**00683/11/EN**
**WP 184**

# Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments

**Adopted on 5 April 2011**

**The Working Party on the Protection of Individuals with regard to the processing of personal data**

established by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (OJ L 281, 23.11.1995, p. 31),

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 following working document:

## I. INTRODUCTION

1. This Article 29 Working Party document takes stock of the status and the way in which Member States are transposing the personal data breach provisions of the ePrivacy Directive in their national laws[1].

2. The aim of this exercise is threefold: ***First***, the Article 29 Working Party wishes to obtain a broad understanding of the current situation on this topic. This includes both basic aspects, such as the status of transposition, and more complex ones, for example, identifying any initial differences of approach in different areas (e.g., the scope of the obligation, whether national guidance developing some aspects of the ePrivacy Directive is foreseen, the national competent authority, etc). Pinpointing any developing differing national approaches might, even at this late stage, enable Member States to align their views and avoid fragmented implementation.

3. ***Second,*** this activity is helping national data protection authorities to take note of the findings and it has brought to their attention the need to engage in some follow-up activities, described in this working paper. It emerges from this activity that competent authorities ought to continue working towards defining internal rules and procedures for data controllers to notify individuals and competent authorities. Furthermore, taking into account that data controllers will be increasingly notifying cross-border personal data breaches, the need for authorities to liase to discuss a cooperation method becomes obvious.

4. ***In addition***, this exercise has given the Article 29 Working Party an opportunity to further reflect on the matter and reach some conclusions as to future policy developments in the area of personal data breach notification. These conclusions which complement the views of Article 29 Working Party on the topic given at other occasions[2] builds on the experience on security breach notification that has been gained by those national data protection authorities already implementing personal data breach notification requirements. The Article 29 Working Party wishes that these findings are taken into account in the context of further policy developments regarding personal data breach. More particularly, such policy developments are expected in the following two contexts:

   **a)** To complement the personal data breach framework of the ePrivacy Directive. Article 4(5) of the ePrivacy Directive delegates powers to the Commission to adopt technical implementing measures (referred to as "delegated powers" *ex* Art 290 of TFEU, after the adoption of the Lisbon Treaty) in order to ensure consistent implementation and application of the

---

1 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L337/11, 18.12.2009.

2 See WP 29 Paper entitled "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", adopted on 01.12.2009 (WP 168); Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), adopted on 10.02.2009 (WP 159); Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), adopted on 15.05.2008 (WP 150).

personal data breach legal framework in some well-defined areas, (i.e., circumstances, format and procedures applicable to the information and notification requirements).

**b)** To extend the personal data breach framework of the ePrivacy Directive in the context of the review of Directive 95/46. The Commission committed before the European Parliament to initiate without delay the appropriate preparatory work, including consultation with stakeholders, with a view to presenting proposals in this area, as appropriate, by the end of 2011..."[3]. This commitment was confirmed in the Commission's Communication "*A comprehensive approach on personal data protection in the European Union*"[4].

5. The above items are developed as follows: After a summary of the main elements of the personal data breach provisions in the ePrivacy Directive (Section II), this working document summarizes the personal data breach legislation in Member States (Section III). The summary is based on information provided by the national data protection authorities ("DPAs") but not reproduced here given the evolving character of the transposition. Section IV puts forward various actions to be carried out by competent authorities and by the Article 29 Working Party towards developing internal processes and setting forth cooperation procedures. Section V and VI focus on the new policy developments by recalling the overall scope and procedures for the expected policy actions regarding personal data breach and providing policy recommendations.

6. The views expressed here are without prejudice to possible more specific guidance in the future, including in the context of the adoption by the Commission of technical implementing measures *ex* Article 4(5) of the ePrivacy Directive.

## II. PERSONAL DATA BREACH UNDER THE ePRIVACY DIRECTIVE

7. The revised ePrivacy Directive lays down, for the first time in the EU, a mandatory personal data breach notification framework. This framework only applies to providers of publicly available electronic communications services (e.g., providers of communications and Internet access).[5] The framework

---

3 See Commission declaration on data breach notification made before the European Parliament in 2009 in the context of the reform of the Regulatory Framework for Electronic Communications. Retrievable at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-ta-2009-

4 COM (2010) 609 final, adopted on 04.11.2010.

5 As defined in Article 2 of the Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by Directive 2009/140/EC and Regulation 544/2009 ("Framework Directive") covering providers of services normally provided for remuneration that consists wholly or mainly in the conveyance of signals on an electronic network. The definition excludes provision of content and also of information society services, which do not consist wholly or mainly in the conveyance of signals on electronic communications.

provides for certain core elements that must necessarily be transposed in Member States' legislation.

## II.1 Common core elements

8. The core elements set out in the ePrivacy Directive are:

   a. The ***definition of data breach*** *ex* Art. 2 (i) which establishes that a personal data breach "*means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized 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*". Thus, for the personal data breach to occur, it must include "personal data", as defined under Art. 2(a) of the Data Protection Directive[6]. A personal data breach encompasses cases of unauthorized disclosure or unauthorized access to personal data but also cases of simple accidental destruction or alteration which is not followed (or very unlikely to be followed) by unauthorized access.
   b. The applicable legal ***thresholds*** to notify individuals and authorities (Art. 4(3), subparagraphs 1-2). The thresholds define when an entity suffering a breach is obliged to notify the breach to authorities and affected individuals. The ePrivacy Directive requires notification to individuals "*When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual...*". All data breaches shall be reported to the authorities.
   c. The ***content and time of the notification***. The time of notification to individuals, according to Art. 4(3) subparagraphs 1-2: is "*...without undue delay...".* As for content of the notification, it should include the nature of the personal data breach, contact information and recommend measures to mitigate possible adverse effects. The notification to the competent national authority must also describe steps taken by the provider to address the breach.
   d. The possible exceptions relating to ***technological protection measures*** and law enforcement (Art 4(3) subparagraph 3).

9. While this framework should ensure harmonized rules throughout the EU, some factors further described below may nevertheless lead to differences of approach among Member States.

## II. 2 Areas where different approaches are possible

10. The areas where possible different approaches may emerge are three, further described below.

---

6 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 Official Journal L 281 , 23/11/1995. Article 2(a) of the Data Protection Directive: "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".

11. ***Scope of application of the obligation:*** The obligation to notify personal data breaches under the ePrivacy Directive applies to providers of publicly available electronic communications services. However, Recital 59 of the ePrivacy Directive contains stimulus to encourage Member States to expand the scope of application (emphasis added): "*... Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), regardless of the sector, or the type, of data concerned."*

12. ***Issuance of guidelines by competent authorities:*** The ePrivacy Directive (Article 4(4)) specifically enables national competent authorities to adopt guidelines and issue instructions on the three items mentioned below. Namely:
    a. the circumstances in which providers are required to notify personal data breaches;
    b. the format of the notification, and
    c. the manner in which the notification is to be made.

    Item (a) above enables competent authorities to, for example, determine certain personal information, which due to its sensitivity, if compromised, would inevitably meet the threshold and trigger the need to notify[7]. It may enable them to define situations below a certain threshold that may not require notification.
    Depending on whether and how the competent authorities use this competence it could mean that, at least on these items, there will be some differences of approach. Any guidelines or instructions by the competent authorities are however subject to any implementing measures adopted by the Commission, see further under Sections V and VI.

13. ***Technological protection measures:*** Differences may also arise as far as the implementation of the exception relating to technological protection measures, which must render the data unintelligible to any person who is not authorized to access it. Such possible divergences may arise because under Article 4(3) it is for national competent authorities to assess whether the technological measures are appropriate and if they were applied.

## III. PERSONAL DATA BREACH IN MEMBER STATES

14. The Article 29 Working Party has reviewed the status of the transposition of the new personal data breach provisions into Member States laws. The review is limited in scope (only covering the main lines) and based on the current situation regarding implementation, which is undergoing continuous change as the transposition procedures progress. Therefore these findings should be

[7] Such compromise would constitute "adverse effects" in the sense of Article 4(3) subparagraph 2 (over and above the cases identified in recital 61 as always involving adverse effect);

considered as interim, subject to the changes that will occur as Member States finalise their legislative procedures towards the implementation of the ePrivacy Directive. The following summarizes the findings:

15. ***Status of transposition*.** Transposition of the ePrivacy Directive is due by 25 May 2011. Currently, a minority of Member States are engaged in public consultation. Most of the Member States have draft texts, although the vast majority of them have not reached the status of proposed legislation. None of the Member States appear to have adopted legislation yet.

16. In principle, the above indicates that the implementation efforts have not reached an advanced stage. Regrettably, an important number of Member States appear unlikely to meet the transposition deadline.

17. ***Common core elements.*** The input received from the information collected by national data protection authorities as to the situation in the respective Member States indicates that most Member States are in the process of transposing the provisions of the ePrivacy Directive in a way that is very close to the wording of the Directive. More particularly:

    a. **Definitions.** Most Member States seem to have taken up the definitions of the ePrivacy Directive.

    b. **Thresholds to notify individuals.** Most Member States seem to have copied the threshold of the Directive. However, some Member States have included some changes. For example, the Czech Republic is proposing to add "serious"; Sweden has proposed requiring notification if the breach "can be assumed to impact [the subscribers or users whose data is affected] to a larger extent".

18. **Areas where different approaches are possible.** The input received from Member States illustrates the emergence of some slight differences of approach, further outlined below.

    a. ***Scope***. Despite the incentives to expand the scope of application to actors other than providers of electronic communication services, most Member States have not broadened the scope of the obligation. The exceptions are Germany and Austria. However, this is due to the fact that these Member States had already enacted laws setting forth a personal data breach framework applicable across sectors. Also, in other Member States, national data protection authorities have encouraged notification to themselves and to affected individuals as a matter of good practice. For example, this is the case in the UK and Ireland.

    b. ***Guidance:*** Almost half of the Member States that have draft texts or proposed legislation foresee the adoption of guidelines.

       The body competent for such adoption varies. In most cases, the issuance of guidelines is entrusted to the national data protection authority (such as

in Estonia, Luxembourg, UK and potentially France[8] as well) or to the national electronic communications regulatory authority (Sweden and Finland). In other cases the competence is shared (Germany).

In most Member States, the items regarding which guidance is foreseen basically coincide with those of the ePrivacy Directive. In some cases, however, it appears as if the guidance could be broader. This is the case for Estonia (the national data protection authority can decide exceptions to the obligation to notify) and potentially France[9]. In some cases, the scope of possible guidance seems undetermined (Italy) and in other cases seems more limited than foreseen in the Directive. Most competent authorities have not yet developed any guidance. However, some competent authorities already had some practices or guidelines (such as the UK, Ireland and Germany).

## IV. FUTURE ACTIONS TO BE CARRIED OUT BY COMPETENT NATIONAL AUTHORITIES AND BY THE WORKING PARTY 29

19. This exercise has shown that the awareness and status of implementation of personal data breach notification procedures varies from one Member State to another. As pointed out above, some Member States have already gained experience on this topic whereas others have not done so yet.

### *a) Setting up a platform to raise authorities' awareness on security breach procedures*

20. The Article 29 Working Party considers that this situation should be remedied so that national data protection authorities are on a similar playing field. To achieve that, the Article 29 Working Party is committed to creating a sub-group which should operate as a platform to exchange views and knowledge. The goal of the platform is to foster harmonised procedures and concepts applicable to security breach notification across Member States[10].

21. More particularly, and without prejudice of future changes to this list in the light of the needs, the Article 29 Working Party would like to initially concentrate on the following areas: *(i)* the creation of a pool of knowledge regarding the circumstances under which notification to individuals is necessary; *(ii)* the setting forth of guidelines regarding the procedure and the timing for notification (both to national data protection authorities and to affected individuals); and *(iii)* the establishing of criteria on how to measure the effectiveness of technical protection measures.

---

8 According to non-finalized discussions: future adopted legislation may differ.

9 Idem.

10 It should be noted that it is up to Member States to determine the competent national authority, which has to meet the requirements of Article 3 of the Framework Directive. This means that in some Member States national data protection authorities will be competent to receive notifications for personal data breach notification whereas in other Member States it may be other bodies such as the national regulatory authority. Regardless of this, national data protection authorities expect to be involved in this exercise.

***b) The coordination of procedures in case of cross-border data breaches.***

22. In addition, the platform should be used to coordinate the procedures in case of cross-border data breaches. It is expected that many data breaches will have cross border elements. For example, the data controller may be established in one Member State, and yet the breach may happen in another Member State/s, for example, if facilities where hacked there. It may also happen that the Member State where the breach took place does not coincide with the location of most affected individuals, or that the data breach has happened simultaneously in various establishments. In other cases, it may be uncertain where the breach has happened while the effects are felt in many Member States. In all these cases (and possibly others), there may be a need for competent authorities to coordinate.

23. In the light of the above, the Article 29 Working Party is committed to start a coordination exercise. The first item of this exercise would entail an analysis of the applicable law and competent authority in cases of cross border personal data security breaches. This would entail also looking into information and reporting obligations and the creation of the relevant procedures.

24. This platform will be be set up as soon as possible. This is particularly helpful insofar as it would help the Article 29 Working Party to provide input in the context of the EU legislative policy actions related to personal data breaches (see Section V and VI).

## V. FUTURE EU LEISLATIVE ACTION RELATED TO PERSONAL DATA BREACH

25. As outlined above, the future possible legislative developments in the area of personal data breach are expected in the two contexts further described below.

26. The first one is foreseen ***in the ePrivacy Directive.*** The ePrivacy Directive sets the overall legal framework on personal data security breach. However, in order to ensure consistent implementation and application of the framework, the Directive delegates powers to the Commission (Article 4(5)). This empowerment is justified to ensure that individuals across the Community enjoy an equally high level of protection and that entities that suffer personal data breaches are not burdened with diverging notification requirements. More particularly, the powers refer to the circumstances, format and procedures applicable to the information and notification requirements. These are the areas where national competent authorities are competent to issue guidelines.

27. Given among other things the various consultations the Commission is obliged to undertake, the procedure to adopt technical implementing measures may last for at least a year[11]. Before adopting any measures, the Commission must engage in a consultation of various entities. In particular, *ex* Art. 4(5), with

[11] The procedure involves the preparation of the measures (following consultation with stakeholders), the opinion by the Committee comprised by representatives of Member States and final adoption by the Commission. Afterwards, there is a right of scrutiny by the European Parliament.

ENISA, the EDPS and the Working Party 29. Furthermore, pursuant to the same article, the consultation must also involve other "*relevant stakeholders*", particularly in order to inform of the best available technical and economic means of implementation.

28. ***Policy developments regarding personal data breach have also been announced within the framework of the review of Directive 95/46.*** The review of the ePrivacy Directive gave an opportunity to the legislators to introduce mandatory personal security breach requirements. Given the scope of application of the ePrivacy Directive, the personal data breach obligation was limited to providers of publicly available electronic communications services. However, this sector-specific provision must be complemented with an extension of the obligation to notify to cover all data controllers, to be materialised in the context of the review of Directive 95/46. The Commission's Communication "*A comprehensive approach on personal data protection in the European Union*" confirmed the Commission's view that it is important for individuals to be informed when their data are accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons. Pursuant to the Communication the Commission intends to examine the modalities for the introduction in the general legal framework of a personal data breach notification covering all sectors, which should be consistent and coherent with that set forth in the ePrivacy Directive[12].

29. The Article 29 Working Party welcomes this as it is convinced that notices of security breaches, applying across sectors, will help individuals take the necessary steps to mitigate any potential damage that results from the compromise. Furthermore, the obligation to send notices informing of security breaches will encourage companies to improve data security and enhance their accountability.

## VI. RECOMMENDATIONS FOR FUTURE DEVELOPMENTS ON DATA BREACH NOTIFICATION

30. Having analyzed both the situation in Member States (section III) and the current situation at EU level (Section II and IV), the Article 29 Working Party wishes to formulate some conclusions and recommendations. Namely:

***As to the scope of the obligation***

31. The Article 29 Working Party supports the introduction of a provision on personal data breach notification in the general instrument, to extend this obligation to all data controllers. The reasons that justify the obligation fully apply to data controllers other than providers of electronic communication services. **Therefore, the Article 29 Working Party welcomes that the Commission is considering such an extension in the context of the review of Directive 95/46.**

---

12 See pages 6-7 of the Commission's Communication "A comprehensive approach on personal data protection in the European Union", COM (2010) 609 final, adopted on 04.11.2010.

***As to the core elements (definitions, thresholds) of the personal data breach framework***.

32. Most Member States seem to be following closely the core elements of the personal data breach provisions in the ePrivacy Directive. This includes the definitions, thresholds and other main elements. Accordingly, it is expected that competent national authorities and relevant actors will increasingly rely on these concepts to deal with personal data breaches. In the next years, these concepts and procedures will therefore "solidify" across EU Member States.

33. The above suggests that in broadening the obligation to other actors, **the Commission should rely on the same or very similar core elements as in the ePrivacy Directive**. This applies to the definition and more particularly to the threshold to notify data subjects, which requires notification when personal data breach is likely to adversely affect the personal data or privacy of individuals.

34. After having gained experience applying those criteria, it would be counterproductive to apply different ones to data controllers other than providers of electronic communication services. More importantly, the specific rules on personal data breach in the amended ePrivacy Directive were broadly discussed during the legislative procedure that preceded the adoption of the ePrivacy Directive. In this debate, the opinions of the Article 29 Working Party[13] and the EDPS[14] were taken into consideration together with the views of other stakeholders. The rules reflect the views of different stakeholders. They represent a balance of interests: while the criteria triggering the obligation to notify individuals are, in principle, adequate to protect them, they do so without imposing overly cumbersome and unnecessary requirements. Ultimately, a personal data breach is a personal data breach regardless of whether the controller is a carrier, a bank, a manufacturer or a public sector entity. The rules must therefore be the same, or there will not be a level playing field. The Commission's statement in the Communication "*A comprehensive approach on personal data protection in the European Union"* that a "*consistent and coherent approach on this matter will have to be ensured*" while at the same time stating that the ePrivacy Directive will not be affected, seem to confirm this approach.

***Delegated powers/implementing measures.***

35. Many Member States refer to the provision of the ePrivacy Directive enabling their national competent authorities to issue guidance on circumstances, the format and the procedures applicable to the information and notification requirements. These are the same aspects which the Commission may regulate through implementing measures.

---

13 See WP 29 Opinions 150 and 159 mentioned above.

14 EDPS Second Opinion of 9 January 2009 on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ C 128, 06.06.2009, p. 28.

36. The Article 29 Working Party considers that it would be beneficial to achieve a harmonized personal data breach framework across Member States, and recognizes that such a harmonized framework should take into consideration the experience that is currently being gained by national competent authorities that are already experimenting with personal data breaches.

***a) As to the timing***

37. Taking into account the length of the procedures on implementing measures, and the mandatory consultation with various stakeholders as well as ENISA, the Article 29 Working Party and the EDPS, the ***Article 29 Working Party calls upon the Commission to start this task as soon as possible***. Towards this end, the Article 29 Working Party suggests that the Commission, among other things, engages in a survey of early practices that are being developed by competent authorities, and proposes implementing measures based on collected feedback. National experience that is being gained in Member States may provide very valuable input. It seems particularly important to harmonize the circumstances under which all relevant breaches are notified, particularly with regard to organizations that are established in several Member States. A late intervention would increase the risk of establishing permanent diverging approaches among Member States.

***b) As to the content***

38. Based on the framework provided in the ePrivacy Directive, the Article 29 Working Party wishes to encourage the Commission to consider the following items as possible areas to be subject to exercise of its delegated powers.

***First,*** standardize the circumstances under which a personal data breach should be notified. This would entail fine-tuning the meaning of the threshold for notification to individuals. For example, this could include breaches of personal information, which due to its sensitivity, should be deemed to meet the threshold. Harmonization on this topic is particularly relevant for operators active in more than one Member State (i.e., it would be undesirable if competent authorities issued different notification orders to the same operator for the same personal data breach).

***Second,*** set forth the procedure to follow in case of a data breach. This could include, for example, requiring more concrete deadlines for notification of the breach to the authorities. It could also require concrete procedural steps which may include, for example, a request to restate the security of the system or a requirement to enlist forensic investigators in order to ascertain the facts and circumstances surrounding the breach.

***Third,*** based on the experience gained by national competent authorities, including in the application of Articles 19, 20 and 21 of Directive 95/46, the Article 29 Working Party invites the Commission to develop a standard EU format to be used when notifying. In the case of those addressed to the competent authorities, it should include at least headlines e.g. description of the breach, the effects, and the measures taken/proposed, in order to help

authorities to carry out the assessment of the breach in the context of their supervisory powers.

***Fourth,*** the Article 29 Working Party supports the determination through implementing powers of the allowed modalities for serving notices to individuals, with guidance as to whether email and telephone notification are permitted. The same applies to cases where notification to individuals via newspapers etc will be allowed (for example, if addresses are not known). In doing so, the rules should allow space for the judgement of competent authorities in the light of the circumstances of each case.

***Fifth,*** guidance would also be required in respect of the format applying to the data breach information providers are expected to keep in an inventory[15].

***Sixth,*** based on the experience that is being gained by competent bodies in Member States, and considering the input of stakeholders mentioned under Article 4(5), the Article 29 Working Party also calls upon the Commission to issue guidance on the technological protection measures which, if applied and depending how they were applied, would exempt from notification.

***c) As to their scope of application***

39. Last but not least, the Article 29 Working Party is of the view that any implementing measures developed under the ePrivacy Directive should be applicable also to other data controllers. The Commission should therefore avoid any temptation towards sector specific measures, instead focusing on measures of general applicability. A duplication of efforts is not warranted.

Done at Brussels, on 5 April 2011

*For the Working Party*
*The Chairman*
*Jacob KOHNSTAMM*

[15] Pursuant to Article 4.4., second paragraph covered entities must maintain an inventory of breaches sufficient for the authorities to verify compliance with their notification obligations.