COMP Article 22
15.10.2013

Article 22
Responsibility *and accountability* of the controller

1. The controller shall adopt ***appropriate*** policies and implement appropriate ***and demonstrable technical and organizational*** measures to ensure and be able to demonstrate ***in a transparent manner*** that the processing of personal data is performed in compliance with this Regulation, ***having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself***.

1a. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary.

~~***2. The measures provided for in paragraph 1 shall in particular include:***~~

~~***(a) keeping the documentation pursuant to Article 28;***~~

~~***(b) implementing the data security requirements laid down in Article 30;***~~

~~***(c) performing a data protection impact assessment pursuant to Article 33;***~~

~~***(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);***~~

~~***(e) designating a data protection officer pursuant to Article 35(1);***~~

3. The controller shall ~~***implement mechanisms to ensure the verification of***~~ ***be able to demonstrate*** the ***adequacy and*** effectiveness of the measures referred to in paragraphs 1 and 2. ~~***If proportionate, this verification shall be carried out by independent internal or external auditors.***~~ ***Any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary description of the policies and measures referred to in paragraph 1.***

3a. The controller shall have the right to transmit personal data inside the Union within the group of undertakings the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct ass referred to in Article 38.

~~***4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2,***~~

~~***the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.***~~

Recitals

(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established**,** ***in particular with regard to documentation, data security, impact assessments, the data protection officer and oversight by data protection authorities***. In particular, the controller should ensure and be ~~***obliged***~~ ***able*** to demonstrate the compliance of each processing operation with this Regulation. ***This should be verified by independent internal or external auditors.***