Information Society Services and Mandatory Data Breach Notifications: Introduction to Open Issues in the EU Framework

by **Jelena Burnik**, Slovenia
MSc Communication Regulation and Policy, Information Commissioner of Slovenia.*

Abstract: In 2011 Sony suffered an extensive breach in its online game network that led to the theft of account data of 77 million users from all over the world. This was one of the largest internet security break-ins that resulted in a large scale personal data breach. As an answer to numerous incidents of security breaches where personal data have been compromised, an instrument of mandatory data breach notification is currently being implemented in the European Union that follows the approach taken in the United States. The revised e-Privacy Directive and the fresh proposal for a General Data Protection Regulation both introduced a provision whereby the entity suffering a breach will have to notify the competent authorities of the breach. Many large online service providers, operate globally, offering its services to users in different countries and processing users' data in different locations, in the EU and wider. In case such a provider suffers a data breach, and on condition that European law applies to its operations, the provider will be obliged to report the data breach to the authorities and possibly to the injured individual users.

The paper presents the changes in the regulatory framework in the EU and tackles the question of how the new regulations on mandatory breach notifications will affect online service providers, especially the ones operating across borders. The paper presents the legal framework, assesses its implications and sheds light on the issues that will arise, in terms of applicable law, competencies of the national authorities and the rights of the injured individuals.

Keywords: Information society service providers, Data protection, Mandatory breach notification, EU data protection framework.

Recommended citation: Jelena Burnik, Information Society Services and Mandatory Data Breach Notifications: Introduction to Open Issues in the EU Framework, 3 (2012) JIPITEC 126, para. 1.

A. Introduction

1 In 2011 Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts from all over the world. This was one of the largest internet security break-ins resulting in a large scale personal data breach.[1] Criticism over Sony's response to the break-in accumulated also with regard to its relatively late notification of their customers because it took a few days before the users were notified. The customers argued that Sony did not allow them "to make an informed decision as to whether to change credit card num-

bers, close the exposed accounts, check their credit reports, or take other mitigating actions".[2] The fact that credit card data was said to be encrypted did not mitigate the responsibility Sony had towards its clients. The Sony incident was, however, only the last of the well-publicized breach cases, which opened the questions of when to notify the data subjects and what to do if the data in question was encrypted.

2 As an answer to these incidents of security breaches where personal data is compromised, an instrument of mandatory data breach notification has been introduced in many of the States in the U.S. and is currently being implemented in the European Union. The revised e-Privacy Directive[3] introduces a new obligation for electronic service providers (internet and communications providers) – a mandatory notification to the national authority and the users in the case of a personal data breach. A very similar provision is foreseen in the new proposal of the Data Protection Regulation[4] that is on the way to replace the Data Protection Directive 95/46/EC[5] in the years to come. This provision will horizontally affect all data controllers in all sectors, thus also online service providers. Many large online service providers, such as the mentioned Sony online gaming network, operate globally, offering its services to users in different countries and processing the users' data in different locations, both in the EU and wider. In case such a provider suffers a data breach, and on condition that European law applies to its operations,[6] the provider will be obliged to report the data breach to the authorities and, if necessary, to the injured individual users.

3 As the provisions are only beginning to be introduced in the telecoms sector and are only yet proposed for implementation in all other sectors, many questions regarding practical implementation remain unanswered, such as the what are the thresholds for when a breach must be notified, what are the standards of encryption, what channels should be used for notifying the individuals, etc. Bearing in mind the cross border nature of large online service providers, issues may arise, such as who is the competent authority to receive the notification, which entity of the provider is supposed to report the breach if the provider has establishments in different states, how should the authorities cooperate in such cases, when and how the users should be notified of a breach, etc. To achieve harmonized implementation that will result in greater data protection for the users whose data was compromised, further guidance will be necessary (either from the national authorities, or in terms of harmonization, even better from the European Commission).

4 In the present paper I propose to tackle the question of how the regulations on mandatory breach notifications will affect individuals and information society service providers, especially the ones operating across borders. I will briefly touch upon the U.S. experience with breach notifications, and then proceed to the new legal framework in the EU. I will assess its implications there and shed light on the issues that will arise in terms of content, form and scope of notifications, applicable law, competencies of the national authorities and the rights of the injured individuals.

B. Data breach notifications and the U.S. experience

5 Today we live in a world of online services. We shop online, socialize online, make use of e-government services and e-banking, buy plane tickets, and we play online. The information society services are ever improving, capable of processing immense quantities of our data, remembering our preferences, and also tracking our activities to offer us better service and, of course, to target us with relevant advertisements. The development of information society services is important for societal development and for the economy. However there is an obstacle – we, the citizens need be able to trust the online service providers in order to make the most out of the offers. In this realm, data protection issues are emerging on a daily basis. New technological tools that facilitate seamless gathering of information and sophisticated ways of processing that information have greatly contributed to the increasing severity of today's information privacy problems and concerns.[7]

6 In the last ten years we witnessed immense changes in the ways personal data is processed and got acquainted with new risks, such as identity thefts. Many well publicised cases of unlawful acquisition of individual's data held by reputable organizations added to the idea that we need a more robust data protection framework. Data breaches occurred in the private sector, as well as in government agencies, educational institutions, etc. The compromised data included credit card numbers and security codes, user names and passwords, social security numbers, sensitive data, search histories etc.[8] [9] New frameworks for protection of personal data are thus on the agenda in the U.S., as well as in the EU and globally.[10] As an answer to incidents of security breaches where personal data is compromised, an instrument of mandatory data breach notification is being introduced.

7 The rationale behind the data breach notification legislation that was initially enacted in a number of U.S. states was that by exposing poor security measures of organisations, it would give them incentives to build stronger protection for the data they process in order to avoid potential sanctions and bad reputations. The other rationale was that individual had

a "right to know," to be informed on how organizations used or abused their data, and to be able to take appropriate actions to prevent identity theft, additional financial damage, etc.[11] Such legislation is now seen as especially important in terms of personal internet security. Additionally, traditional civil litigation has proved ineffective when a company's negligence in security of data processing leads to identity theft. It is very hard for the consumer to prove duty, negligence, or causation and is thus unlikely to succeed in court. Another difficulty is the fact that the consumer in this case lacks redress until damages actually occur. The organizations therefore do not have an incentive to share information on possible data breaches.[12]

8 On the other hand, opponents to data breach notification legislation argue that it creates unnecessary costs for organizations and thus reduces innovation and commercial activity. If risks of data exposure or adverse effects on the individuals in case of a data breach are low enough then the organizations only suffer greater costs, whereas the positive effects of greater protection of the individuals is questionable. They also claim that risks of identity theft are actually very low. The opponents do not see the solution in stricter regulation, but in forms of self-regulation, which could also work as market differentiator.[13]

9 An analysis of the U.S. states' data breach laws by Romanosky, Telang and Acquisti[14] shows that legislation is consistent in central themes. The laws of different states require a notification in a timely manner if personally identifiable information has been compromised or has become available to an unauthorised person, and if its exposure presents a negative effect for the injured individual.[15] The trigger or the threshold by which the notification must be made, however, is different. Part of the states require notification when it is reasonably assumed that the data has been acquired by an unauthorised party, whereas the other states have a higher threshold and require notification only if it is reasonable to expect that the exposed information will cause harm to individuals. The benefit of a lower threshold is that the individual is aware of potential breaches; however it may also result in too much reporting and exaggerated actions or ignorance toward the notices.[16] The laws are not applicable across all sectors. Notification processes and channels are defined as well – the entities to receive notifications may be the individuals, law enforcement, state agencies and/or Congress. The channels of notification are prescribed but commercially reasonable channels may be used. The laws include exemptions for the firms already governed by specific legislation; for those that have contacted law enforcement and believe notification to consumers may jeopardize the investigation; if the number of affected individuals is below threshold; and for the data that has been encrypted. Penalties are foreseen for failing to notify.[17]

10 A critique of the U.S. patchwork framework for data breach notifications recognises the clear need for a comprehensive approach and exposes some of the issues: the absence of federal legislation creates legal uncertainty for the organizations and for individuals, and it incurs costs for the cross border data controllers complying with different regimes. Many authors therefore advocate the introduction of a federal law. Inadequate enforcement of state legislation is highlighted.[18] The problem of the risk-based trigger for notification is also raised for putting the interests of the organizations before the interests of the potentially injured individuals.[19] Also, the level of adequate encryption is not specified in the state laws, even though encryption creates an exemption to notification. A call for a clearer specification of encryption is present.[20] Winn argues that the focus should not be on notifications of data breaches but rather on preventive measures where the organizations would reduce risks at a systematic level. Regulation of the security aspects of data processing should not only be statutory but also exist in the form of self-regulation.[21]

C. European data breach framework

11 In the EU it has been argued that today's technology is not the same as when Data Protection Directive 95/46 was adopted. Globalisation has given businesses an increasing worldwide dimension. Cross border data processing and international transfers have tremendously increased over the past years.[22] Also in the light of a number of security and data breaches that have happened over the past years (stolen computers with data on citizens, attacks on networks), culminating with the attack on the Sony online Playstation Network, the new frameworks for data protection and privacy in electronic communication emphasize the importance of an instrument of mandatory data breach notification. A breach notification requirement is seen as having the potential to increase the level of data security in Europe and foster reassurance amongst citizens as to how their personal data is being secured and protected[23] by different data controllers, from the providers of electronic communication services to other online data controllers.

12 As the European Data Protection Supervisor argues, "*...security breach notification serves different purposes and aims. The most obvious one /.../ is to serve as an information tool to make individuals aware of the risks they face when their personal data are compromised. This may help them to take the necessary measures to mitigate such risks. For example, when alerted of breaches affecting their financial information, individuals will be able, among other things, to change passwords or cancel their accounts. In addition, security breach notification contributes to the effective application of other princip-*

les and obligations in the Directive. For example, security breach notification requirements incentivize data controllers to implement stronger security measures to prevent breaches. Security breach is also a tool to strengthen the responsibility of data controllers and, more in particular to enhance accountability /.../. Finally, it serves as a tool for the enforcement by data protection authorities. The notification of a breach to DPAs may lead to an investigation of the overall practices of a data controller."[24]

13 Mandatory breach notifications are a tool for individuals to protect themselves against identity theft, financial loss, loss of business or employment opportunities, and physical harm.[25] Notices of security breaches, applied across sectors, can help individuals take the necessary steps to mitigate any potential damage that results from the information compromise and encourage companies to improve data security and enhance their accountability.[26]

I. The revised e-Privacy Directive introduces a mandatory breach notification

14 In the EU data breaches were firstly addressed with Directive 2009/136/EC, including amendments to the Directive 2002/58/EC – more widely known as the revised e-Privacy Directive. The revised e-Privacy Directive introduced a new obligation for electronic communications service providers (the providers of communications and internet access)[27] – a mandatory notification to the national authority and the users in case of a personal data breach.

15 A personal data breach is defined as *"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"* (article 2(h)). A clear reference is made to personal data, defined in the Data Protection Directive 95/46/EC 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."* A personal data breach therefore means any unauthorized disclosure or unauthorized access to personal data, from cases of simple accidental destruction or alteration, which is not followed (or very unlikely to be followed) by unauthorized access,[28] to cases where large amounts of personal data have been disclosed or accessed by unauthorised entities.

16 Article 4 of the revised e-Privacy Directive specifically places an obligation on the providers of publicly available electronic communications services to notify a personal data breach to the competent national authority *without undue delay*. When the personal data breach is likely to *adversely affect* the personal data or privacy of a subscriber or individual, the provider also has to also notify the subscriber or individual of the breach. The competent national authority may require the provider to notify the subscribers and individuals concerned, if it deems that the breach may likely have an adverse effect on the subscribers or individuals. Such notification to the subscriber or individual is not required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented *appropriate technological protection measures* to the data in breach, that render the data unintelligible to any person who is not authorised to access it.

17 Article 4 of the revised e-Privacy Directive also gives guidance as to the content of the notification. The notification to the subscriber or individual must include at least (1) the description of the nature of the personal data breach and (2) the contact points where more information can be obtained, and must (3) recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority must, in addition, describe the consequences of, and the measures proposed or taken, by the provider to address the personal data breach. Providers must, according to the provision, maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken to enable the competent national authorities to verify compliance.

18 As seen from the above, some common core elements are defined by the Directive. One is the legal thresholds that apply: the provider must notify any breach to the competent authority, but only notify the injured individuals if the breach is likely to adversely affect their personal data or privacy. An exception is included if the data was rendered unintelligible. The content and time (without undue delay) of notification are also defined. However, as the Working Party 29 argues, the provision is not specific enough to prevent un-harmonized implementation among different Member States[29]. Different approaches may emerge in relation to the (1) scope of application of the obligation, (2) technological protection measures and (3) further specific guidance by national authorities. Regarding the scope of application, the obligation to notify a breach is only put on the providers of publicly available electronic communications services. However, the Directive in the recitals encourages Member States to expand the scope of application to other data controllers horizontally, regardless of the sector or data concerned.[30] Differences may also be established regarding the technological protection measures, which must render the data unintelligible to any person who is not authorized – if this is the case the provider is exempt from

notification obligation. National authorities are to be free in the decision regarding appropriate technological measures if not further prescribed by the Commission.[31]

19 The Directive furthermore leaves the door open to the national authorities to issue greater guidance regarding the implementation, such as the circumstances in which providers are required to notify personal data breaches, the format of the notification, and the manner in which the notification is to be made. However if it is deemed necessary to ensure consistency in implementation, such further guidance and measures may be issued by the Commission directly, after consultation with (among others) Working Party 29.[32] As can be observed from one of the recent published documents, the Working Party 29 has given its opinion on the draft measures proposed by the Commission. The Commission is proposing to clarify some parts of the notification procedure: developing the notion of "*undue delay*" and recommending, that the first (incomplete) notification should happen within 24 hours of the discovery, and a detailed one no later than 3 days after initial notification. It details the minimum content of the initial notification and of the completed notification. The Decision clarifies that including "information about a personal data breach in a regular invoice" is not adequate, but mentions notifications through national media. It also highlights 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 suggest that the related cryptographic keys must not be easy to guess and must not have been compromised in any security breach.[33]

20 The deadline for transposition of the amended e-Privacy Directive passed in May 2011; however, many Member States have not yet implemented the changes into their national legislation. One of the rare examples of Member States that has implemented the changes and also issued further guidance regarding data breach notifications is Ireland.[34] Ireland adopted a Personal Data Security Breach Code of Practice[35] which applies horizontally to all data controllers, except for the providers of electronic services. The Code of practice specifies that in case of a breach the data controller must give immediate consideration to informing those affected. In appropriate cases, *data controllers should also notify organisations that may be in a position to assist in protecting data subjects including,* where relevant, the police, financial institutions etc. Guidance as to the technological measures which make data unintelligible to unauthorised entities is offered – a high standard of such measurers (such as encryption) is required.

21 The Irish Code of Practice also offers some specific guidance on the threshold of *when the breach must be reported to the authority*. The e-Privacy Directive provides that all breaches have to be notified to the authorities. That also includes, for example, letters being sent to wrong recipients. It is easy to imagine the burden on the authorities, who are trying to focus on cases that present a higher threat to a greater number of individuals, but must instead devote the resources to all breaches in question. The Irish guidance provides for a threshold – not all breaches have to be reported and thus the resources can be allocated more efficiently.[36] All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when *the full extent and consequences* of the incident *has been reported without delay directly to the affected data subject(s)* and *it affects no more than 100 data subjects* and it *does not include sensitive personal data or personal data of a financial nature*.

22 In case of doubt - in particular any doubt related to the adequacy of technological risk-mitigation measures - the data controller should report the incident to the Office of the Data Protection Commissioner. The initial contact with the Office should happen within *two working days* of becoming aware of the incident, outlining the circumstances surrounding the incident. The Office then makes a determination regarding the need for a detailed report[37] and/or subsequent investigation. The Office may sanction for breach of the Code.

II. The Proposal for a General Data Protection Regulation

23 In January 2012, the European Commission officially published the long expected proposal for a new framework regarding data protection in the EU, in the form of a General Data Protection Regulation, which is to replace national data protection legislation and thus enable full harmonisation of the data protection rules across Member States. During the preparatory phases the Commission emphasised the importance of informing the individuals about data breaches if they occur. The Commission expressed its intention to examine the possibilities for the introduction in the general legal framework of a personal data breach notification covering all sectors, consistent with the one for providers of electronic communication services, set in the revised e-Privacy Directive.[38]

24 Article 29 Working Party has, in recent years, strongly argued for a horizontal obligation for all data controllers to be obliged to notify the authorities and/or users on personal data breaches. The background behind the idea is the ever increasing role of the information society services in everyday life of all EU citizens and the amount of personal data processed by these services, namely e-banking ser-

vices, private sector medical records, online shopping and more.[39]

25 Articles 31 and 32 of the newly proposed General Regulation thus introduce an obligation to notify users of personal data breaches, building on the personal data breach notification in Article 4(3) of the e-Privacy Directive. The General Regulation is at times even more specific and introduces a 24 hour deadline:

> *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours (Article 31 of the General Data Protection Regulation).*

26 It also clarifies the duty of a contractual data processor to alert and inform the data controller immediately after the establishment of a personal data breach. The content of the notification remains similar to the framework proposed by the e-Privacy Directive,[40] so as the obligation put on the controller to document any personal data breaches and make the documentation available for supervisory authorities. The Commission has reserved for itself the possibility to adopt a standard format for notifications and other specific measures.[41]

27 The General Regulation reiterates that the controller must, after the notification to the authorities communicate the personal data breach to the data subject without undue delay when the personal data breach is likely to adversely affect the protection of the personal data or privacy of that data subject. It must describe the nature of the breach and contain at least the information on the contact details of the data controller and the recommendations regarding mitigation of adverse effects. The communication of a personal data breach to the data subject is again not required if the controller demonstrates to the supervisory authority that it has implemented appropriate technological protection measures. The supervisory authority, having considered the likely adverse effects of the breach, may then require the controller to notify the breach to data subjects.

D. Open questions regarding data breach notifications

28 The European model seems to follow the recommendations from the U.S. experience in that the data breach legislation is intended to apply across sectors, to all organizations processing personal data. Oversight is given to competent authorities, and the content of notifications is prescribed.[42] Even though the introduction of the mandatory breach notification is undoubtedly an improvement in the framework for data protection in the EU, there are some yet unsolved issues regarding its successful implementation.

29 In this context the European Network and Information Security Agency (ENISA) found that the following topics have been identified as problematic in the proposed framework: lack of a unified approach towards data breach notifications among sectors and among Member States; different understandings of the nature of a data breach; lack of guidelines on best practices and common formats of notifications; lack of guidelines on effective technical measures for protection of data;, lack of guidelines on follow-up actions after notification, economics of notifications, and cases of exemption from notification; and a lack of reliable and comprehensive data on data breach (trends and statistics).[43] Further work on guidelines regarding the procedure and the timing for notification (both to national data protection authorities and to affected individuals) and on the criteria on how to measure the effectiveness of technical protection measures were among the topics Working Party 29 will concentrate on.[44]

30 In this part I will shortly present some open questions on the procedure and timing for notification and on the technical protection measures. I will focus on the following:

- when to notify the competent authority and the injured individuals;
- the adverse effect on the individuals privacy and data protection;
- the content and form of the notification; and
- technical protection measures

31 Furthermore, I will also address breach notifications in cross border cases, where additional issues of applicable law, competencies of the national authorities and the efficient protection of rights of the injured individuals arise.

I. The threshold of notification

32 The question of a threshold for notifying the competent authority has already been partly addressed above, in the case of the Irish Code of Practice. Considering the resources the authorities have in order to deal with data breach cases, and the danger of notification fatigue if they receive too many notifications,[45] it would seem sensible if certain criteria were developed, so as to allow for the notification of "serious" breaches without undue delay to the authorities, and on the other hand, the breaches with low impact to only be documented, ready to e shown to authorities on request. There might be a thin, fine line between the two types of events. How-

ever, looking from the e-Privacy Directive's perspective or the proposal for a General Regulation, no such thresholds are foreseen at all – all breaches have to be notified to the authorities, and the authorities are left with the task of assessing which notifications are to be given priority.

33 To aid the authorities and the data controllers who have suffered a breach, an impact/severity assessment model was proposed by ENISA, building on two categories: an identifiability[46] requirement and level of exposure. To assess the identifiability requirement one would have to look at the nature of the data breached, e. g. ID data (name, address, data of birth, gender etc), sensitive data in the sense of article 8 of Directive 95/46/EC (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life). The level of exposure would look at the type of breach that took place, e.g. unauthorised or unlawful access, destruction, alteration/modification, disclosure, transmission, processing, storing, and accidental or unlawful loss of personal data. The number of injured individuals should also be taken into account.[47] Such a tool is to be of help to data controllers, when assessing the dimensions of the breach, and also to the authorities when prioritising the cases and when considering whether the injured individuals should be informed.[48]

34 Additionally the deadline for notification "without undue delay" or as proposed in the General Regulation, within 24 hours after the breach was discovered, raises questions. The argument that such prompt notification cannot reveal meaningful information as the breach has not yet been assessed is valid. However, a delay may not always be appropriate due to the potential threats for the injured individuals. ENISA suggested the notification be split into two phases where the initial reaction is merely a report that a breach occurred. The detailed notification can be submitted later, when further analysis of the breach is conducted.[49] As seen from the latest documents the Commission is in favour of such two-tier notification process – the initial notification in 24 hours and an additional one in 3 days.

35 As learned from the review of the U.S. experience with data breach notification criteria, the risk-based approach to the threshold has its drawbacks in terms of protection of the injured individuals but is more favourably accepted by the organizations affected and creates a smaller amount of notifications. A low threshold may produce a significant number of notifications, which may, in turn, produce fatigue (Jones 2007-08). The European model can be said to build on best practices. All data breaches have to be notified to the authorities whereas only the ones that present adverse effect have to be communicated to the individuals as well. The authorities are the safeguard in assessing the adverse effect and may order the organizations to notify the individuals. In a theoretical sense the EU model is expected to produce the desirable outcome, however it has been suggested often that the authorities will be forced to take on a significant number of breach cases (in the telecoms sector and wider), with only limited resources.[50] That is why an assessment model, which would allow authorities to quickly assess the seriousness of the situation and react accordingly, will probably be a necessity.

II. Adverse effect on the individual's privacy and data protection

36 Another open question is the meaning behind the term "adverse effect". European framework foresees that the data controller should notify the injured individual of a breach, when the breach is likely to *adversely affect* the personal data or privacy of that individual. An unauthorised access to a phone number of a member of general society might have a completely different effect on his or her privacy then the unauthorised access and publication of a celebrity's phone number. However, neither the e-Privacy Directive nor the General Regulation offers insight into the tools for assessing the "adverse effect". This seems particularly problematic in the context of the Regulation which does not offer any margin of appreciation as regards to its enforcement in the Member States.

37 ENISA thus proposes that the level of adverse effect is assessed by the following scale:

- low/negligible effect: no or negligible adverse effect - little problems or unpleasantness that can be easily overcome, e.g. loss of time, irritation etc.;
- medium effect: any adverse effects are not very serious and can be overcome, e.g. economic loss;
- high effect: considerable/somewhat serious, but they can be overcome with some effort, e.g. significant economic loss, social/reputation-related adverse effects;
- very high: the adverse effects are extremely serious and significant effort would be required to address them or with possible permanent consequences that cannot be overcome by the persons, e.g. effects on health, or combination of severe economic loss and bruising of one's reputation.[51]

38 A model of severity assessment is not only necessary in the context of clarification of the term "adverse effect," but also in terms of practical implementa-

tion of the data breach legislation. Since all of the breaches will have to be notified to the authorities in the EU, a model for assessment will be of benefit to the authorities, as well as to the data controllers suffering a breach, to be able to locate and resolve the serious cases first. The question of notification to the individuals would be resolved faster, which individuals would benefit from the most.

III. The content and form of the notification

39 The answer to the question of content and form of notification is to an extent offered by the e-Privacy Directive and the proposed General Regulation, which provide for the list of information that should be communicated to the authorities and to the individuals. The authority should receive as detailed information as possible to be able to draw conclusions as to the seriousness of the breach. Development of a standard form, available for electronic notifications, is seen as beneficial[52] in cross border breaches, as well, where authorities from different Member States would have to be notified and would cooperate based on their competencies. The Commission, following the recommendation, proposes two notification forms, with standardised content.[53]

40 Regarding the notification to the individuals, the proposed content includes information about the contact point, information on what personal data has been compromised and how and what service the data controller is offering the individual to mitigate the adverse effects, as well as what steps individuals could consider taking in order to mitigate the adverse effects. The information should be in language that is easy to understand. Other useful information that may be reported includes the type of data, impacts from the breach, and actions being taken by the controller to avoid future breaches.[54]

41 In terms of the content and form of notification, the channel of communication is an open issue (for example, is notification in a newspaper or an e-mail enough in certain situations, or should there be a more proactive phone call if the data in question are sensitive?), as is the language to be used if the controller holds data on subjects residing in different Member States. As seen from the Commission proposal, the national media are recognised as a possible channel for notifications.[55]

IV. Technical protection measures

42 Another open question touches upon the technical protection measures, which may, if they make the data unintelligible to unauthorised persons, provide for an exemption of the notification to the data subjects. The criteria for such technical protection measures should be set in advance and harmonized in all Member States, so as to assure for efficient implementation and legal certainty.

43 ENISA offers some guidance, when the data shall be considered unintelligible:

- if it has been securely encrypted or hashed;[56] and
- if it has been securely deleted (on a media that was physically destroyed, degaussed or deleted with a secure erasure algorithm).[57]

44 The question of technological protection measures is indeed very important as the level of protection present will be the data controllers' strongest argument when unwilling to share the information of a breach with its customers in order to avoid it negatively impacting the sense of trust. Common criteria should be established and harmonized across Member States regarding which technological measures are in fact strong enough, what kind of encryption will suffice, and which standards are to be trusted.

45 Encryption is often regarded as a "silver bullet" that can solve information security problems but it has its limitations. First of all, it can only protect the data at rest and in motion but cannot protect data while the data is actually being processed. Second, it is only as strong as the weakest link.[59] In that sense the Working Party 29 urges the Commission to be more prescriptive regarding encryption and proposes that the 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.*[58]

V. Breach notifications in cross border cases

46 In the ecosystem of providers of electronic communication services and even more in the world of in-

formation service providers (social networks, online gaming environments, online banking, and such) it is expected that data breaches may have cross border dimensions. A data controller may operate in one Member State, but the breach may happen in another if its data centres were attacked there. It may well be that the data controller is processing data of individuals residing in another Member State, or that that the data breach has happened simultaneously in various establishments. The data controller may not be able to uncover where the breach has actually happened, but the effects may be felt in all its establishments in different Member States.[60]

47 The purpose of this chapter is to shed light on the questions of applicable law and cooperation procedures between competent authorities in cases of cross border data breaches. As neither the legislation nor the cooperation procedures have yet been put in place this part will mainly offer open questions and search for potential issues that might arise in the next years due to the horizontal implementation of the data breach notification obligation.

48 The questions in cross border breach cases mainly centre on:

- issues of applicable law, namely which entity of the controller, operating cross borders, should report a breach to which national authority?; and
- how should competent authorities from different Member States cooperate?

49 It may happen that a data controller is established or has capacities in more than one Member State, and serves its clients who are also residing in different Member States. Which authority should therefore receive the notification of a breach in such case? In this case the location of the clients seems irrelevant – they should receive a notification, regardless of the whereabouts of the competent authority. But the authorities must be able to cooperate in this case. In terms of the clients, the language and the channel of communication are more important.

50 A solution might be that each establishment which suffered a breach notifies its national authority. If the breach happened in a German establishment and a UK establishment of the data controller, the German notifies the German authority and the UK establishment notifies the UK authority. The General Regulation proposal introduces a notion of a "main establishment" (Article 4), however in the telecoms sector that notion is missing and other interpretations might be possible. What if a breach happens at a data processor, contracted by one of the establishments? In this case the proposed General Regulation offers a potential answer – the processor should notify the data controller and the latter should refer the notification to the competent authority. What would happen if the location of the breach is unknown? Should the headquarters notify the authority in the Member State where it is established or should all the authorities from all the Member States where the group operates be notified? These are only some of the yet unanswered questions the data controllers that operate across Member States will be faced with.

51 An important aspect in cross border breaches is also cooperation between competent authorities from different Member States. A situation might occur, where more than one authority is competent but the different competent authorities disagree regarding further steps to be taken by the data controller who has suffered a breach in a number of Member States (for example, should it notify the data subjects or not). In this case cooperation procedures should be defined for the authorities to cooperate efficiently, and an instrument should be in place to resolve the situations where authorities disagree. The proposal for a General Regulation offers some guidance in terms of cooperation procedures between data protection authorities (Article 55 and 56), but the terms of cooperation in the context of the telecoms sector are not clear, as the competent authorities are not only data protection authorities but also the national regulatory agencies for telecommunications.[61]

52 What seems to be clear is that the data controllers should not be the ones to decide or search extensively for the authority that is legally competent to receive their notification and consider further actions. The legal framework should be clear enough to allow for a relatively quick decision on the competent authority. Authorities on the other hand should be empowered with tools and guidance to be able to decide efficiently and quickly, whether to deal with a notification or whether to forward it to another authority(es). For the purpose of the telecoms sector a platform should be established to aid communication between competent authorities and the Commission should address the issue of cooperation in its implementation measures. There might be confidentiality constraints in national legislation that prevents the authorities from sharing information openly.

E. Conclusion

53 A great number of security incidents, involving personal data, that have happened in the recent years gave rise to a new mechanism that is now being implemented in the EU – a mandatory breach notification mechanism. The revised e-Privacy Directive and the fresh proposal for a General Data Protection Regulation both introduced a provision whereby the entity suffering a breach will have to notify

the breach to the competent authorities and possibly to the injured individual users.

54 The paper briefly presented the U.S. experience with data breach legislation, focused on changes in the regulatory framework in the EU, and tackled the question of how the new regulations on mandatory breach notifications will affect online service providers, especially the ones operating across borders. The paper assessed the implications of the new proposals and shed light on the issues that will arise, in terms of applicable law, competencies of the national authorities, and the rights of the injured individuals. Even though the introduction of the mandatory breach notification is undoubtedly an improvement in the framework for data protection in the EU, there are some yet unsolved issues regarding its successful implementation. The paper offered insight on the open questions of thresholds, the adverse effect on the individuals' privacy and data protection, the content and form of the notification, and technical protection measures. Breach notifications in cross border cases are also addressed with a focus on the questions of applicable law and cooperation procedures when more than one authority is competent in considering the case of a breach.

55 In order for a successful implementation of the mechanism of data breach notification, it is necessary that the competent bodies (may it be the national bodies, or the Commission) consider all of the described dimensions, where further guidance will be much needed and appreciated, in order to achieve harmonized implementation.

■

* The author can be reached at jelena.burnik@ip-rs.si

1 Tindal, S. (2011). "Sony's data loss didn't breach Privacy Act": http://www.zdnet.com.au/sonys-data-loss-didnt-breach-privacy-act-339323342.htm. Last accessed: 3. 4. 2012.

2 Ogg, E. (2011). "Sony sued for PlayStation Network data breach": http://news.cnet.com/8301-31021_3-20057921-260.html. Last accessed: 1. 4. 2012.

3 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.

4 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), published on January 25, 2012.

5 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.

6 According to the proposal of the General Data Protection Regulation (Art. 4) the Regulation will apply also to data controllers from outside of the EU if they will offer their services to the European citizens or monitor their behaviour.

7 Zarsky, T. (2004). "Information privacy in virtual worlds: identifying unique concerns beyond the online and offline worlds". New York Law School Law Review. 49, 3, 231-270.

8 Such as the CardSystem Solutions, Inc (Faulkner, B., 2007, "Hacking into data breach notification laws" Florida law review 59, pp 1089-1125) and Heartland Payment Systems Inc. (Vijayan, J., 2009, ''Heartland data breach sparks security concerns in payment industry'', Computerworld Security, Last accessed: 1.7.2012) where credit card data were exposed, the Ohio Secretary of State who accidentally posted Social Security numbers of residents; and a recent case of LinkedIn, where user data were compromised (Finkle. J. and J. Saba, 2012, "LinkedIn suffers data breach", http://www.reuters.com/article/2012/06/06/net-us-linkedin-breach-idUSBRE85511820120606, Last accessed 1.7.2012).

9 Jones, M. E. (2007-08). "Data Breaches. Recent Developments in the Public and Private Sectors". A journal of law and policy for the information society. 3(3), pp 556-580.

10 EC, European Commission. (2010). "A comprehensive approach on personal data protection in the European Union". Adopted on 04.11.2010; Department of Commerce (2010a). "Notice of Inquiry. Information Privacy and Innovation in the Internet Economy". Federal Register/Vol. 75, No. 78/Friday, April 23: http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf. Last accessed 28. 1. 2011; Department of Commerce, Internet Policy Task Force (2010b). "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework": http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf. Last accessed 28. 1. 2011; FTC Federal Trade Commission (2010, December). "Protecting Consumer Privacy in an Era of Rapid Change, A proposed framework for Business and Policymakers, Preliminary FTC Staff Report": http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.Last accessed 31. 1. 2011.

11 Romanosky, S., R. Telang, A. Acquisti. (2008). "Do Data Breach Disclosure Laws Reduce Identity Theft?" Heinz First Research Paper.

12 Faulkner, B. (2007). "Hacking into data breach notification laws." Florida law review. 59, p-p 1089-1125.

13 Romanosky, S., R. Telang, A. Acquisti. (2008). "Do Data Breach Disclosure Laws Reduce Identity Theft?" Heinz First Research Paper.

14 *Id.*

15 *Id.*, pp 7-8

16 Jones, M. E. (2007-08). "Data Breaches. Recent Developments in the Public and Private Sectors". A journal of law and policy for the information society. 3(3), pp 556-580.

17 Faulkner, B. (2007). "Hacking into data breach notification laws." Florida law review. 59, p-p 1089-1125; Romanosky, S., R. Telang, A. Acquisti. (2008). "Do Data Breach Disclosure Laws Reduce Identity Theft?" Heinz First Research Paper, pp 7-8.

18 Picanso, K-. E. (2006). "Protection Information Security Under a Uniform Data Breach Notification Law".Fordham Law Review. 75, p.p. 355-390; Faulkner, B. (2007). "Hacking into data breach notification laws." Florida law review. 59, p-p 1089-1125; Romanosky, S., R. Telang, A. Acquisti. (2008). "Do Data Breach Disclosure Laws Reduce Identity Theft?" Heinz First Research Paper; Winn, J. K. (2009). "Are 'better' security breach notification laws possible?". Berkley Law review. 24(3), pp. 1-32.

19 Jones, M. E. (2007-08). "Data Breaches. Recent Developments in the Public and Private Sectors". A journal of law and policy for the information society. 3(3), pp 556-580.

20 Picanso, K-. E. (2006). "Protection Information Security Under a Uniform Data Breach Notification Law".Fordham Law Review. 75, pp 355-390.

21 Winn, J. K. (2009). "Are "better" security breach notification laws possible?". Berkley Law review. 24(3), pp. 1-32.

22 EDPS, European Data Protection Supervisor (2011): »Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union". Adopted 14 January 2011, p. 5.

23 ENISA, European Network and Information Security Agency. (2011). "Implementation of Article 4, Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive". Adopted December 2011, p. 2.

24 EDPS, European Data Protection Supervisor (2011): »Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union". Adopted 14 January 2011, p. 17.

25 WP29, Article 29 Working Party. (2009). "Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)". Adopted on 10 February 2009, p 5.

26 WP29, Article 29 Working Party. (2011). "Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments". Adopted on 5 April 2011, p 9.

27 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 defines electronic communication services providers as providers of services normally provided for remuneration that consists wholly or mainly in the conveyance of signals on an electronic network. This excludes the provision of content and also of information society services, which do not consist wholly or mainly in the conveyance of signals on electronic communications.

28 WP29, Article 29 Working Party. (2011). "Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments". Adopted on 5 April 2011, p. 4.

29 *Ibid.*

30 Recital 59: "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."

31 WP29, Article 29 Working Party. (2011). "Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments". Adopted on 5 April 2011, p 5.

32 See Article 4(5) Directive 2002/58/EC as amended by Directive 2009/136/EC: " ... the Commission may, following consultation with the European Network and Information Security Agency(ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article."

33 WP29, Article 29 Working Party. (2012)." 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.

34 WP29, Article 29 Working Party. (2011). "Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments". Adopted on 5 April 2011, p. 7.

35 Personal Data Security Breach Code of Practice of 29 July 201, accessible at: http://www.dataprotection.ie/docs/7/7/10_-_Data_Security_Breach_Code_of_Practice/1082.htm

36 Whether this solution is in fact compliant with the e-Privacy directive, is another question.

37 According to the Code the controller might be ordered to compose a report, containing the information on the amount and nature of the personal data that has been compromised, the action being taken to secure and / or recover the personal data that has been compromised, the action being taken to inform those affected by the incident or reasons for the decision not to do so, the action being taken to limit damage or distress to those affected by the incident, a chronology of the events leading up to the loss of control of the personal data and the measures being taken to prevent repetition of the incident.

38 EC, European Commission. (2010). "A comprehensive approach on personal data protection in the European Union". Adopted on 04.11.2010, pp 6-7.

39 WP29, Article 29 Working Party. (2008). "Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)". Adopted on 15 May 2008, p.3; WP29, Article 29 Working Party. (2009). "Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive)". Adopted on 10 February 2009, p. 5.

40 Article 28(3) of the proposed directive states: "The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;

(d) describe the consequences of the personal data breach;

(e) describe the measures proposed or taken by the controller to address the personal data breach.

41 See Article 31(5) and 31(6) of the proposed Regulation:

"5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)."

42 Romanosky, S., R. Telang, A. Acquisti. (2008). "Do Data Breach Disclosure Laws Reduce Identity Theft?" Heinz First Research Paper.

43 ENISA, European Network and Information Security Agency. (2011). "Implementation of Article 4, Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive". Adopted December 2011, p. 2.

44 WP29, Article 29 Working Party. (2011). "Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments". Adopted on 5 April 2011, p. 7.

45 ENISA, European Network and Information Security Agency. (2011). "Implementation of Article 4, Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive". Adopted December 2011, p. 21.

46 The term "identifiability" is somewhat awkwardly used by ENISA as it seems to have different meaning in the ENISA recommendation than in the Directive 95/46/EC.

47 ENISA, European Network and Information Security Agency. (2011). "Implementation of Article 4, Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive". Adopted December 2011, pp. 17-18.

48 WP29, Article 29 Working Party. (2012)." 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.

49 ENISA, European Network and Information Security Agency. (2011). "Implementation of Article 4, Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive". Adopted December 2011, p. 22.

50 WP29, Article 29 Working Party. (2012)." Opinion 1/2012 on the data protection reform proposals". Adopted on 23 March 2012, p. 16.

51 ENISA, European Network and Information Security Agency. (2011). "Implementation of Article 4, Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive". Adopted December 2011, p. 17.

52 *Id.*, p. 25.

53 WP29, Article 29 Working Party. (2012)." 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.

54 ENISA, European Network and Information Security Agency. (2011). "Implementation of Article 4, Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive". Adopted December 2011, pp 26-27.

55 WP29, Article 29 Working Party. (2012)." 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.

56 "(a) The data was encrypted with a standardized secure symmetric or asymmetric encryption algorithm, or was hashed with a standardized cryptographic keyed hash function.

(b) The key used to encrypt or hash the data was not compromised in any security breach.

(c) The key used to encrypt or hash the data was generated so that it cannot be guessed by exhaustive key search with current available technological means." See ENISA 2011 at 5.2.2.

57 ENISA, European Network and Information Security Agency. (2011). "Implementation of Article 4, Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive". Adopted December 2011, p. 17

58 Winn, J. K. (2009). "Are "better" security breach notification laws possible?". Berkley Law review. 24(3), pp. 1- 32, p. 14.

59 WP29, Article 29 Working Party. (2012b)." 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, p. 8.

60 WP29, Article 29 Working Party. (2011). "Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments". Adopted on 5 April 2011, p. 8.

61 Member States have made different decisions regarding competence to receive notifications by operators – in the Netherlands for example it is the telecoms regulator, whereas in Ireland it is the data protection authority.