ARTICLE 29 DATA PROTECTION WORKING PARTY

01079/12/EN

WP197

Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications

Adopted on 12 July 2012

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH

REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION

1 Introduction and scope of the draft Decision

Under Article 4(5) of Directive 2002/58/EC as amended by Directive 2009/136/EC (hereinafter the "*ePrivacy Directive*"), the European Commission (hereinafter the "*Commission"*) has the power to adopt implementing measures concerning paragraphs 2, 3 and 4 of Article 4 of the Directive, after having consulted with the relevant stakeholders including the Article 29 Working Party (hereinafter the "*Working Party*").

As highlighted in particular in recital 5, the draft Commission Decision (hereinafter the "Decision") covers only paragraphs 3 and 4, which relate to personal data breaches. This suggests that the *particular risk of a breach of the security of the network* will be developed in a distinct Commission Decision. The Decision also needs to be examined in light of the draft regulation on data protection[1], which proposes to extend data breach notification to all data controllers.

In this regard, the Working Party welcomes this Decision as it will contribute to the harmonization of the practical rules applied for data breach notifications.

In the following opinion, the Working Party would nevertheless like to draw the Commission's attention to some points of the Decision that require some clarifications or enhancements.

2 Analysis

2.1 Terminology and legal certainty

The Working Party welcomes the Commission's detailed effort to clarify the personal data breach provisions of the Directive.

However, the Working Party is concerned about the frequent use of imprecise language such as "reasonable" or "exceptional circumstances" that may lead to varying interpretations and legal uncertainty that will negatively affect all stakeholders.

a) The words "reasonable" and "reasonably"

Article 2(2) states that "*In the event of a personal data breach, the provider shall notify the personal data breach to the competent national authority no later than 24 hours after the provider has acquired a* **reasonable degree of certainty** *that the personal data breach has occurred*". In order to avoid

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

uncertainty in determining the moment from which the 24 hours delay will start, the Working party suggests simplifying this sentence as follows "*In the event of a personal data breach, 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*".

In addition, the Working Party outlines that the Decision does not clearly address the cases where a provider detects a security incident that may lead or may have led to a personal data breach, without being able to ascertain that the incident actually resulted in a personal data breach. The Decision could highlight that the provider needs to be aware that a detected security incident, which the provider might handle according to industry best practices on security incident management might indeed result in a personal data breach, and should thus be prepared to assess and handle it. .

In Article 2(3), where the word reasonable is also used twice:

- similarly, the words "*the provider shall be permitted to make an initial notification to the competent national authority no later than 24 hours after the provider has acquired a* **reasonable degree of certainty** *that the personal data breach has occurred*" could be replaced by *"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",*

- the words "*despite having made* **reasonable efforts** *to investigate"* could be replaced by *"despite its investigations"* without loss of clarity. In any case, the competent authority will ultimately analyze the arguments provided by the provider to justify any delay in notification.

Article 3(8) also uses the word "reasonable" twice : "*Where the provider, despite having made* **reasonable efforts**, *is unable to identify all individuals adversely affected by the personal data breach within the time period referred to in paragraph 3, the provider may notify the individuals it was unable to identify through advertisements in major national media within that time period. These advertisements shall contain the information set out in Annex 2, where necessary in a condensed form. In that case, the provider shall in addition continue to make* **all reasonable efforts** *to identify those individuals and to notify to them the information set out in Annex 2 as soon as possible.*" The Working Party suggests to simplify this paragraph by removing references to "reasonable efforts" as follows: "*Where the provider is unable to identify all individuals adversely affected by the personal data breach within the time period referred to in paragraph 3, the provider may notify the individuals it was unable to identify through advertisements in major national media within that time period. These advertisements shall contain the information set out in Annex 2, where necessary in a condensed form. In that case, the provider shall in addition continue efforts to identify those individuals and to notify to them the information set out in Annex 2 as soon as possible."*

The use of the word "*reasonable*" should also be avoided in recital 6 and Article 3(3).

Finally, Article 3(7) also mentions that *"the provider shall notify to the subscriber or individual the personal data breach by using* **reasonably** *secure means of communication that ensures prompt receipt of information"*. The Working Party suggests replacing the last part by "*by means of*

communication that ensure prompt receipt of information and that are appropriately secured[2] *according to the state of the art".*

b) The expression "exceptional circumstances"

The expression "*exceptional circumstances*" creates the same uncertainty. The Working Party observes that "exceptional circumstances" may already be defined in national legislation or jurisprudence, referring for example to "*unpredictable events of particular seriousness*", including wars or major public safety events. These interpretations seem inconsistent with the harmonisation and clarification purposes of the Decision.

Therefore, the Working Party recommends clarifying the Decision as follows:

1) In the last paragraph of Article 2(3) the words "**In exceptional circumstances**, *where the provider, despite having* **made reasonable efforts to investigate** *[…]*" could simply be replaced by *"Where the provider, despite its investigations […]*".

For the sake of consistency, a similar wording should be used in recital 6.

In addition, the Working Party recommends that the Decision includes an explicit reference to Article 15a of the ePrivacy Directive to highlight that the absence or the incomplete notification of a personal data breach is likely to constitute an infringement of data breach legislation.

2) Article 3(6) of the Decision states that "*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 for a reasonable period*." The Working Party welcomes the fact that the notification to the competent authority is not delayed in principle and fully understands that in some circumstances, there may be a need to delay the notification to the individuals in order to avoid prejudicing a police investigation for example. However, the use of the words "exceptional circumstances" introduces legal uncertainty about the scope of this exemption, and could give providers broad latitude to delay notification to individuals. The Working Party asks the Commission to explicitly specify the scope of "exceptional circumstances" referred in the text[3]. In this regard, priority should always be given to the protection of individuals when considering the balance between the legitimate interest of a police investigation and the duty to inform individuals in cases where such information can clearly help mitigate the potential adverse effects of the breach.

c) Additional remarks

The first sentence of Recital 6 starts as "*Providers* **should** *notify to the competent authority* […]". The Working Party suggests using the verb "shall" instead of "should" here for the sake of consistency with Article 2.1 of the Decision as well as the Directive.

---

[2] "secured" means "ensuring confidentiality, integrity and availability".

[3] For example, the Commission could use the wording of Article 1 of the Directive 2006/24/EC which refers specifically to "*the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law*", if it wishes to refer explicitly to serious cases in police investigations. The Commission may adopt a different wording if "exceptional circumstances" are meant to refer more specifically to cybercrime.

In addition, the Working Party suggests deleting Article 3(5) of the Decision, since it does not provide additional information, recommendations or requirements with respect to the text already set out in the Directive and in Article 3(1) of the Decision.

2.2 Notification to the competent national authority

According to Article 4(3) of the ePrivacy Directive, "*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*".

The Decision develops the notion of "*undue delay*" by establishing two delays: a first delay of 24 hours after the detection of the breach to provide an "initial notification" with basic information and a second delay of 3 days after this initial notification to provide a fully completed notification. Annex 1 of the Decision details the minimum content of the initial notification (section 1) and of the completed notification (section 2).

Subject to the observations on the use of the word "reasonable" previously highlighted, the Working Party welcomes the fact that specific delays are included in the Decision and supports the two-step notification scheme that allows combining responsiveness and comprehensiveness.

The Working Party proposes several amendments in order to facilitate the communication between the provider and the authority and ensure better harmonization[4].

a) Information to be provided and initial notification

The bare minimum information that a provider must notify to the competent authority within 24 hours after the detection of the breach is limited to the identity of the provider and the name of a contact point (section 1 of Annex 1). As it stands, without additional information, this initial notification is of little value to the competent authority. The Working Party considers that, in order to stimulate providers in implementing a high quality personal data security policy, the provider should be asked to provide some more information to the competent national authority than is proposed by the Commission. The Working Party believes that a provider should notify the competent authority about all the details it is aware of during the first notification phase. At the very least, during the initial notification, a limited number of other items should be mandatory. The Working Party considers that once the provider has detected a breach, it is at least aware of the type of personal data that is concerned, the circumstances of the breach or type of exposure (loss, theft, copying, etc.) and how the breach was detected (detection software in place, analysis of the logs, an employee reported an incident, etc.). This information should be included in the initial notification and supplemented and/or corrected in the 2nd notification.

The Working Party suggests including the following information in the section 1 of Annex 1 of the Decision:

---

[4] When drafting future legislation on personal data breaches, the Commission could also examine if all personal data breaches should be notified to the competent authorities or whether exemptions could apply in certain cases, provided that all breaches are reported in the inventory maintained by the controller. This issue was already addressed by the Working party in its Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications.

- Circumstances of the personal data breach / type of exposure (e.g. loss, theft, copying)
- How the breach was detected
- Date and time of the detection of the incident, as well as date and time at which the incident took place
- Nature and content of personal data concerned
- Implemented controls (especially regarding personal data unintelligibility)

The Decision should also clearly indicate that the provider can amend the elements of the initial notification in the complete second notification.

Finally, in order to enable references to the notification items listed in Annex 1, the Working Party proposes to replace the bullets by numbers. This is also useful in the development of a harmonized approach for an electronic means of notification.

b) Electronic means

The use of electronic means seems appropriate for the transmission of notifications and the Working Party supports the European Commission's initiative to promote such means when possible. However, the implementation of these electronic means across Member States is not immediate: it will be necessary to define a common electronic notification format, adopt adequate security measures, develop and test the electronic means (portal and/or another system such as secure email) that will support this mechanism in each Member State.

Therefore, the Decision should foresee the development of a simple common European electronic notification format (e.g. in XML) in cooperation with relevant stakeholders. Once this common format is defined, the European Commission should allow for a delay of at least 12 months for the implementation of the notification by electronic means. During the transition period, alternative notification means should be allowed.

The Working Party would welcome if the Commission could indicate if and how it could provide financial and logistical support to a possible project of the Working Party and individual DPAs aiming at the definition of a common format and the implementation of a technical solution for the notification of data breaches to DPAs by controllers and the exchange of any information relating to the data breach between authorities in cross-border cases. This project should also take into account the solutions that are already implemented or that are under development in some Member States.

c) The notification to other national authorities concerned

In Article 2(5), the Decision requires the notification to other national authorities concerned "*where the personal data breach involves subscribers or individuals from Member States other than that of the competent national authority to which the personal data breach has been notified*".

The Working Party welcomes and supports active cooperation between Authorities and clearly understands the need for cooperation between competent national authorities. Members of the Working Party are all clearly committed to collaborate with each other on this matter.

However, this obligation does not exist in the Directive and the Working Party wonders about the legal basis of such an obligation and the actual implications in the case of the absence of notification to other national authorities. Moreover, the Working Party notes that the notification form set out in Annex 1 does not allow the national competent authority to determine the location or nationality of the persons affected by the breach and that the Decision does not provide a clear definition of "subscribers or individuals from other Member States".

Therefore, the Working Party advises the Commission to specify the scope of the provision laid down in Article 2(5) and to clarify the practical means the competent authorities should use in order to cooperate.

2.3 Notification to the subscriber or individual

The Working Party welcomes that the Decision describes a procedure in those cases where the persons cannot be reached directly.

The Working Party also welcomes the description of the circumstances to be taken into account when assessing whether a breach adversely affects the personal data or privacy of a subscriber of individual, as described in Article 3(2) of the Decision.

Article 3(7) highlights that including "information about a personal data breach in a regular invoice" is not an adequate means of information to individuals. However, it is not clear if this is just an example or if the Decision simply intends to disallow the use of invoices to inform individuals about a personal data breach. More generally, the Working Party believes that information about a personal data breach should be made to stand out from other information exchanged between providers and individuals. The Working Party suggests therefore that the Decision indicates that the information about the breach shall be dedicated to the breach and not associated with information about another topic.

Regarding the use of the media to reach the individuals the provider has been unable to identify, the Working Party outlines that cases may happen where major national media are not the most appropriate media to use, e.g. when a locally implanted provider wants to reach individuals within a limited geographic area. To reflect this particular point, the words "or regional" could be added after "through advertisements in major national" in paragraph 8 of Article 3.

Finally, as explained in the following section, more detailed guidance should be provided to assist the Authorities and providers to assess the severity of breaches in an objective and harmonized way.

2.4 Assessing severity and adverse effects

With the implementation of Directive 2009/136/EC, competent authorities are receiving an increasing number of personal data breach notifications, which differ widely in scope and severity. It is important for authorities to identify the most critical breaches in order to prioritize their action, which notably includes the possibility to force providers to notify individuals in some circumstances. Furthermore, providers also need to clearly and objectively estimate the adverse effect of a breach to determine if a notification to individuals is warranted.

In the context of the above, the Working Group has identified the necessity of a uniform and easily understandable severity assessment methodology for both providers and competent authorities in Europe. Indeed, Article 3(2) does not propose either a scale or objective criteria to assess the grading of the severity of a breach. In addition it does not clarify any thresholds, which could be considered in order to determine the need of the provider to notify to the persons.

The Decision would strongly benefit from more detailed guidelines in this respect. Indeed, both the competent authorities and the providers need to have a common understanding and assessment of the severity of a personal breach. This understanding is not only relevant on a national level, but also on a European level in order to avoid fragmentation in the implementation of the Directive and of the Decision.

To address this requirement, the Working Party strongly supports the establishment of a pan-European harmonized severity assessment methodology based on objective criteria. The Working Party is currently working on developing such a methodology[5] in cooperation with ENISA. The proposed methodology will provide a severity scale that takes into account the adverse effects on the individuals, the efforts needed to identify the individuals from the data and the level of exposure of the data that is concerned by the breach. Notably, however, the number of individuals concerned by the breach should not be used as a criterion to determine if a notification to the persons is required. The Working Party advises the Commission to ensure that a harmonized approach for severity assessment will be used by all stakeholders. Therefore, the development of a severity assessment framework should be explicitly addressed in a dedicated Article of the Decision.

In addition, the Working Party proposes that the Decision includes among the fields required in Section 2 of Annex I both the relevant criteria used in the severity assessment, as well as the result of the assessment grading the severity (for instance "high", "medium", "low" or "negligible") and the rationale of such assessment.

2.5 Technological protection measures and unintelligibility of data

Article 4 of the Decision specifies in more detail what measures shall be considered adequate to render data unintelligible. These implementing measures, which are mainly based on the recommendations of ENISA, highlight that in order to consider data unintelligible, it must either be the product of an encryption mechanism, a keyed hash function or irreversible deletion. The measures also rightly suggest that the related cryptographic keys must not be easy to guess and have not been compromised in any security breach. The Working Party welcomes such measures and believes that they will drive stakeholders towards stronger security practices while providing stronger legal certainty on the notion of unintelligible data across member states.

If a personal data breach concerns solely data that has been rendered unintelligible, this should rightfully allow the provider to be exempted from notifying individuals in case of a personal data breach. However, the Working Party would like to highlight that this Decision should not give operators the impression that implementing encryption, hashing or secure deletion is sufficient by itself to allow providers to claim more broadly they have fulfilled the general security obligation set forth in Article 17 of Directive 95/46/EC. In this regard, providers also need to implement adequate

[5] Based on ENISA's "Recommendations on technical implementation guidelines of Article 4".

organizational and technical measures to prevent, detect and block personal data breaches. To this effect, providers need to have a risk management framework[6] in place to determine the appropriate measures to be implemented. It is also important that they consider any residual risk that may be present after controls have been implemented in order to understand where there may still be potential for personal data breaches to occur. The Working Party advises the Commission to clarify this point in a recital of the Decision.

Regarding the definition of "*unintelligible data"*, the Working Party would like to suggest some minor changes to the text in order to avoid any ambiguity by splitting paragraph 2(a) in two parts to better distinguish encryption and hashing, as follows:

> *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 authorized 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 authorized to access the key; or*
>
> *(c) it has been irreversibly deleted, either through physical destruction of the medium on which it was recorded or by means of a secure deletion algorithm.*

The suggested distinction between encryption and hashing allows highlighting the following important points that may not be fully clear in the current text of the Decision:

1) The security of encryption more accurately relies on the security of the "decryption" key rather than the "encryption" key. While this distinction is not relevant for symmetric algorithms (such as AES), it is relevant for asymmetric encryption (such as RSA).
2) The security of a keyed hash function relies on the key used to compute the hash function and there is no notion of a "decryption" or "encryption" key.
3) In the case of hashing, it is useful to clarify that the original data has been "replaced" by the hashed value (as in password databases for example) and the hashed value is not combined with other directly or indirectly identifying data.
4) It is important to clarify that the confidentiality of the relevant keys is relative to the persons who are "*not authorized to access the key".* As such, guessing the key by exhaustive key search should not be possible for "*any person who is not authorized to access the key"* as added in the text.

[6] The framework needs to be focused on the protection of personal data, and should identify potential impact for the individuals, as opposed to focusing on the risks concerning the business only, and on the protection of organisations against legal risks.

Additionally, regarding deletion, it is suggested to replace "s*ecurely deleted*" by "*irreversibly deleted"* in order to further clarify the intended results of this measure.

2.6 Other points

The Working Party notes that the draft Decision does not include any provision or recital regarding the inventory mentioned in Article 4(4) of the Directive. Considering the tight links between the notifications and the inventory, the Working Party suggests to add a Recital in the Decision to mention that providers may also refer to the Decision to determine the format of the inventory entries.

Similarly, the draft Commission Decision indicates in Recital 11 that authorities maintain statistics about breaches. The Working Party suggests that the Decision includes a harmonized set of items – that could be extracted from the unified form - to be monitored statistically.

Done at Brussels, on 12/07/2012

For the Working Party
The Chairman
Jacob KOHNSTAMM