Council of the
European Union

Brussels, 6 April 2016
(OR. en)

7587/16

DATAPROTECT 22
JAI 254
MI 196
DIGIT 28
DAPIX 48
FREMP 57
POLGEN 26

COVER NOTE

Subject:	EU institutions and personal data protection accountability - A background paper

Delegations will find in the Annex a background paper by the European Data Protection Supervisor.

EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
SUPERVISOR

SECRÉTARIAT GÉNÉRAL DU
CONSEIL DE L'UNION EUROPÉENNE
SGE16/03248
Reçu le 05-04-2016
DEST. PRINC. Mme ROGER
DEST. COPISTES Mme LOPEZ RUIZ
Service Juridique

Mr Jeppe TRANHOLM-MIKKELSEN
Secretary-General of the General
Secretariat of the Council
General Secretariat of the Council
Rue de la Loi/Wetstraat 175
B-1048 Bruxelles/Brussel

Brussels, 01 April 2016
GB/UK/sn/D(2016)0689 **C 2016-0158**
Please use edps@edps.europa.eu for all correspondence

Subject: Implementing the Principle of Accountability in Data Protection

Dear Mr Tranholm-Mikkelsen,

EU data protection reform is about to touch the EU institutions themselves. The General Data Protection Regulation (GDPR) and the Directive on personal data processing in the police and judicial area will shortly be adopted, and this year the Commission is expected to adopt a proposal for revising Regulation 45/2001, the rules governing how EU institutions process personal information. In early 2017, as a result of a public consultation, the Commission may also to adopt a proposal for revising the rules on confidentiality of communications currently set out in Directive 2002/58/EC.

One of the most important innovations of the GDPR is the incorporation of the concept of accountability. This involves efforts to enable all institutions, including your organisation, to go beyond mere compliance with data protection rules, introduce a proactive policy, allocate internal responsibilities and install a data protection governance model. In short, this means that at the most senior level organisations are responsible for complying and demonstrating compliance with the rules. This goes hand in hand with the drive to reduce bureaucracy and place greater emphasis on safeguards for the individual rather than administrative procedures. This is challenging for all institutions, but, of course, in particular for the larger ones.

As part of your risk management and due diligence activities, we as the data protection authority for EU institutions would like to help prepare you for the forthcoming changes and

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

their gradual implementation over time. We have therefore launched the EDPS Accountability Project, which will enable institutions, beginning with our own organisation, to integrate fully the concept into how data is handled in the performance of our tasks.

In our view this process requires endorsement at the highest level of the organisation. We also regard your direct contact with middle management and your DPO as instrumental; next to you, they will have a central role to play. As part of the accountability project, we consider that an initial high level meeting would be very useful. My office will be in touch with yours to find a date for a visit in the coming months which is convenient for you.

Thank you for your cooperation in this exercise. I look forward to working with you.

Giovanni BUTTARELLI

Cc: Ms Carmen LOPEZ RUIZ, DPO Council of the European Union

Annex: EU institutions and personal data protection accountability: A background paper

EU institutions and personal data protection accountability: A background paper

What is accountability?

In many ways, accountability is not new to EU institutions. Whilst Regulation 45/2001 does not specifically articulate the principle of accountability, it is, for example, implicit in the already existing requirement under Article 4(2) on the controller to ensure that the requirement of data quality is complied with. However, whilst the legal responsibility for compliance has always been with the controller, this has so far often produced mainly formal results.

With the new EU General Data Protection Regulation GDPR comes a quantum shift in emphasis: controllers are responsible – not Data Protection Authorities or Data Protection Officers. Accountability goes beyond compliance with the rules - it implies culture change. And the principle of accountability is meant to take data protection from theory into practice in the digital age.

The last few years have seen an exponential rise in volumes of personal data in storage and in circulation. Increasingly this information is not provided by the individual him- or herself but rather observed, derived or computed, with granular inferences about individuals drawn from statistics through advanced analytics based on algorithms. At best, individuals may be aware at first of this information processing, but they may also soon forget, at worst, individuals are passive objects of this processing or anticipate it at all. This risks processing which is unfair or discriminatory, and which entrenches stereotypes and social exclusion. Accountability should promote sustainable data processing, by ensuring that the task of assessing the legality and fairness of complex processing falls primarily on controllers - with the guidance of regulators - and not on the individual.

The EDPS has long advocated that EU institutions and bodies exercise accountability. The concept has developed since its introduction in the 1980 OECD Guidelines, through the 2009 International Conference of Data Protection and Privacy Commissioners the 'Madrid International Standards', the ISO draft standard 29100 and the APEC privacy framework and its cross border privacy rules and a 2012 workshop hosted by EDPS and other data protection authorities. It is now an explicit pillar of the new EU data protection framework in Article 22 of the General Data Protection Regulation (and defined in Article 5(2)), requiring controllers to implement appropriate technical and organisational measures to ensure and demonstrate compliance. Regulation 45/2001, applicable to the EU institutions, governs how they process personal information, and it is to be revised in 2016 to ensure consistency with the new EU General Data Protection Regulation.

Accountability in personal data processing consists of four stages:

1. Transparent internal data protection and privacy policies, approved and endorsed by the highest level of the organisation's management.
2. Informing and training all people in the organisation on how to implement the policies.

3. Responsibility at the highest level for monitoring this implementation, assessing and demonstrating to external stakeholders and supervisory authorities the quality of the implementation.
4. Procedures for redressing poor compliance and data breaches.

'Leading by example': The EDPS Accountability Project

In our 2015-2019 strategy, our overarching goal is for the EU to lead by example in data protection, starting with ourselves and with EU institutions as data controllers in our own right. Our own internal accountability matrix, for example, consists of:

- The Supervisors as holders of ultimate accountability for how personal data is processed in the performance of our tasks.
- The EDPS Director as the senior official responsible for the EDPS Secretariat, as the appointing authority who nominates and - to whom directly reports - the Data Protection Officer.
- The Data Protection Officer responsible for promoting a culture of accountability, adherence to EDPS guidelines for complying with Regulation 45/2001 and leads the internal accountability project.
- Heads of unit and of sector, the Data Protection Officer and other staff with specific responsibilities like the Local Security Officer, Local Informatics Security Officer and the Records Manager share delegated responsibilities, support the director and apply the EDPS guidelines.

One tool for implementing the accountability principle is a set of questions for everyone who is part of this accountability matrix. This is the main means of assessing periodically and in line with the annual planning cycle, the quality of the high level technical and organisational measures .

The Supervisor intends to carry out several visits in 2016 to introduce the accountability principle among the institutions.

We will explain the new obligations resulting from the revised legal framework and the implications for EU institutions and our work as a supervisor. It is essential for each institution at the most senior level to endorse and take responsibility for personal data processing which occurs as part of the tasks of the institution. More detailed discussions can take place with staff with the assistance of the local Data Protection Officer. This will enable the institutions to perform effective risk management and to identify solutions appropriate for their specific circumstances and functions, with the emphasis on minimising bureaucratic procedures while strengthening safeguards for the individual.

We will report on this project towards the end of 2016, which will provide a basis for an EDPS Opinion on the principle and application of accountability in personal data processing.

Further reading

WP29 Opinion on purpose limitation

EDPS Policy Paper Monitoring and Ensuring Compliance with Regulation (EC) 45/2001

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Policy on Consultations in the field of Supervision and Enforcement

EDPS Strategy 2015-2029

EDPS Opinion 'Towards a New Digital Ethics', September 2016.

Working Party 29 Opinion on the principle of accountability

3