa in October 2011, was rolled-out in the Near East in May 2012, in the Gulf in October 2012, in West Africa and Central Africa in March 2013. The next regions for the deployment will be South America (September 2013), Central Asia, South East Asia and the occupied Palestinian territory (November 2013).

In accordance with the VIS Regulation, the EDPS and national DPAs ensure coordination of data protection supervision of the VIS. Thus, on 11 April 2013, the EDPS hosted the second meeting of the VIS Supervision Coordination Group. Following the adoption of its Rules of Procedure, Peter Hustinx, EDPS, was elected Chair and Ms. Vanna Palumbo, representing the Italian Data protection authority (DPA), was elected Vice-Chair of the group. The UK and Ireland were invited to join the group as observers.

The group was also given a presentation by representatives of the new IT agency, EU LISA, on their work programme objectives that aim to ensure that the technical characteristics of VIS will be able to support a worldwide roll-out.

Following discussions from the first VIS meeting, the group adopted the VIS working programme for the next two years. The objectives of the programme are focused primarily on sharing national experiences after full analysis of the VIS Regulation data protection requirements and the possible undertaking of joint studies such as on the outsourcing of some common tasks to external providers.

The group enjoyed the experiences related by some members as several DPAs have already performed inspections at consulates abroad - no major shortcomings have been identified so far. All members of the group are closely following developments, such as the continued roll out of the system and foresee inspections of national VIS systems in the future.

The next meeting of the VIS Supervision Coordination Group will be held in the Autumn.

> EURODAC Supervision Coordination meeting



On the morning of 12 April 2013, we hosted the 18th meeting of the EURODAC Supervision Coordination Group.

At the meeting, the group took stock of the latest legislative developments in the EURODAC RECAST, where discussions are approaching conclusion and discussed the transfer of operations to the IT agency, EU LISA, in Strasbourg.

An update was also given to the group on the report on unreadable fingerprints. Based on an analysis of the 28 answers received, the main conclusions and recommendations include:

- unreadable fingerprints should not adversely affect an asylum application;
- the procedure for taking fingerprints and dealing with temporary or permanently unreadable fingerprints should be clear;
- agents responsible for taking the fingerprints should be given sufficient training. This measure should be binding and unified throughout the EU.

The report is being finalised and will be adopted by the group in the following weeks by written procedure.

The next meeting of the EURODAC Supervision Coordination Group will take place in the Autumn, back-to-back with the VIS Supervision Coordination Group meeting.



S P E E C H E S A N D P U B L I C A T I O N S

- "The future of the regulation of personal data in Europe: A French-Italian dialogue", speech ([pdf](#)) delivered by Giovanni Buttarelli, Paris (24 April 2013)
- "Sharing personal information and respecting privacy at home", speech ([pdf](#)) delivered by Peter Hustinx at Le Point Conference "Connected and Intelligent Home", Paris (28 March 2013)
- "Data Protection and Criminal Justice - The view of the EDPS", speech ([pdf](#)) delivered by Peter Hustinx at the Conference on European Data Protection Law, Delegation of the Bars of France, Brussels (15 March 2013)
- "Protection of personal data: now part of our DNA" - speech ([pdf](#)) of Peter Hustinx given at the EESC Conference "Towards a more responsible use of the internet - The European civil society perspective", Brussels (6 March 2013)



NEW DATA PROTECTION OFFICERS

> Recent appointments

- Mr. Lucas CAMARENA JANUZEC, European Economic and Social Committee (EESC)
- Mr. Stephan KARAS, European Securities and Markets Authority (ESMA)
- Mr. Martin GARNIER, Translation Centre for the bodies of the EU (CdT)

☞ See full list of [DPOs](#).

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;
- cooperate with similar authorities to ensure consistent data protection.

☞ **You can subscribe / unsubscribe to this newsletter via our [website](#)**

© Photos: iStockphoto/Edps, European Union and ICO

🐦 Follow us on Twitter: [@EU_EDPS](#)

CONTACTS

www.edps.europa.eu

Tel: +32 (0)2 283 19 00

Fax: +32 (0)2 283 19 50

NewsletterEDPS@edps.europa.eu

POSTAL ADDRESS

EDPS

Rue Wiertz 60 – MTS Building

B-1047 Brussels

BELGIUM

OFFICE ADDRESS

Rue Montoyer 30

B-1000 Brussels

BELGIUM

EDPS – The European guardian of data protection