COMP Article 31
17.10.2013

Article 31
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay ~~***and, where feasible, not later than 24 hours after having become aware of it,***~~ notify the personal data breach to the supervisory authority. ~~***The notification to the supervisory authority shall be accompanied by a reasoned justification where it is not made within 24 hours***~~.

2. ~~***Pursuant to point (f) of Article 26(2),***~~ ***T***he processor shall alert and inform the controller ***without undue delay*** ~~***immediately***~~ after the establishment of a personal data breach.

3. The notification referred to in paragraph 1 must at least:
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;
(c) recommend measures to mitigate the possible adverse effects of the personal data breach;
(d) describe the consequences of the personal data breach;
(e) describe the measures proposed or taken by the controller to address the personal data breach ***and mitigate its effects***.
The information may if necessary be provided in phases.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must ***be sufficient to*** enable the supervisory authority to verify compliance with this Article ***and with Article 30***. The documentation shall only include the information necessary for that purpose.

4a. The supervisory authority shall keep a public register of the types of breaches notified.

5. The ***European Data Protection Board*** ~~***Commission***~~ shall be ***entrusted with the task*** ~~***empowered to adopt delegated acts in accordance with Article 86 for the purpose***~~ of ***issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b)*** ~~***further specifying the criteria and requirements***~~ for establishing the data breach ***and determining the undue delay*** referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

~~*6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Recitals

(67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial economic loss and social harm, including identity fraud, to the individual concerned. Therefore~~*, as soon as the controller becomes aware that such a breach has occurred,*~~ the controller should notify the breach to the supervisory authority without undue delay, ***which should be presumed to be not later than*** ~~*and, where feasible, within*~~ ***72*** hours. ~~*Where this cannot be achieved within 24 hours*~~***. If applicable,*** an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.