EDPS launches Accountability Initiative

The General Data Protection Regulation (GDPR) and the Directive on personal data processing in the police and judicial area were adopted last month, and this year the Commission is expected to adopt a proposal for the review of Regulation 45/2001, the rules governing how EU institutions process personal information. These are expected to reflect the changes brought about by the GDPR - EU data protection reform is therefore about to touch the EU institutions themselves.

With the visit to the European Court of Auditors on 1 June 2016, the EDPS initiated a series of accountability visits to small, medium and big EU institutions and bodies to explain the new obligations as a result of the revised legal framework and the implications for EU institutions and the EDPS' work as their supervisory authority. Whilst this accountability initiative specifically targets EU institutions and bodies, other data protection authorities and controllers outside the EU institutions may also find this guidance helpful.

EU institutions and bodies should, at the most senior level, endorse and take responsibility for personal data processing inside their organisations which occurs as part of the tasks of the institution. The EDPS, leading by example, is conducting an internal accountability exercise (see samples **here**) that may lead at a later stage to the sharing of some practical tools tested and some lessons learned.

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 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 GDPR, however, comes a quantum shift in emphasis: controllers are responsible – not data protection authorities or data protection officers alone. Accountability goes beyond compliance with the rules - it implies culture change.

Accountability in personal data processing involves:

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.

The GDPR in Article 5(2) includes a direct reference to ***accountability*** as a principle and Article 22 GDPR requires appropriate technical and organisational measures (further described in other Articles) to ensure and demonstrate compliance. Other examples of new obligations under the GDPR include documentation, data security, data protection impact assessments (DPIA) and data protection by design & by default.

The EDPS has recently provided guidance on two pillars of accountability: on **security measures in the sense of Article 22 of Regulation 45/2001** (on what EU institutions should do to comply with their security obligations) and on the elements of a DPIA. In the GDPR, both the obligations for information security based on state of the art risk management (Article 32) and for a DPIA are included. In this process, a risk assessment is the starting point. The use of the same words in both obligations makes it more difficult to recognise the differences, but the **EDPS has clarified** that the objective of a DPIA is much broader than the security of processing.

This factsheet 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.

CONTACTS

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

POSTAL ADDRESS

EDPS
Rue Wiertz 60 - MTS Building
B- 1047 Brussels
BELGIUM

OFFICE ADDRESS

Rue Montoyer 30
B-1000 Brusels
BELGIUM

EDPS
European Data Protection Supervisor

www.edps.europa.eu

@EU_EDPS EDPS European Data Protection Supervisor