EUROPEAN COMMISSION
Information Society and Media Directorate-General

Electronic Communications Policy

ePrivacy Directive: circumstances, procedures and formats for personal data breach notifications

Public consultation

Publication date: 14 July 2011
Closing date for responses: 9 September 2011

This document does not represent an official position of the European Commission, but is intended to stimulate debate on the part of stakeholders and the public. It does not prejudge the form or content of any future proposal by the European Commission.

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111

1. INTRODUCTION

ePrivacy Directive

The ePrivacy Directive (2002/58/EC)[1] regulates the processing of personal data and the protection of privacy in the EU electronic communications sector. Its provisions are crucial to ensuring that users can trust the services and technologies they use for communicating electronically. The Directive forms part of the regulatory framework for publicly available electronic communications networks and services, which comprises four other Directives on the general framework, access and interconnection, authorisation and licensing and universal service.

The regulatory framework was amended in December 2009 with the adoption of the "Telecoms Reform". The reform package includes Directive 2009/136/EC[2] ('the amending Directive') providing amendments to the ePrivacy Directive designed to clarify and strengthen the rules on the protection of privacy in the electronic communications sector.

New obligation to notify personal data breaches

One new element introduced by the reform is an obligation for electronic communications providers to notify **personal data breaches**. Personal data breaches are security incidents by which personal data is compromised, e.g. by unauthorised access, alteration or destruction. Providers of electronic communications services have to report the breaches to the relevant national authority, and also to individuals when there is a risk to their personal data or privacy. These provisions are laid down in new paragraphs of Article 4 of the Directive:

– Paragraph 3 sets the rules for the notification;

– Paragraph 4 enables national authorities to issue guidelines and instructions on the notifications;

– Paragraph 5 allows the Commission to adopt **technical implementing measures** on the **circumstances, formats and procedures** for the notification requirements under Article 4 to ensure consistent implementation of the provisions across Member States.

These technical implementing measures allow for the adoption of practical rules on top of the existing legislation, and are the focus of the present consultation.

It should be noted that the new provisions do not affect the existing obligation under paragraph 2 for operators to notify risk of security breaches.

Adoption procedure

Such technical implementing measures would take the form of a Commission Decision adopted in the regulatory comitology procedure, with the following steps:

---

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF

– **Stakeholder involvement**: the Commission is required to involve stakeholders, to provide input about the best available technical and economic means of implementation.

– **Consultation of relevant bodies**: as part of the adoption procedure, the Commission would subsequently consult the European Network and Information Security Agency (ENISA), Article 29 Data Protection Working Party and the European Data Protection Supervisor (EDPS). National regulatory authorities (NRAs) would also be consulted, through the Body of European Regulators for Electronic Communications (BEREC), since they are the competent authorities for breaches in some Member States.

– **Member State approval**: under the regulatory comitology procedure, Member States would then have to agree to the Commission proposal, within the Communications Committee.

– **Parliamentary scrutiny**: the European Parliament would then have three months to scrutinise whether the draft measure is consistent with the Commission's mandate.

Purpose of this consultation

With the transposition deadline for the revised ePrivacy Directive having recently passed (on 25 May 2011), the Commission has now started its preparatory work on these implementing measures, having taken full account of the ENISA study[3] and the Article 29 Working Group opinion[4] on data breach notifications.

As a first step, the Commission wants to engage all relevant stakeholders – such as telecoms operators, Internet Service Providers, Member States, data protection authorities, national regulatory authorities and consumer organisations, as well as ENISA and EDPS – in a public consultation process in order to gather practical input based on existing practice and initial experience with the new rules. This will help the Commission to determine whether technical implementing measures are required to ensure harmonised national measures on personal data breach notifications, and if so, what form they should take.

Respondents are encouraged to provide practical examples of how they handle data breaches and notifications in the Member State(s) where they are active. The Commission also invites organisations not directly involved in the notification process, such as consumer groups, to express their views on the issues involved, even if it may not be possible to provide answers to all questions.

It should be noted that the data breach provisions of the ePrivacy Directive and its technical implementing measures concern only providers of publicly available electronic communications services. As part of its review of the general Data Protection Directive (95/46/EC), the Commission is considering the extension of breach notification obligations to cover not only electronic communications providers, but all data controllers. This issue is, however, separate from the implementation of the ePrivacy Directive and as such is not covered by the present consultation.

[3] http://www.enisa.europa.eu/act/it/library/deliverables/dbn

[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf

The European Commission invites written comments on the questions raised in this document. Responses should reach the Commission by **9 September 2011** at INFSO-DATABREACH@ec.europa.eu. See the annex for further information on submitting your response.

2. CIRCUMSTANCES OF PERSONAL DATA BREACH NOTIFICATIONS

2.1. Notifying the national authority

Under the revised ePrivacy Directive, providers have to report personal data breaches to the competent national authority:

"In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority." *Article 4(3)*

A personal data breach is defined as:

"…a breach 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 Community." *Article 2(i)*

In the Commission's view, the obligation and definition as set out in the Directive should be sufficiently clear to allow for harmonised national rules, given that all breaches should be notified and that it should be straightforward to assess whether personal data is involved. Nevertheless, the Commission wishes to learn about how data breach notification is being implemented in practice at national level, in order to determine whether further harmonising measures beyond the new EU rules may in fact be required.

To this end, please also provide information on guidelines and instructions in relation to the ePrivacy Directive that have already been issued, and/or on data breach legislation unrelated to the ePrivacy Directive that is already in force in your Member State.

Question 1: Does your organisation[5] 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?

2.2. Notifying the subscriber or individual

Under the revised ePrivacy Directive, providers also have to report breaches to subscribers or individuals when there is a risk to their personal data or privacy:

"When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay." *Article 4(3)*

[5] 'Organisation' refers to electronic communication service providers or to competent national authorities.

Under Recital 61 of the amending Directive, guidance is provided on the meaning of "adversely affect":

"[…]A breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community.[…]"

In comparison with the general obligation to notify all personal data breaches to the national authority, this obligation to notify individuals leaves more room for interpretation, specifically in relation to what should be considered as adversely affecting personal data or privacy. Here, the Commission sees a potential risk of divergent rules and therefore wishes to have more information on the thresholds that are applied at national level, as well as on specific examples of data breaches that have triggered or would be likely to trigger this additional requirement.

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?

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

2.3. Exception relating to technological protection measures

The service provider does not have to notify the individual if sufficient technological protection measures have been applied to the data to make them effectively unintelligible:

"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 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." Article 4(3)

Again, the Commission sees a potential risk of divergent rules and therefore wishes to have more information on how this provision is being applied at national level.

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?

2.4. National authority requiring notification of individual

The national authority also has the power under the Directive to require the provider to notify the individual:

"Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the

personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so." Article 4(3)

Here, the triggers for requiring notification of the individual would clearly be linked to those applying to the measure in section 2.2 above. Nevertheless, the Commission is interested to learn more about whether and when this requirement would actually be applied in practice.

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?

2.5. Interests of law enforcement authorities

Recital 64 of the amending Directive sets out the following guideline in relation to law enforcement authorities:

"[…] such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach."

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?

3. PROCEDURES FOR PERSONAL DATA BREACH NOTIFICATIONS

3.1. Notification deadline – 'undue delay'

For both types of breach notification – to the authority and to the subscriber or individual – the provider is required to notify "*without undue delay*".

This is an area where there is a clear risk of divergent national implementation. The Commission would want to ensure that the notification deadlines are common across the EU, and therefore wishes to have more information on the deadlines applied at national level, for both types of breach notification.

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?

3.2. Means of notification

The ePrivacy Directive does not mention specifically the means (e.g. email or letter) by which national authorities or individuals should be notified. However, the Commission expects that national authorities may address this issue in their guidelines or instructions, and would want to ensure that the means of notification is also common across the EU.

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?

3.3. Procedure for an individual case

The Commission also wishes to have more information on the lifecycle of a data breach, e.g. detection, assessment, notification and follow-up. This will help the Commission to determine whether further measures are needed on the deadlines and procedures required for the various stages of a breach beyond the initial notification.

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?

4. FORMATS FOR PERSONAL DATA BREACH NOTIFICATIONS

The ePrivacy Directive sets out the minimum requirements for the format and content of both types of breach notification:

"The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach." Article 4(3)

In the Commission's view, these requirements are clear and the elements described should be included in all notifications as appropriate. However, as implied by the phrase "at least", the Commission would expect and welcome the inclusion of additional information. In this context, the Commission wishes to have more information on other elements that should be included in the notifications, and on existing standard formats or best practices, from this and other fields.

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?

5. ADDITIONAL ISSUES

5.1. Inventory of personal data breaches

Under the Directive, providers are to maintain an inventory of personal data breaches:

"Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph. The inventory shall only include the information necessary for this purpose." *Article 4(3)*

Further explanation of this provision is provided in Recital 58 of the amending Directive:

"The competent national authorities should promote the interests of citizens by, inter alia, contributing to ensuring a high level of protection of personal data and privacy. To this end, competent national authorities should have the necessary means to perform their duties, including comprehensive and reliable data about security incidents that have led to the personal data of individuals being compromised. They should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services. Providers should therefore maintain an inventory of personal data breaches to enable further analysis and evaluation by the competent national authorities."

The Commission attaches high importance to this provision and wishes to facilitate a feedback cycle that allows for continual improvement of breach notification procedures by all parties. In this context, the Commission wishes to have more information on the format of existing and planned inventories, and the ways of allowing national authorities to access them.

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?

5.2. Audits by national authorities

Under the Directive, national authorities may also audit whether providers have complied with their obligations:

"[National authorities] shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so." *Article 4(3)*

The Commission wishes to have more information on how this provision will be applied in practice, to help to determine whether further harmonising measures may be needed.

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?

5.3. Cross-border breaches

Harmonisation of national measures on the circumstances, procedures and formats for personal data breach notifications would have particular relevance for breaches with a cross-border element, for example where the data controller is established in one Member State but the breach happens in another, or the individuals affected are based elsewhere. The Commission is particularly interested in learning more about these cases, to ensure that any future implementing measures take full account of the needs all parties involved.

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?

5.4. Notification of risk of security breach

The technical implementing measures may also cover the following provision on notification of risk of security breach, which is not a new obligation and was present in the previous version of the Directive:

"In the case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved." *Article 4(2)*

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

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

The "Telecoms Reform" also modified the Framework Directive (2002/21/EC), which sets out the common regulatory framework for electronic communications networks and services. Its new chapter IIIa "security and integrity of networks and services" provides for the security breach notification scheme (Art.13a(3)) and enables the Commission to adopt technical implementing measures to harmonise the national measures (Art. 13a(4)):

"3. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and

Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest.

Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph.

4. The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to harmonising the measures referred to in paragraphs 1, 2, and 3, including measures defining the circumstances, format and procedures applicable to notification requirements…"

In some cases the same data breach could possibly require a notification under Article 4 of the ePrivacy Directive as well as under Article 13a of the Framework Directive. The Commission would like to know the internal procedures in place that will allow such cases to be addressed, in particular the channels of communication between the authorities responsible for the two types of breach.

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?

6. ADDITIONAL INFORMATION

Respondents are invited to raise any other issues relating to personal data breach notifications under the ePrivacy Directive that they might want to address in this consultation.

ANNEX

Responding to the consultation

The Commission invites written views and comments on the issues raised in this document, to be submitted **by 9 September 2011**. Please include the following information in your reply:

– whether you are responding in a private capacity or on behalf of an organisation or interest group (if the latter, please indicate its approximate size);

– the name and email address of a contact person in your organisation for any questions on your contribution; and

– if applicable, your registration number in the Commission's Register of Interest Representatives.

Contributions, together with the identity of the contributor, may be published on the website of the Directorate-General for Information Society and Media, unless the contributor objects to publication of personal or confidential data on the grounds that such publication would harm his or her legitimate interest. For more details, please see the Commission's general statement on personal data protection[6] as well as the specific privacy statement for this consultation[7].

Please note that we do not need a hard copy in addition to the electronic version.

Contact address:

Policy Development Unit (B1), BU33 7/40
DG Information Society and Media
European Commission
B-1049 Brussels
Belgium
Tel +32 2 297 1622

Email: INFSO-DATABREACH@ec.europa.eu

6 http://ec.europa.eu/geninfo/legal_notices_en.htm#personaldata

7 http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/index_en.htm