Personal data protection: processing and free movement of data (General Data Protection Regulation)

2012/0011(COD) - 10/10/2014

The Council reached a **partial general approach** on specific aspects of the draft regulation setting out a general EU framework for data protection. The partial general approach includes **chapter IV of the draft regulation (controller and processor),** on the understanding that:

- nothing is agreed until everything is agreed;
- it is without prejudice to any horizontal questions;
- it does not mandate the presidency to engage in informal trilogues with the European Parliament on the text.

Chapter IV was discussed intensively during the first half of 2013. Whilst at the Council meeting on 6-7 June 2013, all delegations congratulated the Irish Presidency on the very important progress achieved in this regard, a number of issues were still outstanding, in particular the need to further **reduce the administrative burden/compliance costs flowing from this Regulation by sharpening the risk-based approach**.

According to the approach, the likelihood and severity of the risk should be determined in function of the nature, scope, context and purposes of the data processing. **Risk should be evaluated on an objective assessment**, by which it is established whether data processing operations involve a high risk.

A high risk is a particular risk of prejudice to the rights and freedoms of individuals, in particular:

- where data processing which could lead to physical, material or moral damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, [breach of (…) pseudonymity], or any other significant economic or social disadvantage;
- where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable individuals, in particular of children, are processed;
- where processing involves a large amount of personal data and affects a large number of data subjects.

The orientation prescribed that **where a controller not established in the Union** is processing personal data of data subjects residing in the Union, the controller should designate a representative, **unless the processing it carries out is occasional** and unlikely to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing or the controller is a public authority or body.

The representative should be explicitly designated by a written mandate of the controller to act on its behalf with regard to the latter's obligations under this Regulation. The controller or processor should **maintain records** regarding all categories of processing activities under its responsibility.

In **assessing data security risk**, consideration should be given to the risks that are presented by data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, which may in particular lead to physical, material or moral damage.

In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller [or the processor] should be responsible for the carrying out of a **data protection impact assessment to evaluate**, in particular, the origin, nature, particularity and severity of this risk.