



E-PRIVACY DIRECTIVE: Personal Data Breach Notification



PUBLIC CONSULTATION

BEUC Response

Contact: Kostas Rossoglou – digital@beuc.eu

Ref.: X/2011/092 - 13/09/11

BEUC, the European Consumers' Organisation
80 rue d'Arlon, 1040 Bruxelles - +32 2 743 15 90 - www.beuc.eu

 EC register for interest representatives: identification number 9505781573-45 

Summary

The European Consumers' Organisation welcomes the launch of the consultation on the implementation of the data breach notification requirement as required by the revised e-privacy Directive. Further guidance is needed to ensure the coherence of national rules regarding the circumstances, the format and the procedures applicable to notification of data breaches. In particular, BEUC has identified a number of areas where further guidance is necessary:

- ✚ The definition of **'adverse effect' of data breaches should be risk-based**, taking into account both quantitative and qualitative indicators while reflecting not only economic losses, but also immaterial damages;
- ✚ **Notification to the authorities should occur as soon as the breach has been identified**, at the latest within one week, and should include all relevant information;
- ✚ In case the complete information is unavailable within the specific deadline, the **notification could be spread over time** with the initial notification taking place as soon as the breach has been identified and with follow up notifications being sent as breach details become available;
- ✚ The **notification to the individuals** should be given in such a time as to enable the individual to mitigate the adverse effects of the breach. In order to prevent notification fatigue, it should be for the competent authority to decide whether individuals need to be notified and instruct the service provider accordingly;
- ✚ **Individuals should be informed** about the personal information involved in the breach, the timing, the person/entity responsible for the breach and the number of people affected;
- ✚ It is crucial to provide individuals with **clear information as to recommended actions and practical advice** to mitigate the adverse effects, as well as means of seeking redress;
- ✚ BEUC would support the development of **standard EU format** for notification which should at least include the headlines to be addressed in the notification, e.g. description of the breach; the effects and the measures taken; and the recommended actions for individuals.
- ✚ Given that it is almost impossible to ensure the full anonymisation of personal data, the **effectiveness of technical protection measures will have to be assessed on an *ad hoc* basis**;
- ✚ The notification requirement should be extended to **breaches** occurring while personal data is being processed **by the data processor**;

BEUC would also like to reiterate its support for the introduction of **a horizontal data breach notification obligation beyond the telecommunications sector**. A general breach notification obligation should be construed on the basis of the provisions of the revised e-privacy Directive. Therefore, we call upon the European Commission to use the feedback from the current consultation in the ongoing revision of the Data Protection Directive.

INTRODUCTION

BEUC welcomes the opportunity to submit its views on the implementation of specific aspects of the data breach notification obligation that has been introduced in the revised e-privacy Directive¹. It is important to ensure the consistency of national legislation, particularly with respect to the circumstances, format and procedures applicable to notification of data breaches, thus allowing individuals to enjoy an equally high level of protection across the Community.

BEUC would also like to reiterate its support for the introduction of a horizontal data breach notification obligation beyond the telecommunications sector. Consumers can suffer at least the same harm from the undue disclosure of their bank account details as from the disclosure of their telephone bills. From the consumer's perspective, it does not matter whether personal data are lost by a provider of communication services or by someone else.

A general breach notification obligation should be construed on the basis of the provisions of the revised e-privacy Directive, which has achieved a fair balance between the fundamental right of data subjects to be informed about the handling of their personal data and the need to avoid notification fatigue. Therefore, we call upon the European Commission to use the feedback from the current consultation in the ongoing revision of the Data Protection Directive.

CIRCUMSTANCES OF PERSONAL DATA BREACH NOTIFICATIONS

Notifying the national authority

Question 1: Does your organisation handle personal data breaches?

Question 2: If yes, how does your organisation handle personal data breaches currently, and how does it comply, or intend to comply, with this new obligation? What procedures does it have in place? What would be examples of the most common types of personal data breach?

BEUC shares the position of the European Commission that the provisions of the revised e-privacy Directive regarding the definition of data breach are clear enough to allow for harmonised national rules. However, we are concerned that the different implementation of the definition of personal data, as in the Data Protection Framework Directive², might result in different implementation of the data breach notification obligation.

¹ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

² Article 2.a Article 2.a of the Data Protection Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

BEUC believes the definition of what information constitutes personal data should be in line with the Data Protection Directive and the guidance provided by Article 29 Data Protection Working Party³. The current broad definition provides the necessary flexibility to adapt to rapid technological developments and should therefore be reiterated in the revised framework. The issue which needs to be addressed is not the definition itself, but rather the different interpretations and the subsequent lack of clarity at national level. Clarification could be provided by the Article 29 Working Party within the framework of the enhanced role it should assume in the future.

It is also important to note that the data breach notification should be interpreted as also covering breaches occurring while personal data is being processed by the data processor. As there is no obligation for the data processor to notify breaches to relevant authorities and to individuals, the data controller should be responsible for notifying the authority.

Notifying the subscriber or individual

Question 3: In your view, what types of breaches would adversely affect the subscriber or individual? In what kinds of cases has your organisation notified the subscriber or individual so far, or received such notifications?

Individuals have the right to be informed about the use of their personal data, including when their data have been compromised. The right to information is a fundamental principle of the EU Data Protection Framework⁴ and therefore applies to the sector specific e-privacy Directive. According to the research carried out by the UK consumer organisation Which?, the vast majority of UK consumers (74%) would always wish to be notified of a data breach.

BEUC recognises that a general obligation to notify individuals whenever personal data has been compromised might be counter-productive and lead to “notification fatigue” and desensitisation. This risk has been taken into consideration in the provision of revised e-privacy Directive which has achieved a fair balance in providing meaningful notification while respecting the right to be informed.

As regards the definition of breaches that would *likely adversely affect* the individual, BEUC supports a broad definition that would encompass not only those breaches that result in economic loss, but also breaches which may cause immaterial damages, such as any moral and reputational damages. Additional criteria, such as time spent in attempts to rectify the breach and distress should be considered when assessing the adverse effect.

BEUC supports a **risk-based definition** of the adverse effect of data breaches. In order to determine the level of risk, both quantitative and qualitative indicators need to be considered. For example, the type of data, the number of individuals affected and the amount of data breached would have to be considered.

³ Article 29 Data Protection Working Party, Opinion 4/2007 of 20 June 2007 on the concept of personal data.

⁴ Articles 10-11 of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In addition, when defining the likelihood for the adverse effect to happen, as required by Article 4.3, it is necessary to consider not only the circumstances of the specific case, but also the overall objective of the data protection legislation to protect the fundamental right to protection of personal data and privacy. To this end, BEUC considers the **mere probability of the adverse effect happening should suffice to require a notification**⁵.

BEUC is concerned with the provision of the revised framework, according to which the primary responsibility for defining the adverse effect of the data breach lies with the service providers. Due to the possible negative impact of a data breach for companies, both in terms of reputational damage and subsequent financial losses, it is questionable whether companies will notify all breaches that might have an adverse effect.

Therefore it is crucial to guarantee that the competent authority reserves the right to intervene and overrule any finding by the service provider of no likelihood of adverse effect. The possibility of intervention by an authority serves both to protect the individuals concerned by the breach and to allow for the development of a harmonised approach as to when notification is necessary.

Question 4: What are the most common cases where the subscriber and individual would not be the same person or entity?

In the electronic communications sector, the subscriber may not always be the same person as the user. The relevance of the distinction between user and subscriber relates to the fact that subscribers can be legal persons as well as natural persons. The e-privacy Directive applies to both legal and natural persons and therefore has a wider scope than the Data Protection Directive which only applies to natural persons.

This distinction is relevant for example when data is processed in order to provide value-added services which do not necessarily have to relate to the subscriber to the service, but they can also relate to a user. For example, within a family a father can have a subscription to a service that locates the mobile phone of his children. In this situation, the father is the subscriber, the children are the users. The distinction has also an impact on the issue of consent and whether consent needs to be given by the subscriber to the service or by the person to whom traffic data relate to⁶.

An additional issue relates to the implementation of Article 6(2) of the e-Privacy Directive which concerns an exception to process traffic data necessary for the purposes of subscriber billing and interconnection payments. Processing of this data is allowed, but only with regard to subscribers of a service, not its users.

⁵ Data Protection in a Profiled World, Sege Gutwirth, Yves Poulet, Paul de Hert.

⁶ According to recital 31 of the revised e-privacy Directive: *"whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it."*

Exception relating to technological protection measures

Question 5: What are examples of technological protection measures that can render data unintelligible?

Question 6: In your view, what should be the criteria and methods for assessing their sufficiency? At which stage of the notification process should this be examined?

According to the new rules, the exception relating to technological protection measures is not an automatic safe harbour. Such measures need to be approved by the competent authority and must be actually applied.

Furthermore, the requirement for technological protection measures to render the data unintelligible is an absolute one and therefore, measures which only make access more difficult or which can be compromised in other ways do not meet the standard⁷. However, it is questionable whether technological protection measures can actually render data unintelligible. Currently, it is almost impossible to ensure the full anonymisation of personal data and it is often possible with astonishing ease to 're-identify' or 'de-anonymise' individuals hidden in anonymised data⁸.

As a result, it would be difficult to establish a list of pre-approved measures, as their effectiveness will have to be assessed on an *ad hoc* basis. There is also the risk that a formerly approved measure is bypassed with the use of new technology. In that case, the competent authority should have the possibility to ask the service provider to notify.

National authority requiring notification of individual

Question 7: Has this happened in relation to your organisation? If yes, what were the circumstances, timeframe and exchanges with the provider or authority? If not, can circumstances be envisaged where this power would need to be invoked?

See comments on the power of competent authorities to require notification in question 3.

Interests of law enforcement authorities

Question 8: How should the legitimate interests of law enforcement authorities be taken into account, and how should this affect the two requirements to notify breaches?

⁷ Data Protection in a Profiled World, Sege Gutwirth, Yves Poullet, Paul de Hert.

⁸ The question of the effectiveness of anonymised data is subject to significant academic debate with several recent publications in the United States highlighting the ease with which anonymised data can be 'deanonymised'. De-anonymizing Social Networks, Narayanan and Shmatikov, Security and Privacy, 2009. Also, Broken promises of privacy: responding to the surprising failure of anonymisation, Paul Ohm.

A way to take into account the interests of law enforcement authorities would be to introduce specific rules regarding the timing of notification. A specific deadline could be established when there is the risk that timely notification might impede a criminal investigation. However, such an extension request should be made following a specific request in writing by law enforcement authorities with sufficient justification, and should not exceed the necessary time.

PROCEDURES FOR PERSONAL DATA BREACH NOTIFICATIONS

Notification deadline – 'undue delay'

Question 9: What should "undue delay" mean in the context of notifying national authorities? What would be the most effective and realistic approach, taking into account issues such as consumers' needs and administrative burden?

Question 10: What should "undue delay" mean in the context of notifying subscribers or individuals? What would be the most effective and realistic approach, taking into account issues such as consumers' needs and administrative burden?

BEUC supports the definition of clear deadlines for notification both to the competent authorities and to individuals. Notification to the **authorities** should take place as soon as the breach has been identified and at the latest within one week from the breach. It should also be complete. This deadline would allow data controllers to establish whether a breach has taken place and to take the measures necessary to prevent further breaches. In case complete information is unavailable within the specific deadline, the notification could be spread over time with the initial notification taking place as soon as the breach is identified and with follow up notifications being sent as breach details become available.

The notification to **individuals** should be given in such a time as to enable the individual to mitigate the adverse effects of the breach. In order to prevent notification fatigue, it should be for the competent authority to decide whether individuals need to be notified and instruct the service provider accordingly. In that case, notification to individuals should be made within a maximum of 72 hours after notification to the authorities.

Means of notification

Question 11: Which communications channels should be used for notifying national authorities? What would be the most efficient way of reducing administrative burden for all parties?

Question 12: Which communications channels should be used for notifying subscribers or individuals? What would be the most efficient way of reducing administrative burden for all parties?

When data has been breached, providers could use a variety of communication channels to notify the **competent authority**, including emails and phone calls. This would allow the authority to be alerted and to receive the initial information in order to assess whether notification to individuals should take place. Following the initial notification, a formal notification in a standardised format with the complete information should take place. If the breach has a cross-border element and concerns individuals in more than one Member State, the authority receiving the notification should inform the authorities in the countries concerned when assessing whether notification to individuals is necessary.

On the contrary, notification to **individuals** should reflect the contact information that a company holds. However, it should be taken into account that consumers might not easily identify the importance of the email or it may get lost in the spam filter. When the contact details of individuals are not known and upon approval by the competent authority, it may be acceptable to notify indirectly by publishing a notice in major newspapers.

Procedure for an individual case

Question 13: For an individual case of data breach, how long does it take to gather all necessary information, and what information should be gathered at first?

Question 14: What information should be provided to the authority/individual, and at which stages?

Question 15: What kind of feedback and follow-up should the provider and national authority expect from each other?

As noted above, should the complete information be unavailable within the specific deadline, the notification could be spread over time with follow up notifications being sent as breach details become available. As regards the specific information to be included in the notification, please see our response to the questions 16-17.

Once the breach has been notified, further notifications with updates on how the breach is solved should be addressed to the competent authority. Following the resolution of the breach, there should be an evaluation of the procedure with the participation of the provider and the competent authority with the aim of identifying areas for improvement.

FORMATS FOR PERSONAL DATA BREACH NOTIFICATIONS

Question 16: What should be included in the notification to national authorities? Where possible, please indicate a "minimum" and "maximum" list of elements.

Question 17: What should be included in the notification to subscribers or individuals? Where possible, please indicate a "minimum" and "maximum" list of elements.

Question 18: What kind of standard formats does your organisation use for breach notifications?

Question 19: Are there examples of best practice from other fields?

Question 20: Would it be feasible to have a standard EU format for notifications, and if so, what form should it take? Would this reduce or add to the costs of notification?

The revised e-privacy Directive requires the notification to individuals to describe at least the nature of the data breach, the contact points where more information can be obtained and the recommended measures to mitigate the adverse effects. BEUC considers these headlines to be the minimum information which should be provided to individuals. However, they need to include more specific information. **Individuals need to receive the information needed to understand the breach and what they can do in order to protect themselves.**

To this end, individuals should be informed about the personal information involved in the breach, the timing, the person/entity responsible for the breach and the number of people affected. With respect to the **contact points**, these should include the phone number, email and address of the competent authority, of the provider as well as of consumer organisations. Lastly, it is essential that individuals receive clear and understandable information about **recommended measures**, including practical advice to mitigate the adverse effects and to protect personal data in the future, as well as information about possible next steps, such as available means of redress.

The aim of the notification should be to inform the individuals when their personal data has been compromised and to enable them to take action in order to mitigate the effects of the breach. To this end, the information to be provided should be **clear and comprehensive**, i.e. without technical terms; it should be sufficient for individuals to read the notification to understand the risks. Furthermore, in order to avoid confusion, the notification should not be allowed to contain offers from the provider to sign up for additional services, such as identity theft insurance etc⁹.

The **notification to the competent authority** should include more detailed information about the incident and the measures taken by the provider to correct the breach. In addition, the number of affected individuals and the nature of the data involved would allow the authority to assess the adverse effects of the breach and recommend notification to individuals. Competent authorities should also be informed about the steps taken to solve the breach and any communication towards the relevant data subjects. Furthermore, the contact details of the team dealing with the breach should be provided, as well as the description of the measures implemented to prevent similar breaches in the future.

BEUC would support the development of standard EU format for notification which would help to remove the administrative burden from both companies and the competent authorities. Such a format should at least include the headlines to be addressed in the notification, e.g. description of the breach; the effects and the measures taken; in order to help authorities carry out an assessment of the breach. The Article 29 Data Protection Working Party could play a leading role in preparing such standard formats.

⁹ See further P.M. Schwartz and E.J. Janger, op. cit. 951 ff, regarding fuzzy notification letters, mentioning examples of breached entities including offers for credit monitoring and identity theft insurance in notification letters.

ADDITIONAL ISSUES

Inventory of personal data breaches

Question 21: Which elements should be included in the inventory of personal data breaches that providers are to maintain? Where possible, please indicate a "minimum" and "maximum" list of elements.

Question 22: should there be a common format and if so, what?

Question 23: Which parties should have access to the inventory? What would be the most efficient way to allow national authorities access to the inventory?

BEUC supports the development of an inventory of data breaches, to include information about the facts of the breach, the effects and the actions taken to remedy the breach. However, it is crucial that access to the inventory for data protection authorities is guaranteed after a simple request. In addition, in order to allow for comparative analysis, the interoperability between the different inventories must to be ensured. Failure to comply with the requirements regarding the development, update and access to the inventory should entail sanctions by the authorities.

Audits by national authorities

Question 24: What is your organisation's experience so far with audits? In which circumstances and when should audits take place?

Question 25: Should there be a common EU format for audits and if so, what?

N/A

Cross-border breaches

Question 26: Has your organisation dealt with a cross-border data breach before? If so, how was it resolved? In general, what are the frequency and circumstances of these cases, and what would be the most effective way of dealing with them?

Although the frequency of reporting cross-border data breaches remains relatively low¹⁰, the cross-border aspect of data breaches is likely to increase, given the ease with which information can be instantly transferred at anytime, to any place¹¹. Cross-border cases may occur when the data controller is not established in the Member State where the breach happens, or the same breach happens simultaneously in various locations. To this end, a clarification of the rules on applicable law is necessary, while data protection authorities should strengthen their cooperation. It is

¹⁰ OECD report on cross-border enforcement of privacy laws:
<http://www.oecd.org/dataoecd/17/43/37558845.pdf>

¹¹ For example, in July 2006, a computer hacker located in Germany gained access to the computer system of a local government agency in the United States that contained the personal information of 4, 800 public housing residents:
<http://www.montereyherald.com/mld/montereyherald/news/15133805.htm>

equally important to ensure that individuals whose data has been breached receive notification in their own language.

Notification of risk of security breach

Question 27: Is there a need for harmonisation of national measures relating to this provision?

As with the notification of data breach, efforts to standardise the notification of risk of security breach should be undertaken, at least with respect to the headlines of information to be provided to subscribers.

Relationship with security breach notifications under Article 13a of the Framework Directive

Question 28: How will your organisation handle incidents that might be subject to the notification requirements under both Article 4 of the ePrivacy Directive and under Article 13a of the Framework Directive? Are there any internal procedures for informing national competent authorities other than the one responsible for notifications of personal data breaches under Article 4 of the ePrivacy Directive?

N/A

END