

EUROPEAN DATA
PROTECTION SUPERVISOR

EDPS Newsletter

No. 43 | October 2014

IN THIS ISSUE

HIGHLIGHTS

- 1 Handover at EDPS to be expected soon



SUPERVISION

- 1 International Data Transfers: Ensuring the protection of EU data abroad
- 2 Your email account: for your eyes only?
- 2 Addressing access to documents requests
- 2 Achieving consistency through cooperation
- 2 Targeted action increases compliance
- 3 Data protection standards in good health
- 3 Dealing with allegations of scientific misconduct
- 3 Conducting an effective survey



CONSULTATION

- 3 Banking on data protection
- 4 Space: the final frontier
- 4 Branching out just got easier
- 4 A platform for data sharing in Europe
- 4 A portal for justice across the EU



IT POLICY

- 5 Smart policies for smart grids
- 5 Keeping EU institutions mobile



EVENTS

- 5 The IPEN workshop: pledging privacy to technology
- 6 Three years in EU data protection reform: state of play and perspectives, Brussels
- 6 EU data protection competition announced
- 6 The EDPS newsletter: what do you think?



SPEECHES AND PUBLICATIONS



DATA PROTECTION OFFICERS

HIGHLIGHTS

Handover at EDPS to be expected soon

In the coming weeks, a new team of Supervisors is likely to be appointed at EDPS. Although the adoption of a formal decision by the European Parliament and the Council may take a few more weeks, all available information suggests that Giovanni Buttarelli, now Assistant EDPS, will become the new Supervisor, and Wojciech Wiewiórowski, now Inspector General for Personal Data Protection in Poland, will become the new Assistant EDPS. Peter Hustinx, now Supervisor, will step down after having been in the job for more than ten years. A formal handover is expected on the first day of the new mandates entering into effect.

During the previous two mandates, the EDPS has been set up and gradually become more visible as an institution, and developed its role in the supervision of EU institutions and bodies. It also advised the Commission, the Parliament and the Council on new policies and legislation, as well as the Court of Justice in relevant cases, and cooperated with national data

protection authorities to improve consistency of data protection in the EU. In recent months, the EDPS has taken other initiatives relating to privacy and technology (see page 6 on IPEN) as well as privacy and competition in the age of big data.

The new team will take over at a crucial moment of continuing great challenges. The first and foremost priority is to support the adoption of a new EU legal framework for data protection in the course of 2015, and preferably by the next spring. This is an essential condition in order to ensure that privacy and data protection continue to play their key role in the digital internal market. The EDPS is likely to provide the secretariat for the European Data Protection Board that will help to ensure consistency in supervision and enforcement of the new framework across the EU. This will call for the necessary dedication and diplomacy from the new team of Supervisors and their staff.

Meanwhile, the EU institutions and bodies will have to ensure that privacy and data protection requirements

are embedded in their use of cloud computing and other new digital services. New policy initiatives announced by the new Commission will have to be evaluated on their conformity with privacy and data protection requirements as set out in the Charter and the applicable legal frameworks. The negotiations between the EU and the US on transatlantic agreements for trade and investment or law enforcement data sharing will be among the many challenging subjects calling for attention of the new team of Supervisors.

The preceding issues of this newsletter have recorded the rapid growth and increasing impact of the EDPS as an institution dedicated to good privacy and data protection practice. We will continue to inform you about the ways in which the new team of Supervisors will guide and develop the precious heritage and the resources of our institution in the interest of European citizens.



SUPERVISION

International Data Transfers: Ensuring the protection of EU data abroad

On 14 July 2014, the EDPS adopted a [position paper](#) designed to provide guidance to EU [institutions and bodies](#) on how to interpret and apply the rules laid down in Regulation (EC) No 45/2001, when transferring personal data internationally.

EU institutions and bodies increasingly need to transfer personal information to third countries or international organisations. For example, international data transfers are necessary to facilitate cross-border cooperation, enabling the successful implementation of EU projects abroad or contributing to the resolution of EU investigations.

Additionally, the EU is employing more services abroad than ever before, such as in the fields of IT and translation. All these activities involve the transfer and sharing of data and the new EDPS position paper provides concrete guidance on how to interpret the rules on this subject.

Our guidance focuses mainly on the notion and applicability of adequate protection, and on how to assess [adequacy](#). It also analyses exceptions to the [adequacy requirements](#) and putting in place appropriate safeguards, for those situations in which the recipient country does not provide an adequate level of data protection. Examples are given

to facilitate the task of [data controllers](#) and [data protection officers](#) (DPOs) in applying these rules, as well as a checklist with the steps to be followed when applying Article 9 of Regulation 45/2001. The paper also provides the relevant information on the supervisory and enforcement roles of the EDPS within the context of data transfers.

[EDPS Position Paper](#)



Your email account: for your eyes only?

The EDPS received a complaint from a former member of staff of an EU body, alleging that his email account (firstname.name@body.europa.eu) had not been deactivated after his departure. Instead, the account remained open and all of the emails he received were forwarded to the general functional mailbox of the EU body concerned, where they could be accessed by a large number of other staff members.

We found that the fact that the complainant's email account was not deactivated after his departure was a breach of the security rules of Regulation 45/2001. Furthermore, the subsequent

automatic forwarding of the complainant's messages to the general functional mailbox was not only a breach of the security rules but was also unlawful as it was not necessary.

Our Decision of 17 July 2014 finds that the forwarding of emails from the account of a former employee should only be possible in exceptional circumstances, if it can be justified for reasons of business continuity. The EU body in question, therefore, could have opted for less privacy intrusive measures when dealing with this case. Options to consider might have been:

(1) to set up an automatic response for the individual email

account, asking for important correspondence to be resent to another email address; or

(2) to give one person, in cooperation with the DPO, authorisation to access the account.

Additionally, the EU body should have informed the complainant when it decided to forward his emails, thus allowing him to exercise his right to object.

We asked the EU body to act immediately and we will follow up in due course, in order to ensure that the necessary steps have been taken to remedy the situation.



Addressing access to documents requests

The EDPS investigated an access to documents case involving the European Commission. The applicant was asked by the Commission to provide them with his postal address, a request which he found to be excessive.

However, we found several reasons why the collection of this personal information should be considered legitimate including:

- to ensure legal certainty as to when the reply was received;
- to counter requests for access under a false identity; and
- to verify whether the person requesting access to documents is situated in the European Economic Area (EEA).

Based on this, we decided that asking for an applicant's postal address was not an excessive requirement for access to

documents requests. Nevertheless, it is important to provide applicants with information explaining why their postal details are needed. Accordingly, the Commission now includes this information in its privacy statement.



Achieving consistency through cooperation

One of the tasks of the EDPS, set out in the data protection Regulation, is to improve consistency in the application of the rules on the processing of personal data throughout the European Union. In particular, this involves cooperating and sharing knowledge with data protection authorities (DPAs) in the EU.

One way in which we do this is to conduct visits to DPAs. These allow us to better understand the way in which other DPAs work and the challenges they face. Visits help us to learn from one another and thus foster more profitable cooperation in the future. This is especially pertinent as the new data protection reform expected in the near future means that all data protection bodies should start to anticipate the changes to come.

To this end, we visited the Spanish DPA on 18 July 2014, with the primary objective of exchanging experiences on specific supervision and enforcement issues, such as the role of the DPO; intervention

in court cases; access to public documents; and complaints about access to personal data. The fruitful discussions will no doubt be helpful for adapting to the new rules.



Targeted action increases compliance

In certain cases, the EDPS uses visits as a compliance tool. It is a way for us to take targeted action through engaging the commitment of an institution or agency to comply with the Regulation. In the past, visits have proved a particularly successful tool for increasing awareness and bringing institutions up to speed with their data protection responsibilities: nearly all eight of the EU bodies we visited in 2012 and 2013 have since shown considerable improvement in their compliance rates.

It was in this context that, in July 2014, we carried out visits to the EU Satellite Centre (EU SatCen)

and the GNSS Supervisory Authority (GSA), both of which failed to demonstrate a satisfactory data protection compliance record in the [2013 EDPS survey](#).

When conducting our survey, we found communication to be a problem: neither agency replied to our survey with sufficient evidence of satisfactory compliance by the deadline we set them. Taking this into account, we decided to conduct these visits at a working-level. This involved trainings and Q&A sessions conducted by EDPS case officers, with the aim of providing hands-on help to the agency and educating



staff and management on how best to integrate data protection principles into their working environment. The visit included discussions on issues ranging from human resources management to IT security and the tasks of different actors within the organisation in relation to data protection. Both agencies engaged with us fully and have expressed their commitment to improving compliance with data protection principles. We are planning another visit of this kind to the European Union Institute for Security Studies (EUISS) in October 2014 and hope for a similarly positive response.



Data protection standards in good health

Under Regulation 45/2001, [EU institutions and bodies](#) are all accountable to their supervisory authority, the EDPS. In other words, they are responsible for ensuring and demonstrating their compliance with data protection rules and an inspection by the EDPS is an opportunity for an institution to do this.

In March and April 2014, we conducted thematic targeted inspections at the Medical Service of the Commission and the Medical Service and the Welfare Unit of the Council. These inspections were important due both to the size of the institutions, and thus the amount of data they process, and to the particularly sensitive and personal nature of the data involved.

Our inspections focused on the obligation of professional secrecy for non-medical staff, such as secretaries and social workers; the handling and processing of personal information related to Commission and Council employees; and the physical and organisational security measures used to protect the health data processed by both institutions.

Our inspection reports of 23 July 2014 concluded that, subject to some improvement measures, both institutions are in line with the relevant personal data protection rules. We welcome the positive results of these recent inspections as a good example of two large institutions applying the principle of accountability in a sensitive field.

Dealing with allegations of scientific misconduct

To ensure the highest standards of research integrity, the European Research Council Executive Agency (ERCEA) has developed a procedure for dealing with any information it receives concerning alleged [scientific misconduct](#). This term covers a wide range of possible cases, such as fraud and the violation of regulations.

In the context of proposals submitted to the European Research Council (ERC) or projects financed by an ERC grant, the notion of scientific misconduct is interpreted in a broad sense and considered applicable whenever a person's behaviour jeopardises the value of science and, in particular, the reputation of those in the scientific community, as well as of the bodies funding or hosting these scientists. For example, if an author commits plagiarism or fails to comply with ethical standards when submitting a proposal to the ERC, that person is considered guilty of scientific misconduct.

As the agency receives allegations of scientific misconduct through



various channels, including anonymously, we addressed the issues in our [Opinion](#) of 9 July 2014. We stressed the importance of taking the appropriate steps to ensure a high level of accuracy when dealing with personal data. We also welcomed that the person alleged to have acted in breach of good scientific conduct has the opportunity to comment on the allegations against them.

We also noted that the ERCEA pays special attention to all individuals whose data might be collected as part of the procedure, such as that

of informants. We reinforced that their identities should be kept confidential as long as this does not contravene national rules regarding judicial proceedings. As stated in the EDPS [Guidelines](#) on the Rights of Individuals with regard to the Processing of Personal Data, we reminded the ERCEA that [data subjects](#) have to be informed of the main reasons for any restriction to their right of access to their data and of their right to consult the EDPS in such cases.

[EDPS Opinion](#)

Conducting an effective survey

The EDPS issued an [Opinion](#) on plans by the European Anti-Fraud Office (OLAF) to launch an analysis of the services it provides through human resources. As part of its Human Resources (HR) Strategic Plan, the institution aims to develop an HR strategy which better serves employee needs.

The process will involve each manager interviewing every jobholder individually. The answers from these interviews will be recorded on a standard questionnaire composed of various entries, such

as position in the unit, education, professional skills, previous training, comparison to ideal profile and training needs. The completed questionnaires will be submitted to OLAF's HR unit for analysis, and managers will be instructed not to retain any copies of the completed questionnaires, nor to use the data for performance evaluation purposes. Our opinion focused on the need to ensure the accuracy of the data collected. We recommended that this should be done by asking staff members to sign the questionnaire

filled in by their manager during the interview. Additionally, staff must clearly understand the purpose for which their data is being collected. Therefore, we also recommended that all participants should be informed that though the data gathered in the context of the "needs analysis" will not be used to assess performance, it will feed into the construction of individual training plans, the follow-up of which is part of the staff appraisal by their line manager.

[EDPS Opinion](#)



CONSULTATION

Banking on data protection

On 11 July 2014, the EDPS published an [Opinion](#) on two Commission proposals. The first of these concerned the resilience of the European banking system. The second addressed reporting and transparency securities financing transactions or, more simply, lending and borrowing activities associated with [shadow banking](#).

As with previous proposals in the area of financial services regulation, we recommended implementing appropriate safeguards against the mishandling of personal information. For instance, we advised that, when an individual breaches the rules, the publication of warnings and sanctions about

this identified individual should not be automatic. Instead, each individual should be assessed on a case by case basis, taking into account the need and proportionality of publishing their personal details.

[EDPS Opinion](#)



Space: the final frontier

On 11 July 2014, the EDPS issued comments on a Commission proposal for a directive on the distribution for commercial use of data collected by earth observation satellites.

The proposed directive aims to define rules for the dissemination of high resolution satellite data (HRSD). HRSD is produced by satellite operators and then distributed by data providers to the so-called value added service industry, which includes geo-information service providers, for example. These are commercial

operators who combine satellite data with other information valuable to customers. The final product is then made available to businesses which request it.

Our [Comments](#) underlined that, although in principle there were currently no data protection concerns, combining HRSD with data from the value added service industry could in many cases lead to the processing of data relating to directly or indirectly identifiable individuals. We stressed, therefore, that the processing of this data must

comply with the rules set forth in Directive 95/46/EC and in its national implementing laws.

Furthermore, though we noted that HRSD technology does not currently allow for the direct identification of individuals, technological progress could allow for this in the future. We therefore recommended that the Commission takes this possibility into account by including an article on data protection as part of the proposal.

[EDPS Comments](#)



Branching out just got easier

The Commission proposal on single member private limited liability companies is designed to make it easier for any potential company founder, and in particular for SMEs, to set-up companies in other EU member states. It aims to do this through harmonising 'the conditions of setting-up and operation of single-member limited liability companies'. In order to ensure transparency, the proposal requires registration and/or publication of certain information about the single-member

company, some of which might include personal information.

In our [Opinion](#) of 23 July 2014, we welcomed the safeguards the Commission included in their proposal, such as limiting the collection of data on an individual's disqualification to those which are currently in effect. This means that no historic data will be processed. We also welcomed the fact that the Commission specifies the possibility that information exchanges might occur through the Internal Market Information System (IMI).

However, there were some areas for improvement. In particular, we recommended that the proposal should:

- be more explicit on what personal data may be exchanged via IMI, including whether additional information can be collected with regard to disqualifications;
- more clearly specify which documents will be made publicly available and specify that any publication of information will only be made subject to data protection safeguards under national law;
- specify that the personal data made publicly available under the proposal may only be used for purposes of transparency and accountability;
- ensure that technical and organisational measures are put in place to limit accessibility to any information regarding individuals that is listed in the registers after a certain period of time has passed.

[EDPS Opinion](#)



A platform for data sharing in Europe

As part of its proposal to enhance cooperation between national enforcement authorities, the Commission and other relevant organisations in the prevention and deterrence of undeclared work, the Commission has proposed the establishment of a 'European Platform'. Composed of national enforcement authorities and the Commission, the Platform will be used to:

'examine ways to improve data sharing in compliance with the Union data protection rules, including exploring possibilities to use of the Internal Market Information System (IMI) and the Electronic Exchange of Social Security Information (EESSI)'.

Under the proposal, information sharing will only apply to information which relates to policies and measures put in

place by the member states to tackle undeclared work. As yet, information sharing does not apply to the personal data of any individual undeclared workers or individuals or organisations that employ workers without declaring them.

The EDPS issued [Comments](#) on this proposal on 23 July 2014. We welcomed the fact that it is not actually providing a legal basis for the exchange of personal data, rather, it is providing a legal basis for developing mechanisms to improve the exchange of personal data. Once the Commission proposes specific plans with regard to exchanges of personal data through this platform we will provide them with further guidance and advice on this topic.

[EDPS Comments](#)



A portal for justice across the EU

On 5 September 2014, the EDPS published an [Opinion](#) on the protection of personal data in the European eJustice Portal. The portal, designed and managed by the Commission in close cooperation with the member states, was launched in 2010. It aims to facilitate judicial cooperation and ease access to justice and cross-border electronic judicial proceedings. However, in order to fulfil these aims, all national registers must be combined and this process carries some data protection risks.



To mitigate these risks, our Opinion encouraged the Commission to increase its efforts to adopt the new regulation on eJustice. We also provided the Commission with preliminary guidance on drafting this future regulation, along with a non-exhaustive list of items that should be addressed as the portal is developed, including:

- the scope of the portal, in terms of which specific national databases will be interconnected via the portal, and what

interactive services will be provided;

- the legal grounds for the processing of data in the portal;
- the specific responsibilities of the Commission and the various other parties involved as [data controllers](#) or [processors](#), including with regard to security and data protection by design;
- the purpose limitations and restrictions, where applicable, on data combination.

[EDPS Opinion](#)



Smart policies for smart grids

On 9 March 2012, the Commission published a [recommendation](#) on preparations for the roll-out of smart metering systems. The recommendation was designed to provide guidance to member states and to ensure a high level of security and protection for consumers' personal data.

In our [Opinion](#) of 8 June 2012, we welcomed the Commission's

efforts to provide guidance to member states, though we also felt that more specific, comprehensive and practical guidance should have been provided. We were particularly enthusiastic about the Commission's plans to develop a Data Protection Impact Assessment (DPIA) template, which could be used by member

states as a tool to evaluate the potential impact of processing the personal data of consumers using smart meters and grids.

Accordingly, the Commission mandated the [Smart Grids Task Force](#) (SGTF), in conjunction with representatives from the energy industry, to produce a draft template. This has now been submitted twice to the Article 29 Working Party for an Opinion, with the EDPS playing a prominent role in the assessment work carried out.

The template will now enter a test phase before it is made available as part of a new Commission recommendation, which will define the context and terms for its review and revision. The template will also be accompanied by a document on Best Available Techniques (BAT), to which the EDPS is actively contributing through the work of the Smart Metering BAT Stakeholder Forum, which started this month. We will continue to offer support to the Commission on all matters related to smart meters and grids so as to ensure that viable solutions are found to mitigate all data protection risks.

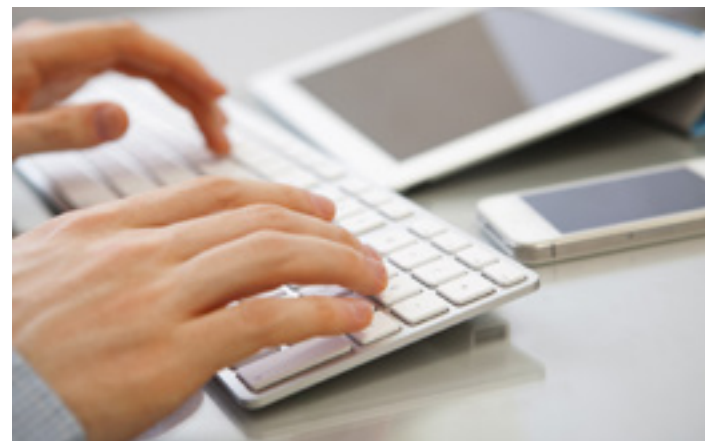


Keeping EU institutions mobile

Mobile devices are becoming increasingly common in the daily work of the EU institutions. They are offered to management and staff with specific professional needs, while others are allowed to use their own private mobile devices to help them in their tasks. Not only have the EU institutions found a way to accommodate the ever-increasing need for mobility within the institutions, but they have also seen increased employee satisfaction and cost savings.

These benefits, however, must be accompanied by an effective data protection strategy. The EDPS will soon begin a consultation

process with [EU institutions and bodies](#) to develop guidelines on the protection of personal data on mobile devices used by the EU institutions. Aimed principally at data protection officers, as well as IT and IT security staff, these guidelines will provide practical advice concerning the processing of personal data via mobile devices. They will also include a toolbox to provide guidance on the risk management process: to assess the security risks involved in using mobile devices for processing personal data and how to then put measures in place to mitigate or eliminate these risks.



The IPEN workshop: pledging privacy to technology

In response to the widening gap between user expectations concerning data protection and the reality of current technologies, the IPEN initiative hosted data protection experts and IT engineers from around Europe in Berlin on 26 September 2014. The theme of our debate was: "How can we develop internet services and apps which respect users' privacy and personal data?"

This workshop was the first organised by the Internet Privacy Engineering Network (IPEN), an initiative launched by the EDPS in 2014 (see [Newsletter 42](#)). Working in collaboration with national data protection authorities (DPAs), engineers, academics and civil society, the initiative aims to develop

engineering practices which incorporate privacy concerns and encourage engineers to build privacy mechanisms into internet standards, services and apps.

The workshop included presentations from distinguished speakers such as Peter Hustinx, EDPS; Dr. Alexander Dix, Berlin Commissioner for Data Protection and Freedom of Information; and Peter Schaar, Chairman of the European Academy for Information Freedom & Data Protection (EAID). The focus was on defining priorities for the IPEN initiative and strategies for how to achieve them.

Among the projects proposed was the creation of a 'data protection cookbook' for system development. Designed for IT

developers, this manual will provide a *step by step* guide on how to incorporate privacy considerations into internet tools and development processes. Participants also recommended the creation of a 'business process design cookbook', which aims to provide guidance to businesses using IT solutions.

In addition, participants agreed on the necessity of finding ways to bridge the communication gap between lawyers and engineers. It was agreed that greater understanding and cooperation between the two communities is essential to ensure that personal data protection is incorporated in the technology that we use on a daily basis.

Following the success of its first workshop, the IPEN initiative is

now focused on developing and addressing the projects it has prioritised. IPEN will continue to explore ways to develop privacy-friendly technologies and to ensure that privacy becomes an essential consideration for all IT developers.

More information on the IPEN initiative, including how to sign up to our mailing list, is available on our website.

[IPEN Website](#)

[Press Release](#)



Three years in EU data protection reform: state of play and perspectives, Brussels



The recent rulings of the Court of Justice of the European Union on data retention and search engines (Google Spain) illustrate the increasing relevance of the fundamental rights to privacy

and data protection in new information services and data transfers.

Against the backdrop of rapid technological developments and the growing reality of ubiquitous

surveillance of personal data by private and public entities alike, the EU is striving to put in place rules that will effectively protect personal data in an interconnected world.

On 5 November 2014, Andrea Voßhoff, the German Federal Commissioner for Data Protection and Freedom of Information and Peter Hustinx, EDPS, will welcome senior institutional and political

representatives to debate the outstanding issues and steps to be taken to bring the reform of EU data protection law to a timely and successful conclusion.

[More information](#)

EU data protection competition announced

From 6 November to 9 December 2014, the European Personnel Selection Office (EPSO) will be accepting registrations for an EU competition on data protection. Candidates who succeed in the exams will then be able to apply for posts of administrator (AD6) in the field of data protection within the EU institutions and bodies.

[More information](#)

The EDPS newsletter: what do you think?

We're interested in your views about our newsletter so that we can make it an even better read for you! There are nine questions about what you think of our newsletter which will take you 8-10 minutes to answer.

The survey is completely anonymous unless you want to take part in a prize draw where you can win one of 20 stylus pens. If you give us an email address, we can let you know if you are one of the 20 lucky winners and then we'll delete it from our files.

Your feedback is important to us and will help us to improve our newsletter and your experience of it so we encourage you to take part in our survey.

[EDPS Newsletter Survey](#)



DATA PROTECTION OFFICERS

Recent appointments

- Mr. Massimo Attoresi, European Data Protection Supervisor (EDPS)



French and German versions of this newsletter will be online shortly.

SPEECHES AND PUBLICATIONS

- "Ensuring more effective data protection in an age of big data", contribution ([PDF](#)) by Peter Hustinx to European Voice online debate on big data and consent (14 July 2014)
- "European Leadership in Privacy and Data Protection", article ([PDF](#)) by Peter Hustinx which will be published in "La propuesta de Reglamento Europeo de Protección de Datos: principales desafíos actuales", Castellon 2014 (8 September 2014)
- "European Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", article ([PDF](#)) by Peter Hustinx based on a course given at the European University Institute's Academy of European Law in July 2013 which will be published in "Collected Courses of the European University Institute's Academy of European Law, 1-12 July 2013", (15 September 2014)
- "A World Order for Data Protection – Our Dream Coming True?", speech ([PDF](#)) by Peter Hustinx during the 36th International Conference of Data Protection and Privacy Commissioners, Plenary II – Privacy with no Territorial Bounds, Balaclava Fort, Mauritius (15-16 October 2014)



About this newsletter

This newsletter is issued by the European Data Protection Supervisor (EDPS) – 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.

CONTACTS


www.edps.europa.eu
Tel: +32 (0)2 2831900
Fax: +32 (0)2 2831950
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

 Follow us on Twitter:
[@EU_EDPS](#)

© Photos: iStockphoto/EDPS & European Union

EDPS - The European guardian of data protection