REGULATIONS

COMMISSION REGULATION (EU) No 611/2013

of 24 June 2013

on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [1], and in particular Article 4(5) thereof,

Having consulted the European Network and Information Security Agency (ENISA),

Having consulted the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [2] (the Article 29 Working Party),

Having consulted the European Data Protection Supervisor (EDPS),

Whereas:

(1) Directive 2002/58/EC provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Union.

(2) Under Article 4 of Directive 2002/58/EC, providers of publicly available electronic communications services are obliged to notify the competent national authorities, and in certain cases also the subscribers and individuals concerned, of personal data breaches. Personal data breaches are defined in Article 2(i) of Directive 2002/58/EC as breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Union.

(3) In order to ensure consistency in implementation of the measures referred to in Article 4(2), (3) and (4) of Directive 2002/58/EC, Article 4(5) thereof empowers the Commission to adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in that Article.

(4) Different national requirements in this regard may lead to legal uncertainty, more complex and cumbersome procedures and significant administrative costs for providers operating cross-border. The Commission therefore considers it necessary to adopt such technical implementing measures.

(5) This Regulation is limited to the notification of personal data breaches and therefore does not set out technical implementing measures concerning Article 4(2) of Directive 2002/58/EC on informing the subscribers in case of a particular risk of a breach of the security of the network.

(6) It follows from the first subparagraph of Article 4(3) of Directive 2002/58/EC that providers should notify to the competent national authority all personal data breaches. Therefore, no discretion should be left to the provider whether or not to notify to the competent national authority. However, this should not prevent the competent national authority concerned from prioritising the investigation of certain breaches in the way it sees fit in accordance with the applicable law, and to take steps as necessary to avoid over- or under-reporting of personal data breaches.

(7) It is appropriate to provide for a system for the notification of personal data breaches to the competent national authority, which consists, where certain conditions are fulfilled, of various stages, each subject to certain time limits. This system is meant to ensure that the competent national authority is informed as early and as fully as possible, without however unduly hindering the provider in its efforts to investigate the breach and to take the necessary measures to confine it and remedy the consequences thereof.

[1] OJ L 201, 31.7.2002, p. 37.
[2] OJ L 281, 23.11.1995, p. 31.

(8) Neither a simple suspicion that a personal data breach has occurred, nor a simple detection of an incident without sufficient information being available, despite a provider's best efforts to this end, suffices to consider that a personal data breach has been detected for the purposes of this Regulation. Particular regard should be had in this connection to the availability of the information referred to in Annex I.

(9) In the context of the application of this Regulation the competent national authorities concerned should cooperate in cases of personal data breaches having a cross-border dimension.

(10) This Regulation does not provide for additional specification of the inventory of personal data breaches that providers are to maintain, given that Article 4 of Directive 2002/58/EC specifies its content exhaustively. However, providers may refer to this Regulation to determine the format of the inventory.

(11) All competent national authorities should make available a secure electronic means for providers to notify personal data breaches in a common format, based on a standard such as XML, containing the information set out in Annex I in the relevant languages, so as to enable all providers within the Union to follow a similar notification procedure irrespective of where they are located or where the personal data breach occurred. In this connection, the Commission should facilitate the implementation of the secure electronic means by convening meetings with the competent national authorities where necessary.

(12) When assessing whether a personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, account should be taken, in particular, of the nature and content of the personal data concerned, in particular where the data concerns financial information, such as credit card data and bank account details; special categories of data referred to in Article 8(1) of Directive 95/46/EC; and certain data specifically related to the provision of telephony or internet services, i.e. e-mail data, location data, internet log files, web browsing histories and itemised call lists.

(13) In exceptional circumstances, the provider should be permitted to delay the notification to the subscriber or individual, where the notification to the subscriber or individual may put at risk the proper investigation of the personal data breach. In this context, exceptional circumstances may include criminal investigations, as well as other personal data breaches that are not tantamount to a serious crime but for which it may be appropriate to postpone notification. In any event, it should be for the competent national authority to assess, in each case and in the light of the circumstances, whether to agree to the postponement or require the notification.

(14) While providers should have contact details of their subscribers, given their direct contractual relationship, such information may not exist for other individuals adversely affected by the personal data breach. In such a case, the provider should be permitted to notify those individuals initially through advertisements in major national or regional media, such as newspapers, to be followed as soon as possible by an individual notification as provided for in this Regulation. The provider is therefore not obliged as such to notify through media, but rather is mandated to act in this way, if it so wishes, when it is still in the process of identifying all individuals affected.

(15) The information about the breach should be dedicated to the breach and not associated with information about another topic. For example, inclusion of information about a personal data breach in a regular invoice should not be considered as an adequate means to notify a personal data breach.

(16) This Regulation does not set out specific technological protection measures that justify derogation from the obligation to notify personal data breaches to subscribers or individuals, as these may change over time as technology advances. The Commission should, however, be able to publish an indicative list of such specific technological protection measures according to current practices.

(17) Implementing encryption or hashing should not be considered sufficient by itself to allow providers to claim more broadly they have fulfilled the general security obligation set out in Article 17 of Directive 95/46/EC. In this regard, providers should also implement adequate organisational and technical measures to prevent, detect and block personal data breaches. Providers should consider any residual risk that may be present after controls have been implemented in order to understand where personal data breaches may potentially occur.

(18) Where the provider uses another provider to perform part of the service, for example in relation to billing or management functions, this other provider, which has no direct contractual relationship with the end user, should not be obliged to issue notifications in the case of a personal data breach. Instead, it should alert and inform the provider with which it has a direct contractual relationship. This should apply also in the context of

wholesale provision of electronic communications services, when typically the wholesale provider does not have a direct contractual relationship with the end user.

(19) Directive 95/46/EC defines a general framework for personal data protection in the European Union. The Commission has presented a proposal for a Regulation of the European Parliament and of the Council to replace Directive 95/46/EC (the Data Protection Regulation). The proposed Data Protection Regulation would introduce an obligation for all data controllers to notify personal data breaches, building on Article 4(3) of Directive 2002/58/EC. The present Commission Regulation is fully consistent with this proposed measure.

(20) The proposed Data Protection Regulation also makes a limited number of technical adjustments to Directive 2002/58/EC to take account of the transformation of Directive 95/46/EC into a Regulation. The substantive legal consequences of the new Regulation for the Directive 2002/58/EC will be the object of a review by the Commission.

(21) The application of this Regulation should be reviewed three years after its entry into force, and its content reviewed in the light of the legal framework in place at that time, including the proposed Data Protection Regulation. The review of this Regulation should be linked where possible to any future review of Directive 2002/58/EC.

(22) The application of this Regulation may be assessed based, inter alia, on any statistics maintained by competent national authorities of the personal data breaches of which they are notified. These statistics may include, for example, information on number of personal data breaches notified to the competent national authority, number of personal data breaches notified to the subscriber or individual, the time taken to resolve the personal data breach, and whether technological protection measures were taken. These statistics should provide the Commission and the Member States with consistent and comparable statistical data, and should reveal neither the identity of the notifying provider nor of the subscribers or individuals involved. The Commission may also hold regular meetings with competent national authorities and other interested stakeholders for this purpose.

(23) The measures provided for in this Regulation are in accordance with the opinion of the Communications Committee,

HAS ADOPTED THIS REGULATION:

Article 1

Scope

This Regulation shall apply to the notification of personal data breaches by providers of publicly available electronic communications services ('the provider').

Article 2

Notification to the competent national authority

1. The provider shall notify all personal data breaches to the competent national authority.

2. The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible.

The provider shall include in its notification to the competent national authority the information set out in Annex I.

Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

3. Where all the information set out in Annex I is not available and further investigation of the personal data breach is required, the provider shall be permitted to make an initial notification to the competent national authority no later than 24 hours after the detection of the personal data breach. This initial notification to the competent national authority shall include the information set out in Section 1 of Annex I. The provider shall make a second notification to the competent national authority as soon as possible, and at the latest within three days following the initial notification. This second notification shall include the information set out in Section 2 of Annex I and, where necessary, update the information already provided.

Where the provider, despite its investigations, is unable to provide all information within the three-day period from the initial notification, the provider shall notify as much information as it disposes within that timeframe and shall submit to the competent national authority a reasoned justification for the late notification of the remaining information. The provider shall notify the remaining information to the competent national authority and, where necessary, update the information already provided, as soon as possible.

4. The competent national authority shall provide to all providers established in the Member State concerned a secure electronic means for notification of personal data breaches and information on the procedures for its access and use. Where necessary, the Commission shall convene meetings with competent national authorities to facilitate the application of this provision.

5. Where the personal data breach affects subscribers or individuals from Member States other than that of the competent national authority to which the personal data breach has been notified, the competent national authority shall inform the other national authorities concerned.

To facilitate the application of this provision, the Commission shall create and maintain a list of the competent national authorities and the appropriate contact points.

Article 3

Notification to the subscriber or individual

1. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall, in addition to the notification referred to in Article 2, also notify the subscriber or individual of the breach.

2. Whether a personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual shall be assessed by taking account of, in particular, the following circumstances:

(a) the nature and content of the personal data concerned, in particular where the data concerns financial information, special categories of data referred to in Article 8(1) of Directive 95/46/EC, as well as location data, internet log files, web browsing histories, e-mail data, and itemised call lists;

(b) the likely consequences of the personal data breach for the subscriber or individual concerned, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation; and

(c) the circumstances of the personal data breach, in particular where the data has been stolen or when the provider knows that the data are in the possession of an unauthorised third party.

3. The notification to the subscriber or individual shall be made without undue delay after the detection of the personal data breach, as set out in the third subparagraph of Article 2(2). That shall not be dependent on the notification of the personal data breach to the competent national authority, referred to in Article 2.

4. The provider shall include in its notification to the subscriber or individual the information set out in Annex II. The notification to the subscriber or individual shall be expressed in a clear and easily understandable language. The provider shall not use the notification as an opportunity to promote or advertise new or additional services.

5. In exceptional circumstances, where the notification to the subscriber or individual may put at risk the proper investigation of the personal data breach, the provider shall be permitted, after having obtained the agreement of the competent national authority, to delay the notification to the subscriber or individual until such time as the competent national authority deems it possible to notify the personal data breach in accordance with this Article.

6. The provider shall notify to the subscriber or individual the personal data breach by means of communication that ensure prompt receipt of information and that are appropriately secured according to the state of the art. The information about the breach shall be dedicated to the breach and not associated with information about another topic.

7. Where the provider having a direct contractual relationship with the end user, despite having made reasonable efforts, is unable to identify within the timeframe referred to in paragraph 3 all individuals who are likely to be adversely affected by the personal data breach, the provider may notify those individuals through advertisements in major national or regional media, in the relevant Member States, within that timeframe. These advertisements shall contain the information set out in Annex II, where necessary in a condensed form. In that case, the provider shall continue to make all reasonable efforts to identify those individuals and to notify to them the information set out in Annex II as soon as possible.

Article 4

Technological protection measures

1. In derogation from Article 3(1), notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent national authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

2. Data shall be considered unintelligible if:

(a) it has been securely encrypted with a standardised algorithm, the key used to decrypt the data has not been compromised in any security breach, and the key used to decrypt the data has been generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key; or

(b) it has been replaced by its hashed value calculated with a standardised cryptographic keyed hash function, the key used to hash the data has not been compromised in any security breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access the key.

3. The Commission may, after having consulted the competent national authorities via the Article 29 Working Party, the European Network and Information Security Agency and the European Data Protection Supervisor, publish an indicative list of appropriate technological protection measures, referred to in paragraph 1, according to current practices.

Article 5

Use of another provider

Where another provider is contracted to deliver part of the electronic communications service without having a direct contractual relationship with subscribers, this other provider shall immediately inform the contracting provider in the case of a personal data breach.

Article 6

Reporting and review

Within three years from the entry into force of this Regulation, the Commission shall provide a report on the application of this Regulation, its effectiveness and its impact on providers, subscribers and individuals. On the basis of that report the Commission shall review this Regulation.

Article 7

Entry into force

This Regulation shall enter into force on 25 August 2013.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 24 June 2013.

For the Commission
The President
José Manuel BARROSO

ANNEX I

Content of the notification to the competent national authority

Section 1

Identification of the provider

1. Name of the provider

2. Identity and contact details of the data protection officer or other contact point where more information can be obtained

3. Whether it concerns a first or second notification

Initial information on the personal data breach (for completion in later notifications, where applicable)

4. Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident

5. Circumstances of the personal data breach (e.g. loss, theft, copying)

6. Nature and content of the personal data concerned

7. Technical and organisational measures applied (or to be applied) by the provider to the affected personal data

8. Relevant use of other providers (where applicable)

Section 2

Further information on the personal data breach

9. Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved):

10. Number of subscribers or individuals concerned

11. Potential consequences and potential adverse effects on subscribers or individuals

12. Technical and organisational measures taken by the provider to mitigate potential adverse effects

Possible additional notification to subscribers or individuals

13. Content of notification

14. Means of communication used

15. Number of subscribers or individuals notified

Possible cross-border issues

16. Personal data breach involving subscribers or individuals in other Member States

17. Notification of other competent national authorities

ANNEX II

Content of the notification to the subscriber or individual

1. Name of the provider

2. Identity and contact details of the data protection officer or other contact point where more information can be obtained

3. Summary of the incident that caused the personal data breach

4. Estimated date of the incident

5. Nature and content of the personal data concerned as referred to in Article 3(2)

6. Likely consequences of the personal data breach for the subscriber or individual concerned as referred to in Article 3(2)

7. Circumstances of the personal data breach as referred to in Article 3(2)

8. Measures taken by the provider to address the personal data breach

9. Measures recommended by the provider to mitigate possible adverse effects