The John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 3 Article 2

2014

Breach Notification Requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance, 31 J. Marshall J. Info. Tech. & Privacy L. 317 (2014)

Samson Esayas

BREACH NOTIFICATION REQUIREMENTS UNDER THE EUROPEAN UNION LEGAL FRAMEWORK: CONVERGENCE, CONFLICTS, AND COMPLEXITY IN COMPLIANCE*

SAMSON YOSEPH ESAYAS†

ABSTRACT

The European Union (EU) legal landscape on data privacy and information security is undergoing significant changes. A prominent legislative development in recent years is the introduction of breach notification requirements within a number of regulatory instruments. In only the past two years, the Community legislator has adopted, and proposed, four different regulatory instruments containing breach notification requirements. There are also existing requirements for the telecom sector. This creates a complex mesh of regulatory frameworks for breach notification where different aspects of the same breach within the same company might have to be dealt with under different regulatory instruments, making compliance with such requirements challenging. In this article, the existing and en route breach notification requirements under the EU legal framework are examined – elaborating their potential areas of convergence or conflict and the resulting complexity in compliance with such requirements. To this end, the article

* This article was written as part of the Confidential and Compliant Clouds (Coco Cloud) and RASEN research projects. Both projects are funded by the European Commission (EC) via the Seventh Framework Programme, grant agreements no. 610853 and 316853 respectively.

† Samson Yoseph Esayas is a researcher at the Norwegian Research Center for Computers and Law (NRCCL), University of Oslo. His current research focuses on data privacy, legal aspects of cloud computing, and compliance risk management in using and developing information technology services. Other areas of research include Internet governance and policy, largely from the perspective of developing countries. Thanks are due to my colleagues on the Coco Cloud and RASEN projects.

examines the scope of the notification regimes, the types of breaches, when a breach is considered to occur under the relevant rules, and the relevant requirements to notify stakeholders. Furthermore, the article examines why a proactive approach to compliance with breach notification requirements is essential and suggests the need to address breach notification requirements in conjunction with security risk analysis, which is being mandated in most of the regulatory instruments.

1. INTRODUCTION

Advancements in technology and the Internet are significantly changing the way people behave and interact – making day-to-day life easier and more efficient. However, such developments also bring their own concerns. Privacy and security are at the forefront of such concerns, both for individuals as well as for businesses. According to a survey, four out of five Europeans are concerned about the recording of their behavior and feel a loss of control over their privacy.[1] Similarly, 91% of Americans "'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies."[2]

From the business side, "three out of four respondents to a…survey said information security and privacy have become significant areas of concern."[3] Information security breaches are commonplace, with 57% of respondents to European Commission study experiencing incidents that had a "serious impact on their activities."[4] Such incidents would negatively affect the economic and financial wellbeing of the companies.[5] Nonetheless, economic and financial losses are not the only reasons for concern over security and privacy. Organizations are equally concerned

---

1. EUROPEAN COMM'N, SPECIAL EUROBAROMETER 359: ATTITUDES ON DATA PROTECTION AND ELECTRONIC IDENTITY IN THE EUROPEAN UNION: REPORT 2 (2011), *available at* http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

2. Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CENTER (2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

3. HARVARD BUS. REV., MEETING THE CYBER RISK CHALLENGE: REPORT 1 (2012), *available at* http://www.computerweekly.com/blogs/public-sector/Meeting%20the%20Cyber%20Risk%20Challenge%20-%20Harvard%20Business%20Review%20-%20Zurich%20Insurance%20group.pdf.

4. Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union 2, COM (2013) 48 final (Feb. 7, 2013) [hereinafter *Proposed NIS Directive*].

5. For example, the global average cost of data breach is estimated to be around $136 per record. *See* PONEMON INSTITUTE, 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1 (May 2013), *available at* http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf.

about the legal and regulatory threats resulting from security breaches and non-compliance with privacy rules. Three out of the top five concerns of respondents to the Harvard Business Review survey are related to legal and regulatory issues.[6] In particular, more than half of the respondents cited the upcoming data protection rules in the EU and "almost half cit[ed] a proposed breach notification requirement."[7] This is particularly important given the size of the financial penalties for breaching these rules. The proposed General Data Protection Regulation (GDPR) introduces a penalty up to 100 Million Euro or 5% of global annual turnover should organizations fail to comply with the regulatory requirements, including data breach notification requirements.[8] In light of such heightened concerns and heavy sanctions, investing in compliance should become a priority for undertakings. This article seeks to contribute to the achievement of organizations' compliance with such requirements by examining the breach notification requirements under the EU legal framework.

Compelling organizations to provide notice of a breach is a specific example of "'regulation through disclosure,' which [is] termed as 'one of the most striking developments' in the last [few decades.]"[9] Such development is associated with the "'communit[ies] right to know' laws, which were developed in order to improve the efficacy of environmental laws[,]"[10] breach notification laws have a similar essence.

In the U.S., the first breach notification law took effect in California in 2003 and currently, 47 States, 3 territories, and the District of Columbia have enacted data breach notification laws.[11] There are also additional state and federal level breach notification requirements target-

---

6. HARVARD BUS. REV., *supra* note 3, at 5.

7. *Id*.

8. 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), at 92, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *GDPR*]. Article 79(6) of the initial Commission draft provides for a penalty of 1 Million Euro or 2% of the annual worldwide turnover but the proposed amendment from the Parliament increases this figure to 100 Million Euro or 5% of the annual worldwide turnover. *See Committee on Civil Liberties, Justice & Home Affairs, art. 79(2a)(c), Report on the 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* at 173 (Nov. 21, 2013) [hereinafter *LIBE Draft*], *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN.

9. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches,* 105 MICH. L. REV. 913, 955 (2007).

10. Jane K. Winn, *Are Better Security Breach Notification Laws Possible*, 24 BERKELEY TECH. L.J. 1133, 1166 (2009).

11. *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

ing certain industries "such as banking, credit unions, insurance, and health care."[12] On average, the penalties for non-compliance with such laws range from "$500 to $1,000 per person whose data is compromised, and some providing for trebling of damages for willful non-compliance."[13] A federal level notification regime for personal data is under consideration in the U.S. Congress.[14]

In Australia, the Privacy Amendment Bill that took effect in March 2014 introduced mandatory data breach notification at the federal level. The Bill requires entities to "notify… affected individuals and the Privacy Commissioner" of breaches "that would result in serious harm to [an] individual."[15] Failure to comply with the provisions could result "in penalties of up to 1.7 million AUD for companies and 340,000 AUD for individuals."[16] In a recent amendment to the Personal Information Protection and Electronic Documents Act, Canada introduced a breach notification requirement.[17] According to the amendment, businesses and organizations are required to report to consumers and the privacy commissioner breaches that pose a "real risk of significant harm to an individual[.]"[18] Non-compliance with the requirements could lead to fines up to $100,000 including potential public announcement of non-compliance.[19]

Across the EU, until recent legislative initiatives, breach notification requirements were only limited to the areas of the telecom sector.[20]

---

12. WORLD LAW GROUP, GLOBAL GUIDE TO DATA BREACH NOTIFICATIONS 119 (1st ed. 2013), *available at* http://www.theworldlawgroup.com/Document.asp?DocID=113469.

13. Fred H. Cate, *Information Security Breaches: Looking Back & Thinking Ahead*, CENTRE FOR INFO. POL'Y LEADERSHIP, HUNTON AND WILLIAMS LLP (2008), *available at* http://www.hunton.com/files/Publication/5ad823e3-6eee-45e2-8366-b9a32e197b81/Presentation/PublicationAttachment/0a2c3d3f-0aa9-497f-8079-099d431ce4fe/Information_Security_Breaches_Cate.pdf.

14. Mauricio F. Paez et al., *U.S. Congress Ready to Enact Data Security and Breach Notification Rules after Recent Consumer Data Breaches*, JONES DAY PUBL'NS (Feb. 20, 2014), http://www.jonesday.com/us-congress-ready-to-enact-data-security-and-breach-notification-rules-after-recent-consumer-data-breaches-02-14-2014/.

15. WORLD LAW GROUP, *supra* note 12, at 4.

16. *Id.*

17. Emily Chung, *New privacy rules target data breaches, fraud,* CBCNEWS (Apr. 9, 2014), http://www.cbc.ca/news/technology/new-privacy-rules-target-data-breaches-fraud-1.2604552; Digital Privacy Act, 2013-14, S. OF CAN. Bill [S-4] (Can.) *available at* http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6524312&File=33#3.

18. Digital Privacy Act, 2013-14, S. OF CAN. Bill [S-4] cl. 10.2 (Can.) *available at* http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6524312&File=33#3.

19. Chung, *supra* note 17.

20. However, different Member States have long implemented general data breach notification requirements or requirements targeting a specific sector in their domestic law. For example, the German and Spanish implementations of the Data Protection Directive contain breach notification requirements for controllers of personal data.

Mandatory breach notification requirements within the telecom sector go as far back as the 2002 ePrivacy Directive.[21] However, it was the 2009 telecom reform, which brought a comprehensive legal framework for breach notification, including mandatory personal data breach notifications. In the past two years, there have been significant legislative initiatives regarding breach notifications within the EU. In June 2013, the EU passed Regulation 611/2013,[22] complementing and harmonizing data breach notification requirements by public electronic communications service providers, including both traditional telecom providers such as telephony companies and Internet Service Providers (ISPs). In February 2013, the Commission placed a proposal for a Directive on Network and Information Security (NIS),[23] which contains breach notification requirements for many entities under the name of 'market operators' such as financial, health, and transport service providers. Furthermore, the Commission released its proposal for the data protection Regulation in 2012,[24] which contains a mandatory breach notification requirement for actors processing personal data of EU residents. Further, in July 2014, the Regulation on electronic identification and trust services (eIDAS)[25] was adopted and introduces breach notification requirement for trust service providers, which could range from telecoms service providers, to banks and other financial institutions, or even universities.

The existence of such an array of breach notification requirements within the EU means that an organization might be required to notify for different aspects of the same breach under different notification regimes, creating significant administrative and financial burden for multinational companies. "This is because for example, in some [EU] countries security and privacy breaches [in the] electronic communications services are dealt with by the telecom regulator."[26] Whereas some other

---

21. Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (EC) (ePrivacy Directive).

22. Commission Regulation 611/2013, of 24 June 2013 on the Measures Applicable to the Notification of Personal Data Breaches under Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications, 2013 O.J. (L 173) 2 (EU).

23. *Proposed NIS Directive*, *supra* note 4.

24. *GDPR*, *supra* note 8.

25. Regulation 910/2014, of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, 2014 O.J. (L 257) 73 (EU) (eIDAS Regulation).

26. Dr. Marnix Dekker et al., *Cyber Incident Reporting in the EU: An overview of security articles in EU legislation*, EUR. NETWORK & INFO. SEC. AGENCY 5 (Aug. 2012), *available at* https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu/at_download/fullReport.

countries require the privacy breaches to be reported "separately to the data protection authorities, or to national cyber security [authorities]."[27] This could lead to a situation where a Pan-European Telecom company might have to notify a telecom sector regulator, a personal data protection regulator, and a general cyber security regulator, potentially in different timeframes and with differing levels of formality. Similarly, providers such as Paypal might have to provide notice of breaches under the proposed GDPR, the NIS Directive, and the eIDAS Regulation. Apart from the resulting administrative and financial burdens of such compliance, it is not always easy for an organization to determine when a breach is considered to have occurred, whether the breach affects personal data, and whether the conditions for notifying the authorities and the individual have been fulfilled.

In this article, the breach notification requirements under the EU legal framework will be examined, elaborating their potential areas of convergence or conflict and the resulting complexity in compliance with such requirements. Given the short timeframes for notification and the fact that the breach has to be notified during a potential crisis period within the organization, non-compliance could easily occur. This calls for a comprehensive approach to dealing with breach notification requirements where organizations understand and address such issues in advance, examine the types of breaches that require notification, the parties to be notified (authority or/and individuals), the formalities required, and taking steps to comply with these requirements beforehand. For this reason, the article suggests that organizations are better placed if they can align and integrate their breach notification compliance into the overall risk management framework and their security risk analysis in particular. Such an approach enables organizations to assess which of the identified security risks might trigger the breach notification requirements and put all the appropriate measures in place. This general approach is particularly relevant given that most breach notification regimes require organizations to conduct security risk assessments.

The remainder of this article is organized as follows: Section 2 introduces the rationales behind breach notification requirements, followed by a discussion of the notification regimes within the EU in Section 3. Section 4 highlights the significance of aligning breach notification compliance with security risk analysis. The article then concludes with some observations.

2. RATIONALE BEHIND AND CHALLENGES OF BREACH NOTIFICATION REGIMES

Compelling entities to disclose a breach carries two major objec-

27. *Id.*

tives: *ex ante* (in terms of shaping the future behavior of the entities) and *ex post* (in terms of increased effectiveness in mitigating the harm of the breach). In its *ex ante* rationale, disclosing a breach imposes a reputational cost on the entity subject to breach and the potential negative publicity serves as an incentive for operators to identify more effective methods of security including an increase in security budgets.[28] This, in turn, is believed to drive forward the market for data security technology.[29] In this regard, data breach notification requirements reinforce another fundamental principle of data privacy within the EU, which is the principle of data security. Somehow related to this rationale is the claim that breach notification enhances an organization's transparency and accountability thereby improving an organization's ability to respond to an incident. Notification of breaches could also be relevant from public policy perspective in the sense that the relevant authorities will be able to learn where policy interventions and cooperation might be required. Nonetheless, frequent notifications are less likely to enhance organizations' security efforts and could also dry up regulatory authorities' resources.

In serving its *ex post* objective, breach notification can help both customers and entities mitigate the harm caused by the breach. On the one hand, organizations will respond more "effectively and vigorously to a breach due to increased public and regulatory scrutiny of its practices."[30] On the other hand, it allows affected individuals to mitigate the damages of the breach. In this regard, breach notification regimes often strive to achieve this objective by compelling the notifying organization to suggest some measures in order to mitigate the harm. Furthermore, the notification of breaches to individuals reinforces the right to information, which is a fundamental principle of the EU legal framework.[31]

---

28. Commission Staff Working Document Impact Assessment: Accompanying document to the Commission proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/19/EC, 2002/20/EC and 202/21/EC Commission proposal for a Directive of the European Parliament and the Council amending European Parliament and Council Directives 2002/22/EC and 2002/58/EC Commission proposal for a Regulation of the European Parliament and the Council establishing the European Electronic Communications Markets Authority, {COM (2007) 697 final, COM(2007) 698 final, COM (2007) 699 final, SEC (2007) 1472 final}, SEC (2007) 1473 final [hereinafter *Impact Assessment*].

29. EUR. NETWORK & INFO. SEC. AGENCY, RECOMMENDATIONS FOR A METHODOLOGY OF THE ASSESSMENT OF SEVERITY OF PERSONAL DATA BREACHES 1 (Clara Galan Manso & Sławomir Górniak eds., 2013), *available at* http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity/at_download/fullReport.

30. Schwartz & Janger, *supra* note 9 at 936.

31. *See, e.g.*, Council Directive 95/46, art. 10-11, of 23 November 1995 on the Protection of Individuals with Regard to Processing of Personal Data and the Free Movement of such Data, 1995 O.J. (L 281) 31 (EC) (Data Protection Directive). Particularly Recital 39 recognizes the right of individual to be informed when data about him/her is disclosed to third parties. *Id*.

In reality, notifying individuals of breaches has failed to provoke the desired behavior from consumers either because of the communication, with 61% of consumers having problems understanding the notification, or because consumers are not paying attention to the notices they receive.[32]

Another major challenge on the effective implementation of breach notification requirements is disclosure disincentives. This is related to the lack of sufficient positive incentives and public resources in such laws that encourage disclosure and "increase the probability of apprehension and conviction for failures to report breaches."[33] This implies that if the probability of detecting unreported breaches is low, organization would be deterred from disclosing breaches that could subject them to enormous financial penalties. This is just beyond a theoretical claim. A survey of 300 security professionals across Europe shows that "only 2% of surveyed EU companies are willing to go public if they suffer a security breach" and only "38% are willing to inform the relevant authorities."[34] Similarly, a study from the U.S. shows that only 11% of security breaches are actually reported.[35] The disclosure disincentive is particularly a challenge with the growing trend for adopting cloud computing services where organizations under such obligation use third party providers to perform certain tasks. The fact that these third parties might not be under similar notification obligations means the disclosure disincentive is especially strong in such cases.[36] In the EU, recent legislative initiatives seem to consider such disincentive by imposing notification obligations on such third parties.[37]

Furthermore, breach notification requirements, particularly those involving notification to individuals are considered as counterproductive and that give rise to "notification fatigue."[38] On the one hand, organizations may be forced to comply with such requirements rather than spending resources on the actual remedying of the breach sustained. For this reason, there are suggestions that incident response

---

32. PONEMON INSTITUTE, 2012 CONSUMER STUDY ON DATA BREACH NOTIFICATION 10 (June 2012), *available at* http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf.

33. Winn, *supra* note 10, at 1144; *see also* Cate, *supra* note 13.

34. *Breach Notification is Now EU Law for Communications Providers*, INFO SECURITY (Aug. 29, 2013), http://www.infosecurity-magazine.com/news/breach-notification-is-now-eu-law-for/.

35. Thomas Claburn, *Most Security Breaches Go Unreported*, INFORMATIONWEEK (Jul. 31, 2008), http://www.darkreading.com/attacks-and-breaches/most-security-breaches-go-unreported/d/d-id/1070576?.

36. Schwartz & Janger, *supra* note 9, at 936.

37. *See infra* Section 0 for more detail.

38. EUR. CONSUMER ORG., E-PRIVACY DIRECTIVE: PERSONAL DATA BREACH NOTIFICATION 2 (2011), *available at* http://www.beuc.org/publications/2011-09742-01-e.pdf.

rather than incident reporting should be prioritized under such laws.[39] Moreover, breach notification regimes might actually disadvantage organizations with substantial investment in security. As Winn notes, spotting a breach requires some kind of sophistication where "smaller and less sophisticated organizations might not even realize they are suffering security breaches."[40] This is particularly alarming given that many EU notification regimes exempt Small and Medium Enterprises (SMEs) from their scope.[41]

On the other hand, notifying individual users of a breach often generates an overload of information to the user that is of little use. Citing the "The Boy who Cried Wolf" fable, Schwartz and Janger argue that if consumers are flooded by frequent cautions with putative harms, it is likely that they "will fail to act when important warnings finally arrive."[42] Supporting such claim is a survey conducted by Ponemon Institute, which found that consumers do not pay sufficient attention to the notices they receive with over 36% of respondents taking their breach notification letter as a junk mail whereas 13% of respondents taking their breach notification email as spam.[43] Therefore, a balance needs to be struck by compelling organizations to notify only those breaches that significantly affect the rights of individuals. In this regard, recent legislative initiatives within the EU adopt a risk-based approach where users only need to be notified of those breaches that 'adversely affect' their rights.[44] Another challenge of breach notification requirements is that the process of conveying information between the businesses and regulatory authorities and between the businesses and individuals opens another door of security vulnerabilities. For example, consumers are already experiencing phishing attacks via emails informing them of data breachs.[45] Similarly, the regulatory authorities themselves may become a repository of large amounts of personal data and, thereafter, a target for attacks.[46] The potential for such instances could be found within the EU legal framework that requires the national authorities to notify individuals if the provider has not already done so or to notify individuals residing in other Member States.

---

39. DEKKER ET AL., CYBER INCIDENT REPORTING IN THE EU, *supra* note 26, at 9.

40. Winn, *supra* note 10, at 1149.

41. *Proposed NIS Directive*, *supra* note 4, art. 14(8).

42. Schwartz & Janger, *supra* note 9, at 916.

43. PONEMON INSTITUTE, 2012 CONSUMER STUDY ON DATA BREACH NOTIFICATION, *supra* note 32, at 8.

44. Breach notification requirements could employ acquisition-based triggers or risk-based triggers. *See* Mark Burdon et al., *Encryption safe harbours and data breach notification laws*, 26 COMP. L. & SEC. REV. 520, 523 (2010).

45. Schwartz & Janger, *supra* note 9, at 952.

46. *Id*. at 963.

3. BREACH NOTIFICATION REQUIREMENTS UNDER THE EU LEGAL FRAMEWORK

3.1. BREACH NOTIFICATION IN THE ELECTRONIC COMMUNICATION SECTOR

The telecom sector is the first of all sectors subject to mandatory breach notification requirements under the 2002/58 ePrivacy Directive. Throughout the years, this regime has evolved through a number of amendments including the 2009 reform on electronic communications and the Regulation 611/2013. Such a development introduces complexity in compliance with the breach notification requirements. At present, there are some breaches that require notification under the Framework Directive.[47] Other breaches might have to be made public together with or separate from the former within the ePrivacy Directive,[48] whereas notification of breaches specifically effecting personal data have to be handled according to Regulation 611/2013.[49] This implies that different aspects of the same breach experienced by a telecom service provider could be subject to different regulatory notification requirements. In this regard, a study of data breach notifications in the telecom sector identifies the need for better clarification and guidance at the EU and local levels in order to "enable European service providers to comply effectively with [such] requirements."[50] The following paragraphs highlight the scope of the application and the notification requirement under these different regimes. The discussion of the existing requirements is motivated by the fact that the emerging requirements are built or extend on the existing breach notification regimes. It also aims to show the relationship between the rules and the resulting complexity in complying with these rules.

3.1.1. The Framework Directive

The 2002/21 Framework Directive had no clear requirement for breach notification. However, its amendment, Directive 2009/140/EC (revised Framework Directive)[51] introduces a breach notification obliga-

47. Directive 2002/21, art. 13a(3), 2002 O.J. (L 108) 33, 55 (EC).

48. Directive 2002/58, art. 4, 2002 O.J. (L 201) 37 (EC) (ePrivacy Directive).

49. Commission Regulation 611/2013, art. 2-3, of 24 June 2013 on the Measures Applicable to the Notification of Personal Data Breaches under Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications, 2013 O.J. (L 173) 2 (EU).

50. EUR. NETWORK & INFO. SEC. AGENCY, DATA BREACH NOTIFICATIONS IN THE EU 4 (Jan. 2011), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn/at_download/fullReport.

51. Directive 2009/140, of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, 2002/19/EC on Access to, and Inter-

tion under Article 13(a)(3) stating that: "Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services."[52]

Subject Matter of the Framework Directive and the Breach Notification Requirement

Overall, the objective of the Framework Directive is to establish a harmonized framework for the regulation of electronic communications services, electronic communications networks, associated facilities and services, and certain aspects of terminal equipment to facilitate access for disabled users. However, the breach notification requirement only applies to providers of *electronic communication network or electronic communication services* that are *publicly available*.

Electronic communications network – Article 2(a) of the revised Framework Directive defines electronic communication networks to include transmission systems and switching or routing equipment that "permit the conveyance of signals by wire, radio, optical, or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals." In addition to the traditional telecommunications networks, such a definition also covers networks for radio and television broadcasting irrespective of the type of information conveyed within these networks. The Directive does not cover the physical kit or any other components that are connected to an electronic communication network or services such as end-user equipment that is used to initiate and receive communications.[53] However, communication networks should be understood as to include "both physical and/or logical networks, including switches and other parts that are crucial to the capacity of the networks to convey signals both within the communications network itself as well as between different communications networks."[54]

---

connection of, Electronic Communications Networks and Associated Facilities, and 2002/20/EC on the Authorisation of Electronic Communications Networks and Services, 2009 O.J. (L 337) 37 (EC).

52. *Id*.

53. TELECOMMUNICATION LAWS IN EUROPE: LAW AND REGULATION OF ELECTRONIC COMMUNICATIONS IN EUROPE 147 (Joachim Scherer ed., 6th ed. Bloomsbury Professional, 2013).

54. BO MARTINSSON ET AL., SWEDISH POST & TEL. AGENCY, WHICH SERVICES AND NETWORKS ARE SUBJECT TO THE ELECTRONIC COMMUNICATIONS ACT? GUIDANCE 7 (Mar. 11, 2009), *available at* https://www.pts.se/upload/Rapporter/Internet/2009/services-e-com-act-2009-12.pdf.

This implies that although the breach notification requirement under Article 13(a)(3) of the revised Framework Directive seems to exclude associated facilities and services, the notification requirements might still apply if such facilities and services are considered to be "crucial to the capacity of the network to convey signals."[55]

Electronic communication services – is defined as a "service normally provided for remuneration which consists wholly, or mainly, in the conveyance of signals on electronic communications networks, including telecommunication and transmission services in networks used for broadcasting."[56] Examples include providers of services of fixed telephony, mobile telephony, fixed Internet access, and mobile Internet access. The Directive does not cover the content of services delivered over electronic communications networks, such as broadcasting content or financial services. In practice, determining whether a certain service is an electronic communication services or not has proven to be very difficult. One of the most controversial issues in such assessment is to what extent and if, for example, Voice over IP (VoIP) providers are covered under the Directive. Another issue of controversy relates to whether the provision of hardware infrastructure services as in the use of cloud computing can be deemed as 'electronic communications service.'[57]

The following three criteria are essential to assessing whether a certain service comprises an electronic communications service. First, "the service is provided to another (external) party."[58] The use of the term "service" implies that there are at least two parties involved, i.e., one providing the service and another party accessing such service.[59] Second, "the service is provided…on commercial grounds."[60] The use of the phrase "normally provided for remuneration" implies that only services provided on a commercial basis are subject to the legislation although this does not exclude remuneration in other forms than direct payments.[61] This means services that are clearly non-profit in nature including but not limited to research networks are outside the scope of the Directive. Third, "the service consists mainly in the conveyance of signals."[62] This is deemed to be the case if the service provider "has con-

---

55. *Id.* at 20.

56. Directive 2002/21, art. 2(c), 2002 O.J. (L 108) 33, 46 (EC).

57. BENNO BARNITZKE ET AL., SEVENTH FRAMEWORK PROGRAMME, CLOUD LEGAL GUIDELINES: DATA SECURITY, OWNERSHIP RIGHTS AND DOMESTIC GREEN LEGISLATION (PART II) 25 (Nov. 2011), *available at* http://www.optimis-project.eu/sites/default/files/content-files/document/optimis-cloud-legal-guidelines-part-ii.pdf.

58. MARTINSSON ET AL., *supra* note 54, at 7.

59. *Id.* at 19-20.

60. *Id.* at 7.

61. *Id.* at 20.

62. *Id.* at 17.

trol (through ownership or agreement) over the signal (the bearer of the information), and thereby has influence over factors such as transmission and quality."[63] For example, Internet service providers have control over the quality of the Internet service. On the contrary, providers of services such as Skype, which built their services on the Internet service provided by the ISPs, do not have any influence or control over the conveyance i.e. over the signal (the bearer of the information).[64] This is because such providers use the end user's existing Internet service, and cannot influence or control the quality of the Internet service.

Publicly available – for the breach notification requirement to apply, the communication networks or services have to be *publicly available*.[65] One major indicator of a service being available to the public is that there is a "general opportunity to connect to the service" for "anyone who is willing to both pay for the service and comply with the conditions for its provision."[66] This means operators of private networks, such as internal company networks (intranets) as well as services to a predetermined user groups are excluded from the scope of application. Examples of services to a predetermined user group include Internet services provided by cafés and hotels, [67] though the status of such services might differ among the Member States.

What kind of breaches should require notification?

The Directive does not define what *a breach of security or loss of integrity* under Article 13(a)(3) constitutes. However, Recital 44 sheds some light, "System complexity, technical failure or human mistake, accidents or attacks may all have consequences for the functioning and availability of the physical infrastructures that deliver important services to EU citizens, including e-Government services." From the Recital, the focus of the "breach of security" is on the "the functioning and availability of the physical infrastructures." In the areas of networks and network interconnections "integrity" is also related to "the ability of the system to retain its specified attributes in terms of *performance and functionality*."[68] Thus, a breach under Article 13(a)(3) of the revised

63. *Id.* at 20.

64. However, a general consensus seems to exist in most EU Member States in considering VoIP services with access to telephone number as electronic communications services covered within such regime whereas Peer-Peer VoIP services precluded from the scope. There are also differences with regard to other services such as e-mails. *See* MARTINSSON ET AL., *supra* note 54.

65. Directive 2009/140, 2009 O.J. (L 337) 37 (EC).

66. MARTINSSON ET AL., *supra* note 54, at 28.

67. *Id.*

68. DR. MARNIX DEKKER & CHRISTOFFER KARSBURG, EUR. NETWORK & INFO. SEC. AGENCY, TECHNICAL GUIDELINE ON INCIDENT REPORTING TECHNICAL GUIDANCE ON THE INCIDENT REPORTING IN ARTICLE 13A 5 (Oct. 24, 2014), *available at*

Framework Directive essentially focuses on breaches that effect the functionality or continuity of the network or service. In addition, the provision specifically addresses breaches related to an electronic communication network or service. This implies that data breaches are not governed under the Framework Directive.

Furthermore, notification only needs to be provided for breaches with a "significant impact" on the operations of the network or services. There is no clear definition of what the term "significant impact" constitutes; as noted in the above paragraph, the focus of breaches under Article 13(a)(3) is the functionality or availability of the network or service. This implies that the assessment of a breach's significance is determined by taking into account the length and coverage of the interruption with respect to the functionality or availability of the infrastructure or service. A relevant question to ask would be "how long is the functionality or availability of the network or service interrupted? And, what is the coverage of such interruption, in terms of user-base or geographical scope?"

Primarily, the assessment of a significant impact lies in the hands of the organization. The difficulty is that "if a firm controls whether disclosure will occur, it has the ability not to" disclose such a breach.[69] However, the National Regulatory Authorities (NRAs) are entrusted with setting the specific criteria for making such decision. In addition, many Member States provide the possibility for customers or the media to directly report such breaches to the authorities.[70] This gives a platform for the NRAs to assess whether a breach should have been reported despite an organizations decision not to do so. Although there is no EU level criteria for assessing "significant impact," the European Network and Information Security Agency (ENISA) has provided some guidelines regarding the annual summary reporting from the NRAs to the European Commission (EC) about security incidents that have had "significant impact." Accordingly, an incident is considered to have a significant impact if the incident:

> (a) Lasts more than an hour, and the percentage of users affected is more than 15%; or
>
> (b) Lasts more than 2 hours, and the percentage of users affected is more than 10%; or

---

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/technical-guideline-on-incident-reporting/at_download/fullReport.

69. Schwartz & Janger, *supra* note 9, at 931.

70. EUR. NETWORK & INFO. SEC. AGENCY, ANALYSIS OF MEMBER STATES' POLICIES AND REGULATIONS POLICY RECOMMENDATIONS 76 (2009), *available at* http://www.enisa.europa.eu/publications/archive/analysis-of-policies-and-recommendations/at_download/fullReport.

> (c) Lasts more than 4 hours, and the percentage of users affected is more than 5%; or
>
> (d) Lasts more than 6 hours, and the percentage of users affected is more than 2%; or
>
> (e) Lasts more than 8 hours, and the percentage of users affected is more than 1%.[71]

Although the report addresses the notification by NRAs to the EC, it does provide helpful guidance on the concept of "significant impact." However, Member States might have different criteria. For example, in Switzerland, an incident is considered to have significant impact if it affects 50,000 or more people and lasts for more than five hours whereas in Norway, similar incident affecting 10,000 subscribers or a "geographical area larger than a municipality" has to be reported.[72] Once a security breach that is considered to fulfill the "significant impact" requirement occurs, organizations are required to notify the NRAs. Such notification is believed to be a very valuable source of information, enabling the authorities to identify problems and develop adequate regulatory measures for outage prevention.[73] In some cases, the NRAs might notify the public of such a breach or might ask the organizations to do so.[74] This is mainly when the authorities believe that such disclosure of the breach is in the interest of the public. Although the Directive does not specifically address the circumstances for such disclosure, such decision need to balance the interest of the public against the reputational harm to the entities. Such notification might be justified, for example, when the breach would cause significant damage to customers.

The breach notification requirement under the Framework Directive does not involve the notification of individuals. Furthermore, the Directive does not provide a detailed framework for the breach notification in terms of the timeframe, content and procedure. These aspects of the breach are addressed by the domestic legislation of the Member States and there is significant difference among them – ranging from a few hours after the breach to up to a few days.[75] For instance, in Spain providers are required to provide a preliminary report within the following two hours after the disruption and a thorough report within 10 days.[76] Therefore, organizations are required to adhere to such specific national procedures of notification. E-mail communications or call ser-

---

71. DEKKER & KARSBURG, *supra* note 69, at 11.

72. ANALYSIS OF MEMBER STATES' POLICIES AND REGULATIONS POLICY RECOMMENDATIONS, *supra* note 71, at 75.

73. *Impact Assessment*, *supra* note 28.

74. Directive 2009/140, art. 13a (3), 2009 O.J. (L 337) 37, 54 (EC).

75. DEKKER ET AL., CYBER INCIDENT REPORTING IN THE EU, *supra* note 26.

76. ANALYSIS OF MEMBER STATES' POLICIES AND REGULATIONS POLICY RECOMMENDATIONS, *supra* note 70, at 77.

vices (particularly when the breach is reported by customers or media) are often preferred channels in many Member States. In most cases, the content of the notification includes details of the breach, its significance, and incident mitigation plans and measures.[77]

The ePrivacy Directive 2002/58 and its Amending Directive 2009/136/EC

Article 4(2) of the e-Privacy Directive provides that:

> In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.[78]

Article 4(3) of the amending Directive 2009/136/EC further states that: "In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority."[79]

Subject matter of the ePrivacy Directive and the breach notification requirement

The ePrivacy Directive applies to providers of publicly available "electronic communications services" as provided in the Framework Directive and explained in Section 3.1.1. The main point of departure from the above discussion is that the ePrivacy Directive applies only to actors which process personal data[80] in connection with the provision of publicly available electronic communication services.[81] This implies that entities providing infrastructures or networks but do not have their own

77. DEKKER ET AL., CYBER INCIDENT REPORTING IN THE EU, *supra* note 26.

78. Directive 2009/136, art. 4(2), (4), 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, 2009 O.J. (L 337) 1, 22 (EC) [hereinafter *Revised ePrivacy Directive*].

79. *Id*.

80. Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) 31 (EC) (Data Protection Directive). This Directive defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[.]" *Id*.

81. Directive 2002/58, art. 3(1), 2002 O.J. (L 201) 37 (EC).

customers are not covered under this Directive. Another point of departure is that unlike the Framework Directive where notification is only required to be made to the national authorities and sometimes to the public, under the ePrivacy Directive, the providers are obliged to notify personal data breaches to the competent national authorities, and in certain cases also to the subscribers and individuals concerned. Furthermore, the ePrivacy Directive covers two different kinds of notifications i.e. the notification of particular risk of breach of network to subscribers as well as the notification of actual personal data breaches to the national authorities, to the subscribers, and individuals. However, the relevant security risks here are similar to that of the Framework Directive and include risks that affect the *functionally or availability* of the network or services.

It is important to note the notification of personal data breaches under the ePrivacy Directive are replaced by the Regulation 611/2013. This means, commencing from the date where Regulation 611/2013 enters into force,[82] only the notification of particular risk network breach to subscribers is regulated under the ePrivacy Directive. So the breach notification requirements discussed in this section pertain only to the notification of risk of breach of network to subscribers. Such an obligation is related with the obligation under Article 4(1), which requires organizations to take the appropriate technical and organizational measures to safeguard the security of its services taking into account the risks presented. This implies that the law requires the service providers to identify risks that affect the security of the network proactively and notify the existence of "particular risks" to subscribers. One could ask whether the subscriber notification is only limited to the "risk of breach of network," not to the actual breach of network. In fact, actual breaches affecting the security of the network would be reported to the NRAs under the Framework Directive so far as they have a "significant impact" on the operation of networks or services. Yet, the Framework Directive does not require notification to subscribers unless the national authorities notify or cause to notify the public for public interest reasons. So if the network breach does not affect personal data, the provider is not required to notify subscribers of the actual breach under the ePrivacy Directive. This might be intentional given that the rationale for notifying the risk of breach of a network is to take measures to mitigate the harms of the risk to the subscriber. A closer look at Article 4(2) of the Directive shows that the focus of such notification of the risk is to mitigate, for example the financial impacts of the service interruption on the subscriber. Once the breach actually happens, the rationale for

82. Although the Regulation was passed on 24 June 2013, it became operative after two months on 25 August 2013. *See* Commission Regulation 611/2013, art. 7, 2013 O.J. (L 173) 2, 4 (EU).

such notification seems to dissipate or at least become insignificant. Entities could still notify the subscriber regarding such breaches. Although the law is silent on whether all kinds of security risk should be notified, the term "particular risks" within that article seems to imply certain level of significance, which will be a matter left to the NRAs to determine.

Overall, providers of electronic communication services that operate their own public communications network are required to notify for "particular risk" of security of network to subscribers under the ePrivacy Directive and actual breaches of networks with "significant impact" on the operations of the network or services to the NRAs according to the Framework Directive. Whereas providers of electronic communications services that depend on the infrastructure of third parties need to put in place measures that allow them to comply with such requirements regarding the notification of a "particular risk." Article 1 of the ePrivacy Directive emphasizes the need for such service providers to work in conjunction with the provider of the public communications network with regards to the identification of such risk affecting network security and notification thereof. This could often be done through contractual agreements where the infrastructure provider informs the service provider of any security breach or risk. The provision does not mention any timeframe when such notification should be made. However, it should be noted that such notification is aimed at enabling the subscriber to take appropriate measures to avoid or mitigate the consequences of the risk of the breach. Therefore, one could say that the notification of the risks should be made as soon as possible from the time the provider becomes aware of the existence of such risk. Regarding the format and content of notification, Article 4(4) of the ePrivacy Directive provides that the NRAs may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify of a breach and the format and manner in which the notification is to be made.

Apart from notification of a breach under the ePrivacy Directive, providers are also required to "maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken" in a manner that "enable the competent national authorities to verify compliance" with the notification requirements.[83] However, the inventory should only contain "information necessary for this purpose[,]"[84] meaning that it should not, to the extent possible, contain any personal data in order to avoid another potential source of vulnerabilities. Compliance with such obligation could be relevant during enforcement actions by the NRAs and in determining the

83. Directive 2009/136, art. 4(4) ¶ 2, 2009 O.J. (L 337) 1, 22 (EC).

84. *Id.*

size of monetary penalties to be imposed.

Regulation 611/2013

Subject Matter of the Regulation 611/2013 and the Breach Notification Requirement

As briefly noted above, this Regulation covers the notification of personal data breaches previously regulated under the ePrivacy Directive. The Commission recognizes that the different implementation of the breach notification requirements within the ePrivacy Directive creates significant legal uncertainty, along with more complex and considerable "administrative costs for providers operating cross-border."[85] Therefore, the adoption of the Regulation 611/2013 aims at harmonizing such requirements.[86]

The application of the Regulation is limited to the notification of personal data breaches by providers of publicly available electronic communications services as discussed in Section 3.1.1.[87] This means notifications regarding "particular risk" of a breach of the security of the network to subscribers are still dealt under the ePrivacy Directive and the national implementations.[88]

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 Union."[89] Having an EU level definition of personal data breach is expected to harmonize breach notification requirements across the community although differences still exists based on the definition of what constitutes personal data. Meanwhile, when the proposed GDPR hits the statute shelf, it is expected to contribute to addressing such differences, as it will apply uniformly

85. *Id.*

86. Commission Regulation 611/2013, rec. 4, 2013 O.J. (L 173) 2, 2 (EU). In the European legal framework a Directive has to be transposed into national law for its application whereas a Regulation becomes binding on Member States without the need to transpose it into national law. Although the harmonization introduced by the Regulation is a move in the right direction, providers of electronic communication services experiencing a network breach that affects personal data have to deal with the national implementations of Member States in reporting breaches under the Framework Directive and are required to comply with the rules under the Regulation 611/2013. Furthermore, such providers are under obligation to notify their subscribers' risks of security of the network under the ePrivacy Directive. Given the disparities in the national implementation of Article 4 of the ePrivacy Directive, compliance will likely create significant challenge for organizations. *Id*.

87. *Id*. art. 1, at 2.

88. *Id*. art. 2(5), at 5.

89. *Id*. at 2.

across all Member States.

The Regulation 611/2013 applies only to breaches that affect the "personal data" of individuals. Article 2(a) of the Data Protection Directive defines personal data as "any information relating to an identified or identifiable natural person."[90] Identification involves "describe[ing] a person in such a way that he or she is distinguishable from all other persons and recognizable [sic] as an individual."[91] Such identification of the individual could happen directly from the information being processed such as the full name of the person or indirectly from information related to the physical, economic, or social identity of that particular individual. However, for the Directive to be applicable it is not required that the person be identified, meaning that a mere possibility to associate certain information to a particular individual is sufficient. Unlike the Directive, the proposed GDPR broadens the definition of "personal data" to cover device identifiers, IP addresses and location data.[92]

Notification to National Regulatory Authorities (NRAs)

Article 2(2) of the Regulation provides that the provider "shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible."[93]

Unlike the other breach notification rules that require certain degree of significance, the requirement under the Regulation is applicable to any breach regardless of its significance. Therefore, all personal data breaches should be brought to the attention of the relevant authorities within 24 hours of detection. A breach is deemed to be detected "when the provider has acquired '*sufficient awareness'* that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation."[94] The question is: when is the provider's awareness deemed to be "sufficient." According to Recital 8 of the Regulation, neither a simple suspicion nor a simple detection of an incident is sufficient. Of particular relevance in such assessment is the availability of the information referred to in Annex I, which lists the content of the information to be provid-

---

90. EUR. UNION AGENCY FOR FUNDAMENTAL RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 36 (Apr. 2014), *available at* http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

91. *Id*. at 39.

92. *See GDPR*, *supra* note 8, ¶24, at 21.

93. Commission Regulation 611/2013, art. 2(2), 2013 O.J. (L 173) 2, 4 (EU).

94. *Id*. art. 2(2) ¶3, at 4.

ed.[95] Thus, if the organization is in a position to explain the breach well enough in terms of the kind of the breach (whether it is loss or theft/copying of personal data), the time the breach occurred, and the type of data affected, it could be considered as sufficient. Furthermore, the technical and organizational measures in place to detect a breach play a significant role in assessing the sufficiency of the awareness. The less compliant an organization is with its data security obligations, the less likely such phrase would be interpreted in its favor against delay. In other words, if an organization fails to take appropriate security measures such as keeping access logs to detect unauthorized access, it will not be able to justify its delay for lack of "sufficient awareness" in detecting the breach (unauthorized access).

Timeframe for notification – In principle the notification should be made within 24 hours, where feasible. Although the inclusion of the term "where feasible" offers a space for flexibility, it could lead to a situation where different national competent authority could define the term differently making 24 hour disclosure infeasible. However, such term should be interpreted in light of the three phases of notification recognized under the Regulation. First, an initial notification should be made within 24 hours. During the initial phase, the provider "determines whether the detected event is indeed a personal data breach," the circumstances of the breach and its estimated severity and reports it to the national authorities within 24 hours.[96] This is followed by a detailed notification in a standardized format as soon as possible and at least within three days of the initial notification. This will provide further details of the breach including measures taken to mitigate the breach.[97] However, if, despite all the necessary efforts, the provider is unable to provide all information within the three-day period, it has to do so at a later time accompanied by a "reasoned justification for the late notification of the remaining information."[98]

Among other things, the notification to the competent authorities should contain the name of the provider, a contact point within the organization, circumstances of the personal data breach, date and time of detection of the incident, "nature and content of the personal data concerned" and "the technical and organizational measures taken by the provider" to correct the breach.[99] Providers could use a variety of communication channels to notify the competent authority, including

---

95. *Id*. Annex I, at 7.

96. EUR. NETWORK & INFO. SEC. AGENCY, RECOMMENDATIONS ON TECHNICAL IMPLEMENTATION GUIDELINES OF ARTICLE 4, at 22 (Barbara Daskala & Slawomir Gorniak eds., Apr. 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech/at_download/fullReport.

97. Commission Regulation 611/2013, Annex 1 §2, 2013 O.J. (L 173) 2, 7 (EU).

98. *Id*. art. 2(3) ¶2, at 4.

99. *Id*. Annex I §2, at 7.

emails and phone calls. One essential aspect of breach notifications requirements is the principle of "dissociation" where the communication of the breach should contain information regarding the breach as its core and only content.[100] For example, if providers are required to notify the authorities regarding processing of personal data, the notification of breaches should not be communicated in the same e-mail.

Notification to subscribers or individuals

Article 3(1) provides that "when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall, in addition to the notification referred to in Article 2, also notify the subscriber or individual of the breach."[101]

An important aspect of Regulation 611/2013 is that it covers breaches affecting not only natural persons but also legal persons. In this regard, it is important to distinguish between the "subscriber" and "individual" user. Such distinction is important because the subscriber, which can be either a legal person or natural person, may not always be the same person as the user. For example, parents can have a subscription to value added services such as locating the mobile phone of their children in which case the parents are the subscribers and their children are the individual users. Article 3(1) of the Regulation requires that both the subscriber and the individual user be notified when personal data breach is likely to affect the privacy of the subscriber or the individual. Nonetheless, in some cases, such notification to the individual could prove to be difficult because the provider might lack a direct contract or contact information. If the subscriber is only a legal person such as a company, it is less likely that the breach would constitute personal data breach.

Providers are required to notify affected individual or subscribers when the breach "is likely to adversely affect" their personal data or their privacy rights. As noted above, this aims at balancing the interest of the business in terms of "fatigue of notifications" and the privacy rights of the individuals. Article 3(2) of the Regulation lists three factors that should be used to determine whether a breach is "likely to adversely affect" the subscriber or privacy rights of the individuals. These are: (a) the nature and content of data concerned; (b) the likely consequences of the personal data breach for the subscriber or individual concerned; and (c) the circumstances of the personal data breach.[102]

Breaches affecting certain categories of personal data are considered to fulfill such requirement. Examples are breaches affecting finan-

100. *Id*. at 3.
101. *Id*. at 5.
102. *Id*. art. 3(2), at 5.

cial information such as credit card data, special categories of data,[103] "e-mail data, location data, internet log files, web browsing histories and itemized [*sic*] call lists".[104] This is because such breaches might result in "identity theft[,] fraud, physical harm,…[significant] humiliation or damage to reputation."[105] This implies that the assessment is not limited only to "breaches that result in economic loss, but also breaches that may cause immaterial damages, such as any moral and reputational damages."[106] The Article 29 Working Party (Working Party), a group composed of national Data Protection Authorities, underlines the need to consider secondary effects of the breaches such as the time spent in attempts to rectify the breach and the extent of distress suffered.[107] In addition, the reference to the term "likely" implies that the mere likelihood that the breach will adversely affect the individual is sufficient, meaning that an actual adverse effect is not necessary.

Based on the three factors under Article 3(2), ENISA has developed the following, *albeit* complex, methodology for assessing the severity of breaches on the privacy rights of individuals.[108]

$$SE= DPC \times EI + CB$$

SE stands for severity of the breach.[109] DCP stands for *Data Processing Context*, which "addresses the type of the breached data, together with a number of factors linked to the overall context of processing."[110] A score of 1-4 is assigned to the following four categories of data in their order: *simple, behavioral, financial, and sensitive*. EI stands for *Ease of Identification*, which addresses "how easily the identity of the individuals can be deduced from the data involved in the breach."[111] Four levels of EI are identified (negligible, limited, significant and maximum) with a linear increase in score ranging from 0.25–1

---

103. Council Directive 95/46, art. 8, 1995 O.J. (L 281) 31 (EC). This Directive defines special categories of personal data as any information "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" and data relating to offences, criminal convictions or security measures, or to administrative sanctions or judgments in civil cases. *Id*.

104. Commission Regulation 611/2013, 2013 O.J. (L 173) 2, 3 (EU).

105. *Id*. art. 3(2)(b), at 5.

106. EUR. CONSUMER ORG., *supra* note 38, at 4.

107. Eur. Union Article 29 Working Party, Opinion 03/2014 on Personal Data Breach Notification (Mar. 25, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

108. RECOMMENDATIONS FOR A METHODOLOGY OF THE ASSESSMENT OF SEVERITY OF PERSONAL DATA BREACHES, *supra* note 29, at 3.

109. *Id.* at 6.

110. *Id.* at 3.

111. *Id.*

including 0.5, and 0.75.[112] CB stands for *Circumstances of Breach*, which "addresses the specific circumstances of the breach including the type of the breach… [and] any involved malicious intent."[113] Depending on the particular situation, CB could be assigned values of 0, 0.25 or 0.5. Ultimately, the SE result belongs to a certain range of values, which corresponds to one of the four severity levels: low (SE score of <2),[114] medium ($2 \leq SE < 3$),[115] high ($3 \leq SE < 4$)[116] and very high ($4 \leq SE$).[117] Clearly, the use of the above method will not be an easy exercise. However, it might be relevant for organizations, which already use quantitative scales in measuring the likelihoods and consequences of information security breaches. This methodology implicitly strengthens the proposal discussed in Section 4 for the integration of breach notification requirements into overall risk management framework and the security risk analysis in particular. Organizations who manage to address breach notification requirements in conjunction with security risk analysis would find it easier to use this methodology than others. The method above could also be used by national authorities in assessing whether the provider has to notify the individuals involved.

Overall, a cautious approach is recommended by the Working Party in assessing the adverse impact. More particularly, the Working Party recommends that "where there is doubt…regarding… the likelihood of adverse effects… [organizations] should err on the side of caution and proceed with notification."[118] The question that follows is who must make the assessment of the adverse effects on the individual —the authorities or the provider. Primarily, it is the organizations' discretion to determine whether certain breach is likely to have an adverse effect on the privacy rights of the individuals. This sounds logical given the relevant facts and circumstances surrounding the breach are in possession

---

112. *Id.* at 18.

113. RECOMMENDATIONS FOR A METHODOLOGY OF THE ASSESSMENT OF SEVERITY OF PERSONAL DATA BREACHES, *supra* note 29, at 3.

114. *Id.* at 6. A low SE score means "individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.)." *Id.*

115. *Id.* A medium SE score means "individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.)." *Id.*

116. *Id.* A high SE score means "individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.)" *Id.*

117. *Id.* A very high SE score means "individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.)" *Id.*

118. Eur. Union Article 29 Working Party, *supra* note 107.

of the organization. However, a company that suffers a data security breach may be hesitant to disclose information about this event and individuals might not get the chance to take remedial measures. To remedy this problem, there are suggestions for anonymous ways of reporting certain kinds of breaches in order to help individuals mitigate the resulting harms.[119]

Another question is whether the notification to individuals is limited to those affected or to all the customers of the organization. To the extent that such notices are intended to motivate individuals to take steps to mitigate the harms, one could argue that the notification should mainly target individuals affected. However, if there is a lingering risk for other customers, the organization should notify all of such risk. In fact, organizations might be required to notify customers of such risk under the ePrivacy Directive although it only mentions subscribers without mentioning individuals, meaning that under the ePrivacy Directive individuals will only be notified in their status as subscribers. In addition, the reference within Article 3(1) to "a subscriber or individual" makes it clear that notification should be provided when a data breach adversely affects even a single person's privacy.[120]

Exemption – Individuals do not need to be notified in some circumstances, specifically, when providers manage to demonstrate that the data affected by the breach was rendered *unintelligible*.[121] According to Article 4(2) of the Regulation, a data is considered to be unintelligible where: "(a) it has been securely encrypted with a standardized algorithm" or "replaced by its hashed value calculated with a standardized cryptographic keyed hash function;" (b) "the key used to decrypt or to hash the data has not been compromised in any security breach;" and (c) it has been demonstrated that the key used to decrypt or hash the data "cannot be ascertained by available technological means by any person who is not authorized to access the key."[122] The main rationale behind such exception is that if a data was made initially unintelligible, the residual privacy risks of the breach are considered to be minimal – not likely "to adversely affect" the personal data or privacy rights of individuals.[123] Meanwhile, the exception relating to technological protection measures is not an automatic safe harbor and needs to be approved by the competent authority. There are three approaches to providing safe harbor to such obligation: *an exemption, a rebuttable presumption*, *and factor-based analysis*.[124] The EU legislator seems to prefer the fac-

119. Schwartz & Janger, *supra* note 9.

120. Eur. Union Article 29 Working Party, *supra* note 107.

121. Commission Regulation 611/2013, art. 4(1), 2013 O.J. (L 173) 2, 5 (EU).

122. *Id.* art. 4(2)(a), at 5.

123. Eur. Union Article 29 Working Party, *supra* note 107 at 1.

124. *Exemptions* provide a general safe harbour for notification if personal data has been acquired in unintelligible form. *Rebuttable presumptions* create a presumption that

tor-based analysis where the implementation of such measures is one factor in demonstrating to the regulatory authorities that the rights of the data subject are not affected.

In addition, organizations have to still notify the NRAs regardless of such measures. In some cases, the organizations might even be required to notify individuals of the breach even if the data is sufficiently encrypted. This is because, for example, in the absence of adequate backups, a loss or alteration of encrypted data can still negatively affect data subjects.[125] This is important because encryptions cannot prevent loss of data. Thus, for the purposes of the exemptions from notification, it is important to make a distinction among the three kinds of personal data breaches: "availability breach" —which refers to the "accidental or unlawful destruction of data[;]" "integrity breach"—which refers to "alteration of personal data," and "confidentiality breach" that relates to "unauthorized disclosure of, or access to, personal data."[126] This implies that the exception regarding unintelligible data does not prevent "availability breach" and might not exempt the entity from notifying the individual. Although one could argue that breaches affecting *availability* might not in the strict legal sense affect the *privacy rights* of individuals, Article 3(1) of the Regulation refers to "*personal data* or privacy of a subscriber or individual."[127] This implies that breaches affecting availability might still adversely affect the personal data of subscribers or individuals.

Timeframe for notification – According to Article 3(3), "the notification to the subscriber or individual shall be made without *undue delay* after the detection of the personal data breach."[128] Furthermore, the "[n]otification… shall not be dependent on the notification to…national authorities."[129] This implies, for example that an organization should not try to prioritize notification to the authorities over subscribers or individuals. Given the aim of such notification is to avoid or mitigate the consequences of the breach; the notification should be given immediately or in such time as to enable the subscriber or individual to mitigate the adverse effects of the breach. In light of such rationale, it is argued that the term without *undue delay* involves a shorter interval than the notification to the authority, which is within 24 hours after detec-

---

no risk exists if unintelligible data is acquired which can be rebutted if evidence is found to the contrary. In *factor-based analysis,* unintelligibility is merely a factor accounted for in determining whether harm will reasonably result from the breach. *See* Burdon et al., *supra* note 43, at 528-530.

125. Eur. Union Article 29 Working Party, *supra* note 107, at 1.

126. *Id*. at 2.

127. Commission Regulation 611/2013, art. 3(1), 2013 O.J. (L 173) 2, 5 (EU). Emphasis added.

128. *Id*. art. 3(3), at 5.

129. *Id*.

tion of the breach.[130] However, there is a potential for deviating from the "undue delay" requirement. Such circumstances, for example, include "where the notification to the subscriber or individual may put at risk the proper investigation of the personal data breach."[131] It seems that investigations related to other crimes other than the personal data breach itself might also justify the delay. In all other cases, such assessment has to be made on case-by-case basis by the competent national authorities.[132]

Content – The Regulation, under Article 3(4), requires the notification to subscribers or individuals to describe at least the name of the provider, the contact points within the provider where more information can be obtained, description of the causes, timing and the circumstances of the breach, nature and content of the personal data breached and the likely consequences to the subscriber or individual, and measures taken by the provider to address the breach and recommended measures to mitigate the adverse effects.[133] The challenge with information provision rules such as this has always been to strike the balance between the information provided and the usability of the information by the recipient. A study shows that 61% of consumers have problems understanding the notification and 72% claiming that the "notification did not increase their understanding about the data breach."[134] Therefore, Article 3(4) emphasizes the importance of providing clear and easily understandable information outlining the risks and recommended actions without technical terms. Providing clear contact point for the competent authority, of the provider as well as of consumer organizations would also be important. Understandability of the notification would also imply "that individuals whose data has been breached receive the notification in their own language."[135] However, the challenge remains for operators that trade cross-border. For example, an operator providing services across the EU that sustains a personal data breach might need to issue the notification letter with more than 20 different languages. There might also be language issues when the breach affects users residing in a Member State where more than one language is spoken. Furthermore, in order to avoid confusion, the notification should not be allowed to contain advertisements or offers for other services, such as identity theft insurance.[136]

---

130. Barcelo & Traung, *supra* note 122, at 96.

131. Commission Regulation 611/2013, art. 3(5) 2013 O.J. (L 173) 2, 3 (EU).

132. *Id*. at 3.

133. *Id*. art. 3(4), Annex II, at 5, 8.

134. PONEMON INSTITUTE, 2012 CONSUMER STUDY ON DATA BREACH NOTIFICATION, *supra* note 3, at 4, 5, 10.

135. EUR. CONSUMER ORG., *supra* note 16, at 11.

136. Commission Regulation 611/2013, art. 3(4) & Annex II, 2013 O.J. (L 173) 2, 5, 8 (EU).

Means of notification – In principle, the provider can choose any communication means taking into account the state of the art that ensures a prompt receipt of the notification.[137] This will also depend on the contact information in the possession of the company. Therefore, post addresses as well as email communications could be used to inform the individuals or subscribers. However, research shows that consumers do not pay sufficient attention to the notices they receive.[138] Similarly, 49% of respondents to a survey thought that their breach notice was either junk mail (36%) or spam (13%).[139] Therefore, organizations should endeavor to get the full attention of the individual users, for example by using a clearly headed letter of notification and consider a combination of different notification channels. In cases where the provider does not have the contact details of the affected individuals, the provider should take reasonable steps to ensure that all affected individuals are made aware of the breach. Such efforts might include "requesting support from other providers or controllers in possession of the contact details."[140] If, having made reasonable efforts, the provider is unable to identify the individuals within the notification timeframe notification may be made through advertisements in national or regional newspapers. However, such notification via mass media does not seem to be mandatory although such discretion seems to be applicable only where there is no direct contractual relationship between the provider and the end user.[141] What is unclear is the extent of such discretion, if at all, where there is direct contractual relationship between the provider and the end user but the provider claims not having the contact details of the individual. However, given that contact details are part of most contractual relationships in providing a service, such situation is less likely to occur.

3.2. BREACH NOTIFICATION BY 'DATA CONTROLLERS' OR 'DATA PROCESSORS': DRAFT GDPR

Subject matter of the draft GDPR and the breach notification requirement

There have been calls for the introduction of breach notification requirements beyond the telecom sector.[142] This is because breaches oc-

137. *Id*. art. 3(6), at 5.

138. PONEMON INSTITUTE, 2012 CONSUMER STUDY ON DATA BREACH NOTIFICATION, *supra* note 32, at 1.

139. PONEMON INSTITUTE, 2012 CONSUMER STUDY ON DATA BREACH NOTIFICATION, *supra* note 32, at 8.

140. Eur. Union Article 29 Working Party, *supra* note 107, at 13.

141. Commission Regulation 611/2013, art. 3(7), 2013 O.J. (L 173) 2, 5 (EU).

142. EUR. CONSUMER ORG., *supra* note 16, at 3.

curring in the hands of non-telecom actors might be as harmful for consumers as the breaches sustained by telecom providers.[143] The proposed GDPR seems to heed to such quest and extends the personal data breach notifications beyond the electronic communications sector to controllers and, to certain extent, processors. Given that the adoption of EU legislation requires an agreement between the European Parliament and the European Council on the proposal placed by the Commission,[144] at present there are three different drafts of the Regulation that reflect the position of these organs *i.e.*, the initial Commission draft,[145] the draft from the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (hereinafter the *LIBE draft*)[146] and a preliminary draft from the European Council (hereinafter the *Council draft*).[147] The main differences with respect to the breach notification in these drafts will be highlighted when relevant. Any reference to the proposed Regulation is to the initial Commission draft.

It is important to note that the breach notification requirement under Regulation 611/2013 is essentially similar to the proposed GDPR. This is not incidental. It originates from the legislator's intent of harmonizing notification requirements regarding personal data across sectors.[148] Thus, the discussions regarding the types of breaches covered, when a breach is considered to occur, the content and procedures of notification under Section 3.1.3 are more or less relevant to this section. Another reason to focus on the Regulation 611/2013 is because it is currently in force whereas the GDPR is in state of fluidity. This section only focuses on the salient features of the proposed Regulation. The first point of departure in the proposed Regulation is that it applies to "data controller" and "data processor."

Data controller – is defined as "…the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data".[149] For an actor to be considered as a controller, the follow-

143. *Id*.

144. Consolidated Version of the Treaty on the Functioning of the European Union art. 289(1), 2012 O.J. (C 326) 1, 172 (EU).

145. *GDPR*, *supra* note 8.

146. *LIBE Draft*, *supra* note 8.

147. *Council of the Eur. Union, 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* (Dec. 16, 2013) [hereinafter *Council Draft*], *available at* http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT.

148. *See, e.g.*, Commission Regulation 611/2013, 2013 O.J. (L 173) 2, 3 (EU) (referring that the Regulation is fully consistent with the proposed measure under the draft Data Protection Regulation).

149. *GDPR*, *supra* note 8, art. 4(5), at 41.

ing requirements are essential. First, a controller can be a natural or legal person, public authority, agency or any other body. This implies that the form or nature of the entity is irrelevant. Second, the controller determines the purposes, conditions and means of the processing. This is a crucial element and one of the main factors in assessing this aspect is the level of influence and of the details that someone have in determining "why" (i.e. purposes) and "how" (i.e. means) certain processing activities should be performed. In establishing controllership, it has to be noted that the factual circumstance is a more relevant factor than a "fine tune" designation based on contract or law.[150] This means, for example, a clear contractual provision designating a party not as a controller is not relevant if all the other circumstances indicate otherwise. Third, the decision regarding the "purpose and means" can be made jointly with others – where several legally separate entities who together or *jointly with others* process data for a shared purpose.

Data processor – is defined as "any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."[151] To act as a processor a natural being or an entity must fulfill the following two elements. First, it must be a *legally separate subject or legal entity* with respect to the controller. Second, it must process *personal data on behalf of the controller*. This implies that decisions on the "purpose" and "essential means" should be made by the controller.[152] The concept of "essential means" gives a "margin of maneuver" for processors such as cloud providers, to determine technical and organizational questions without being considered "controllers". Thus, often cloud providers are considered data processors so far as the provider adheres to the controllers instructions and does not process the data for its own purposes, for example for advertising.[153]

Territorial scope of the draft Regulation

Not all controllers and processors of personal data are required to comply with the breach notification requirements. The Regulation provides three legal grounds for its application:[154]

(A) Processing of personal data occurs in the context of the activities of the controller or processor established within the EU.[155] This means that for the Regulation to apply two conditions must be fulfilled. These are: (a) the controller or processor has to have an establishment in one of the EU Member States, and (b) the processing should occur in

150. Eur. Union Article 29 Working Party, *supra* note 107, at 8.
151. *GDPR*, *supra* note 8, art. 4(6), at 42.
152. Eur. Union Article 29 Working Party, *supra* note 107, at 15.
153. *Id*.
154. *GDPR*, *supra* note 8, art. 3 at 41.
155. *Id*. art. 3(1), at 41.

the context of the activities of the controller or processor in that Member States. Hence, the mere fact a controller or processor has an establishment in Member State is not sufficient to apply the Regulation. Rather the processing has to relate to the activities of the controller or processor in such Member State.[156]

(B) Processing of personal data of EU residents by a controller or processor established outside the EU where the processing activities are related to the offering of goods or services.[157] Essentially, this requirement applies when a non-EU trader collects personal data through selling goods or services to EU residents. However, it is not necessary that an actual sale of goods or services occurs in order for the Regulation to apply. It is sufficient that the trader is processing personal data while envisaging the offering of goods or services to data subjects residing in one or more Member States in the Union.[158] For example, if a consumer residing in the EU contacts a trader established outside the EEA and thereby the trader becomes in possession of the contact details of the consumer, the trader might have to comply with the Regulation even if the consumer did not purchase the goods or services provided the traded has envisaged offering goods or services in one or more Member States in the Union.

(C) Processing of personal data of EU residents by a controller or processor established outside the EU where the processing activities are related to the "monitoring of the behavior of data subjects."[159] This requirement applies regardless of the commercial nature of the activity so far as the controller monitors the behavior of a data subject residing in the EU for example by storing activity logs of website users through the use of cookies.

It is not the aim of this article to go into a detailed discussion regarding the scope of the Regulation, which is one of the controversial areas of the draft Regulation. But it has to be noted that this provision is broad enough to bring all providers of Internet services including but

---

156. The recent Google decision from the Court of Justice of the European Union (CJEU) further elaborates the concept of 'context of activities of an establishment in a Member State'. The CJEU highlights that "In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable." *See* Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos 2014 E.C.R., ¶55, *available at* http://curia.europa.eu/juris/liste.jsf?num=C-131/12 (not yet published in reporter).

157. *GDPR*, *supra* note 8, art. 3(2(a)) at 41.

158. *GDPR*, *supra* note 8, at 20.

159. *GDPR*, *supra* note 8, art. 3(2(b)) at 41.

not limited to websites, social networks, and app providers under the scope of the Regulation even at the slightest interaction with data subjects residing in the Union. Furthermore, the Regulation is primarily concerned with the processing of personal data "wholly or partly by automatic means."[160] The use of the term "wholly or partly" implies that an automated operation that involves some manual use of personal data is within the realm of the Regulation. In addition, the draft Regulation is also applicable to *non-automated processing which forms part of a filing system or are intended to form part of a filing system* such as specially structured paper file.[161] Essentially, the draft Regulation applies whenever personal data is processed, either automatically or not, barring certain exceptions.[162]

Notification by data controllers to Data Protection Authorities (DPAs)

This part highlights the main differences in the notification of personal data breaches to the relevant authorities in comparison with the discussion of Regulation 611/2013.

First, although the initial Commission and the Council draft were similar to the definition of "personal data breach" as in the 611/2013 Regulation, the LIBE draft leaves out the term "security breach leading…"[163] This seems to be an attempt to focus on the personal data breach as an outcome by itself than "as an end result of security breaches."[164] This implies that for the Regulation to apply the personal data breach does not necessarily need to be a result of a security breach. One such instance could be misuse of access rights by authorized people such as employees where such misuse results in unauthorized disclosure of the data concerned.[165] Nonetheless, one could also put a similar argument regarding the Regulation 611/2013.

Second, the initial Commission draft and the Regulation 611/2013 require the notification of any personal data breaches, regardless of its

---

160. *GDPR*, *supra* note 8, art. 2(1), at 40.

161. *GDPR*, *supra* note 8, art. 4(4), at 41. Article 4(4) defines 'filing system' as any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. *Id.*

162. *GDPR*, *supra* note 8, art. 3(2), at 41. These include: (1) in the course of an activity which falls outside the scope of Community law, for example, processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law; (2) by a natural person in the course of a purely personal or household activity. *Id*.

163. *LIBE Draft*, *supra* note 8, at art. 4(9).

164. W. Kuan Hon et al., *Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation* 37 (Tilburg Law Sch., Legal Studies Working Paper No. 7, 2014), *available at http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2405971_code599.pdf?abstractid=2405971&mirid=1.*

165. *Id*.

impact, to the competent authorities. However, the amendment from the Council limits the breaches to be notified to the DPAs only to data breaches that are likely to "severely" affect rights and freedoms of data subjects. In addition, the Council introduces an exception in notifying the authorities when notification to individuals is not required because of technological measures.[166] Some scholars argue that the "notification of personal data breaches to the DPAs may not be necessary when the rights and freedoms of data subjects are not likely to be affected."[167] However, the rationale behind the notification to the DPAs goes beyond the protection of rights and freedoms of individuals. On the one hand, such notification enables the authorities to identify patterns of breaches and learn where policy interventions and cooperation might be required. On the other hand, the notification to the authorities enables them to assess whether notification to individuals should take place. This ensures that the assessment of whether the rights of the data subjects are likely to be affected does not solely rest in the hands of the entities.[168] Moreover, such requirement would introduce unjustified discrimination between entities processing personal data in the electronic communications sector that have to notify any breaches to the authorities under the Regulation 611/2013 and others that have to notify only for data breaches that are likely to "severely" affect rights and freedoms of data subjects.

Third, unlike the initial draft from the Commission that would require notification to the DPAs "without undue delay and, where feasible, within 24 hours" after the controller becomes aware of the breach, the draft from LIBE requires notification without "undue delay" leaving out any reference to specific timeframe while the draft from the Council extends the time to 72 hours, where feasible.[169] Such changes have to do with the lobby following the release of the initial draft. In light of the short timeframes for notification, the fines were considered by many entities as too high and burdensome.[170] However, the proposed change in the LIBE's draft from the 24-hour time limit to "without undue delay" omitting any reference to a specific timeframe could lead to inconsistent approaches among different Member States. This is particularly true given that Article 21(1) of the proposed Regulation gives Member States the power to restrict through legislative measures certain rights and ob-

166. *Council Draft*, *supra* note 147, art. 31(1a), at 131.

167. Hon et al., *supra* note 164.

168. However, to facilitate this ex-post verification, the communication to the authorities ought to contain an explanation for not notifying the individuals.

169. *LIBE Draft*, *supra* note 8, art. 31(1), at 108; *see also Council Draft*, *supra* note 147, art. 31(1), at 127.

170. Luke Danagher, *An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?* 3 EUR. J.L. & TECH., no. 3, 2012, *available at* http://ejlt.org/article/view/171/260.

ligations laid down under specific provisions of the Regulation. And, Article 32, which lays down the breach notification obligation, is one provision, which could be subject to such restrictions. Although the scope of the power of the Member States would nevertheless need to meet certain conditions listed under Article 21(2), given the wider list of the conditions, different implementations of this provision is not unlikely. This might defeat the main rationale for of the Regulation itself, which is to bring uniformly applicable rules throughout the Community. Therefore, if the wording of the LIBE draft is something to go by, works are required from the Commission in avoiding different approach to what "without undue delay" means. However, this should not be taken to imply an extended period of notification. As we have seen above, the rationale behind the notification for individuals dictates that the term "without undue delay" should be understood as entailing notification of breaches immediately when the data controller has the information regarding the breach.

Furthermore, unlike the Regulation 611/2013, the draft GDPR does not include different phases of notification. The initial Commission draft allows organizations to notify the Regulatory authorities later than 24 hours upon reasoned justification. The LIBE draft completely avoids any reference to such issue whereas the Council draft allows reasoned justification after the 72 hours limit. The different phases of notification in the Regulation 611/2013 enable organization to notify regulators even though they do not have all the necessary information about the breach. However, the approach in the draft GDPR might discourage organizations from notifying unless they have all the necessary information, which might in turn endanger the privacy rights of individuals. In addition, Art 31(4a) of the LIBE draft introduces an obligation on DPAs to maintain a public register of the "types" of breaches. The main objective of such obligation is to enable the authorities verify compliance and use the data for further policy development purposes. The register can also be used to educate the public about the types and amounts of data breaches and "if the register identifies the controllers involved" it imposes a reputational cost through "naming and shaming."[171]

Obligation on 'processors' to alert controllers

According to Article 31(2) processors are required to inform and alert the controller of any personal data breach. The initial Commission draft requires this to happen "immediately" after the establishment of a personal data breach whereas the LIBE and the Council draft uses the term "without undue delay." The importance in such a change in tech-

171. Hon et al., *supra* note 164, at 38.

nology is not clear but given that both the Parliament and the Council are pushing to relax the timeframe for notification, "undue delay" seems to provide more leverage for processors than the term "immediately".

Notification to Individuals

Discussions in Section 3.1.3 regarding the notification of personal data breaches to individuals or subscribers are generally relevant for this Section. This part highlights the main differences in comparison to the discussions in Section 3.1.3.

First, the initial Commission draft requires notification of the individual data subjects when the breach is "likely to adversely affect the protection of *the personal data or privacy of the data subject*,"[172] which is similar to the wording under the Regulation 611/2013. Nevertheless, the LIBE draft uses the term "when the breach is likely to adversely affect *the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject*".[173] This further broadens the scope of the assessment beyond the privacy right of the individual and employs a very broad and unclear terminology of "legitimate interest." This gives a broader discretion to include other impacts on the individual within the assessment. For example, the inclusion of the time spent in attempts to rectify the breach and the extent of distress suffered would be more plausible within such terminology. On the other hand, the Council draft requires notification to the data subject "when the personal data breach is likely to severely affect the rights and freedoms of the data subject."[174] The Council draft does not also limit the effect of the personal data breach to the privacy rights of the individual but it employs a rather restrictive term "severely" as opposed to "adversely".[175]

Second, another deviation could also emerge with regard to the notification of individuals. Article 8 of the draft Regulation specifically dealing with child data is a new feature in the reform. Generally, a child is defined, under the initial Commission draft and the LIBE draft, "as any person below the age of 18 years."[176] The Council draft does not

172. *GDPR*, *supra* note 8, art. 32(1), at 61.

173. *LIBE Draft*, *supra* note 8, art. 32(1), at 110.

174. *Council Draft*, *supra* note 147, art. 32(1), at 130.

175. The Oxford online dictionary defines "adversely" as "unfavorably, harmfully" whereas "severely" as "in a manner, or to a degree, that is distressing or hard to bear." *Adversely*, OXFORD ONLINE DICTIONARY http://www.oxforddictionaries.com/us/definition/english/adversely (last visited Mar. 2, 2015); *Severely*, OXFORD ONLINE DICTIONARY, http://www.oxforddictionaries.com/us/definition/english/severely (last visited Mar. 2, 2015).

176. *GDPR*, *supra* note 8, art. 4(18), at 43; *see also LIBE Draft*, *supra* note 147, art. 4(18), at 67.

contain definition of a child per se but includes a reference to a person below the age of 13 under its Article 8(1).[177] Overall, Article 8(1) of all the three drafts requires the consent of parents or legal guardian in order to process personal data of a child below the age of 13 if the basis for the processing is based on the data subject's consent. This would imply that when a breach of personal data happens that affects the data of children below that age, the controller is required to notify the parents or legal guardian of the children affected in addition to the children themselves.

Third, unlike the Regulation 611/2013, which requires notification to subscribers in certain cases, which might include legal persons, the notification regime under the draft Regulation covers only natural persons. Furthermore, unlike Regulation 611/2013 that provides a detailed description regarding the exemptions for notifying the individual data subjects, the initial Commission draft and the LIBE draft adopt a very general approach without any reference to specific technological measures in rendering data unintelligible.[178] This might be because of the issues of technological neutrality in making specific reference to encryption or hashing within the Regulation 611/2013. However, the Council draft refers to encryption, or pseudonymization, as mechanisms that can be employed to render personal data unintelligible.[179] Given that encryption is one technique of pseudonymization,[180] the reference to both terms seems to be redundant. Although not specifically referenced in Article 32, the use of anonymization would also exempt the controller from notifying the data subjectsprovided the individual cannot be identified via the data. This flows from the general principle that, if data is rendered "non-personal" through anonymization the data protection rules do not apply.[181] Furthermore, the Council draft introduces further exceptions. Accordingly, the controller is not required to notify the data subject where: (a) It has "taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer likely to be severely affected;"[182] or (b) If notification "involves disproportionate effort, in particular owing to the number of cases involved" in which case the controller can resort to public communications or similar measures;[183] (c) If the notification "would adversely affect a substantial

177. *Council Draft*, *supra* note 147, art. 8(1), at 77.

178. *LIBE Draft*, *supra* note 8, art. 32(3), at 111.

179. *Council Draft*, *supra* note 147, art. 32(3)(a), at 131.

180. Eur. Union Article 29 Working Party, *supra* note 107, at 20.

181. Council Directive 95/46, ¶26, 1995 O.J. (L 281) 31 (EC); *see also GDPR supra* note 8, ¶23, at 23.

182. This might include for example if the controller is able to demonstrate that it has recovered a lost data without any unauthorized access or alteration. *GDPR supra* note 8, art. 32(3)(b), at 131; *Council Draft, supra* note 147, art. 32(3)(b), at 131.

183. *GDPR supra* note 8, art. 32(3)(c), at 131; *Council Draft*, *supra* note 147, art.

public interest."[184]

3.3. BREACH NOTIFICATION BY 'MARKET OPERATORS': THE NIS DIRECTIVE

The main objective of the proposed NIS Directive is to "ensure a high common level of network and information security (NIS)."[185] More precisely, the Directive aims to create "a level playing field for businesses across the EU and to avoid a weakest link" and thereby improve the Internet and the private networks and information systems, which are vital for the functioning of the European societies and economies.[186] A prominent feature in the Directive is the obligation for businesses providing critical services to report security incidents. The initial draft from the Commission has undergone some changes including some proposed amendments from the European Parliament's Committee on the Internal Market and Consumer Protection.[187]

Subject matter of the NIS Directive and the breach notification requirement

Article 14(2) of the initial Commission draft requires Member States to "ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the security of the core services they provide."[188] However, the proposed amendment introduced further details by stipulating that:

> Member States shall implement mechanisms to ensure that market operators, notify without undue delay to the competent authority or to the single point of contact incidents having an impact on the security

---

32(3)(c), at 131. This could be approached in light of the discussions in Section 3.1.3 where the controller does not have the contact details of the individual and obtaining such would involve disproportionate effort.

184. *GDPR supra* note 8, art. 32(3)(d), at 132; *Council Draft*, *supra* note 147, art. 32(3)(d), at 132. This could involve, as discussed in Section 3.1.3, the situation in which the notification to the individual might put at risk the proper investigation of the personal data breach or other crimes.

185. *Proposed NIS Directive*, *supra* note 4, at 2.

186. DR. MARNIX DEKKER ET AL., EUR. NETWORK & INFO. SEC. AGENCY, CLOUD SECURITY INCIDENT REPORTING FRAMEWORK FOR REPORTING ABOUT MAJOR CLOUD SECURITY INCIDENTS 8 (Dec. 9 2013), *available at* https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing/at_download/fullReport.

187. *Comm. on Internal Mkt. and Consumer Protection, Report on the Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union* (Dec. 2, 2014) [hereinafter *Comm. on Internal Mkt. and Consumer Protection*], *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0103+0+DOC+PDF+V0//EN.

188. *Proposed NIS Directive*, *supra* note 4, at 24.

> or continuity of the core services they provide. Notification shall not expose the notifying party to increased liability.[189]

Compared with all the above breach notification regimes, the NIS Directive covers a wide range of actors under the name of "market operators." In addition to market operators, the initial text proposed by the Commission covered public administrations. In the initial Commission draft, the term "market operators" is referred to include operators of critical infrastructures and providers of information society services (the non-exhaustive list of the latter includes e-commerce platforms, Internet payment gateways, Social networks, Search engines, Cloud computing services, and application stores).[190] However, the amendment from Parliament limits the scope of "market operators" to providers of infrastructures that are critical in a stricter sense and exclude its application to information society services and public administrations. Yet, the Directive still entitles Member States to extend the application to public administrations.[191] The draft from the Parliament defines a "market operator" as an:

> Operator of infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial market infrastructures, internet exchange points, food supply chain and health, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions, a non-exhaustive list of which is set out in Annex II, insofar as the network and information systems concerned are related to its core services.[192]

Annex II of the NIS Directive provides a non-exhaustive list of operators of critical infrastructure. This includes Banking (credit institutions in accordance with Article 4(1) of Directive 2006/48/CE), Financial market infrastructures (stock exchanges and central counterparty clearing houses), Health sector (including hospitals, private clinics, and other entities involved in health care provisions), energy (electricity and gas suppliers, Electricity and/or gas distribution system operators and retailers for final consumers) and transport (air, maritime, and railways).[193] The draft from the Parliament added the security and defense sector into the list.[194] Primarily, the breach notification requirements apply to all market operators providing services within the EU. It is not

---

189. *Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, art. 14(2), at 53.

190. *Proposed NIS Directive*, *supra* note 4, art. 3(8) & Annex II, at 19, 30.

191. *Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, art. 14(8)(a), at 58.

192. *Id*. art. 3(8)(b), at 34.

193. *Proposed NIS Directive*, *supra* note 4, art. 3(8)(b) & Annex II, at 19, 30.

194. *Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, Annex II, at 67-69.

clear from the Directive that whether the mere fact that an operator has European customers is enough for the law to apply or whether an establishment within one of the Member States is required. However, the draft from the Parliament added that "market operators not providing services in the [EU] may also report incidents on a voluntary basis."[195]

The breach notification requirement under the NIS Directive excludes three actors from its scope.[196] First, undertakings providing public communication networks or publicly available electronic communication services within the meaning of Framework Directive are excluded. This is mainly because such actors are required to report network breaches under the Framework Directive.[197] However, Article 1(a)(5) of the draft from the Parliament provides that "incident notifications referred to in Article 14 shall be without prejudice to the provisions and obligations regarding personal data breach notifications set out in Article 4 of Directive 2002/58/EC and the Regulation (EU) No 611/2013."[198] This implies that if an electronic communication service provider is an operator of a critical infrastructure and sustains personal data breaches, it should comply with the requirements under Article 4 of Directive 2002/58/EC, Regulation 611/2013, and the NIS Directive. Second, trust service providers, as defined in the eIDAS Regulation are excluded from the scope of the NIS Directive. The rationale behind this is also related to the introduction of breach notification requirements for trust providers under the eIDAS Regulation. Third, the Directive does not apply to microenterprises.[199] However, the draft from the Parliament qualifies such exemption by extending the application of the Directive to microenterprises if they act as subsidiaries of market operators as defined under Article 3(8)(b).[200] Software developers and hardware manufacturers are also excluded from the application of the Directive.[201]

Many experts from industry and government warned for the risk of unnecessary costs due to national differences in implementing NIS in-

---

195. *Id*. art. 14(2)(c), at 55.

196. *Proposed NIS Directive*, *supra* note 4, art. 1(3), at 18.

197. *See supra* Section 3.1.1.

198. *Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, art. 1(a)(5), at 31.

199. Defined in Commission Recommendation 2003/361, as constituting "micro, small and medium-sized enterprises (SMEs) made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million." Commission Recommendation 2003/361, title I art. 2, of May 6, 2003 Concerning the Definition of Micro, Small and Medium-sized Enterprises, 2003, O.J. (124) 36, 39 (EC); *see also Proposed NIS Directive, supra* note 4, art. 14(8), at 24.

200. *Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, art. 14(8), at 58.

201. *Proposed NIS Directive*, *supra* note 4, at 14.

cident reporting and potential overlap with the notifications under the proposed GDPR. Particularly, the scope of the initial draft of the NIS Directive from the Commission is so broad that it significantly overlaps with the draft GDPR. This means information service providers such as cloud computing services and online payment service would be subject to the draft GDPR as well to Member States' implementation of the NIS Directive. In this regard, Recital 31 of the NIS Directive requires minimizing the administrative burdens where the incidents also involve personal data breaches by developing information exchange mechanisms and templates in order to avoid the need for two notification templates. However, more work will need to be done to clarify how this is to work in practice particularly to harmonize the implementation of incident reporting provisions whenever possible.

Notification to National Regulatory Authorities (NRAs) or public

Not every breach that is sustained by market operators has to be reported. Rather only those that concern the network and information systems that are related to the core service.[202] This implies that a financial institution which is engaged in charity activities might sustain breaches. In this case, unless there is another law that requires the financial institution to notify breaches, for example, data Protection Regulations, the organization is not required to notify such breaches under the NIS Directive. This is because such charity activities are not related to its core activity as a financial service.

The breach notification regime under the NIS Directive is very similar to the regime under the Framework Directive.[203] One instance of such proximity to the Framework notification regime can be found in the amendment from the Parliament that refers to "incidents having significant impact on the continuity of the core services they provide."[204] This means the main focus of the breach notification is on incidents having significant impact on the functionality or continuity of the services, as elaborated under Section 3.1.1. Article 3(8a) of the draft from the Parliament defines "incident having a significant impact" as an "incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions."[205] Furthermore, the same paragraph of Article 14(2) in the

202. *Proposed NIS Directive*, *supra* note 4, art. 14(2), at 24; *Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, art. 14(2), at 53.

203. *See Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, art. 14(8), at 58. The committee states that the breach notification requirement uses "indicators similar to those laid down in the ENISA Technical Guidelines on reporting incidents for Directive 2009/140/EC." *Id.* at 72.

204. *Id.* art. 14(2), at 53.

205. *Id.* art. 8a, at 34.

draft from the Parliament indicates that in assessing significance of the impact of an incident the following parameters should take into account: (a) "The number of users whose core service is affected; (b) The duration of the incident; and (c) Geographic spread with regard to the area affected by the incident."[206] This is in line with the criteria discussed in Section 3.1.1 regarding Framework Directive. Another addition by the Parliament into Article 14(2) is that the "notification shall not expose the notifying party to increased liability."[207] This provision is an attempt to ensure that notifying entities are not severely punished for exposing more details of the breach or for non-compliance with the procedural requirements of notification.[208] This emanates from the need to avoid that potential sanctions should not dis-incentivize the notification of incidents and create adverse effects.

The initial draft from the Commission requires the notification to be made to the competent national authorities designated by each Member State to monitor the application of the Directive at a national level.[209] However, Article 6(4a) of draft from the Parliament added that where a Union law provides for sector-specific supervisory or regulatory body, the notification of incidents in accordance with Article 14(2) from the market operators should be made to such authority.[210] This means, for example, the financial authorities might be designated to deal with notifications from the financial sector and the health authorities regarding health sector and transport authorities for the transport sector provided there is sector-specific Union law to that effect. The designation of the sector specific regulator to handle the notification is logical because such authorities are believed to possess a better understanding of the threats and vulnerabilities, particular to their sector, and are therefore in a better position to assess the impact of potential or current incidents to their sector.

However, this could lead to a significant challenge where providers that support different critical infrastructures might be required to notify all such authorities. In order to avoid such problem, Article 6(2a) requires that where a Member State designates more than one competent authority, it shall designate a "single point of contact on the security of network and information systems."[211] Moreover, Article 6(4a) underlines the need for close coordination between the sector-specific regulatory authority and the competent authorities or the single point of contact of under Article 6(2)(a). These provisions avoid a duplication of notifica-

206. *Id*. art. 14(2)(a-c), at 53-54.

207. *Id*. art. 14(2), at 53.

208. *Id*.

209. *Proposed NIS Directive*, *supra* note 4, art. 6(1-2), at 20.

210. *Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, art. 6(4a), at 40.

211. *Id*. art. 6(2a), at 38.

tions both to the competent authorities and single point of contact as well as notification to different sector-specific authorities.

Unlike the initial draft from the Commission, which did not contain any reference to the timeframe, the proposed amendment from Parliament added "undue delay" to Article 14(2). Therefore, "undue delay" should be approached as discussed in Section 3.1.3. The details about the content and procedure are left for the implementations by Member States; however, the discussions in the above sections regarding these aspects are generally relevant. Furthermore, Article 14(2a) of the draft from the Parliament further adds that the notification should be made to the competent authority where the core services are affected.[212] If the core services in "more than one Member State are affected, the single point of contact which has received the notification shall, based on the information provided by the market operator, alert the single points of contact in other Member States."[213] It is not clear whether this provision is establishing a single notification regime for providers operating in many Member States and if so, which Member State's single point of contact should be notified. Furthermore, Article 14(2)(a) of the draft from the Parliament indicates that "Market operators shall notify the incidents referred in paragraphs 1 and 2."[214] The reference to paragraph 1 seems to imply that operators have to notify risks that are identified under Article 14(1). This might be the case given Article 14(1) of the same draft requires operators to take measures to detect and effectively manage risks.

Once the notification is received, the competent authority, after consultation with the market operators, might inform the public about the incidents if it is determined that public awareness is necessary. According to the addition in the draft from the Parliament, such awareness is deemed to be necessary if the notification to the public enables to prevent an incident or deal with an ongoing incident, or where that market operator that sustained the breach has "refused to address a serious structural vulnerability related to that incident without undue delay."[215] However, the authorities shall balance the public interest with the interest of the market operator including the possible use of anonymous notification and putting in place appropriate procedural safeguards where the operator is given the opportunity to be heard before going public.

---

212. *Id*. art. 14(2a), at 54.
213. *Id*. art. 14(2a), at 54-55.
214. *Id*. art. 14(2a), at 54.
215. *Id*. art. 14(4), at 56.

3.4. BREACH NOTIFICATION BY 'TRUST SERVICE PROVIDERS': THE EIDAS REGULATION

The eIDAS, which will replace the existing Electronic Signature Directive 1999/93/EC,[216] was adopted by the European legislators on 23 July 2014.[217] As the name indicates the Directive from 1999 essentially focuses on electronic signatures excluding providers of other types of certificates, or complementary services related to electronic certificates but not oriented to electronic signatures such as seals or time stamps, website authentication certificates. Therefore, the Regulation extends the concept of certification services further from electronic signatures to any type of electronic certificates. The main objective of the Regulation is to enhance trust and provide legal certainty for secure and smooth electronic interactions between businesses, citizens and public authorities and thereby increase the effectiveness of public and private online services in the EU.[218] More generally, the main goals of the Regulation could be summarized: (1) Ensuring mutual recognition and acceptance of electronic identification across borders; (2) To give legal effect and mutual recognition to trust services; (3) Enhancing current rules on e-signatures; (4) Providing a legal framework for electronic seals, time stamping, electronic document acceptability, electronic delivery and website authentication; (5) Ensuring minimal security level of trust services providers systems; and (6) Enforcing obligation of notifications about security incidents for trust services providers.[219]

Subject matter of the eIDAS Regulation and the breach notification requirement

The Regulation, under Article 2, lays down two primary legal grounds for its application. First, the Regulation applies to electronic identification schemes that have been notified by a Member State and recognized by the Commission upon fulfillment of certain conditions as stipulated under Articles 7-9. Second, the Regulation applies to trust service providers established within the Union. Article 3(16) of the Regulation defines "trust service" as:

> 'an electronic service normally provided for remuneration' consisting of the following:

---

216. Directive 1999/93, of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999 O.J. (L 13) 12 (EC).

217. Regulation 910/2014, 2014 O.J. (L 257) 73 (EU) (eIDAS Regulation).

218. Regulation 910/2014, 2014 O.J. (L 257) 73 (EU).

219. *Commission Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*, COM (2012) 238 final (June 4, 2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF.

> (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
>
> (b) the creation, verification and validation of certificates for website authentication; or
>
> (c) the preservation of electronic signatures, seals or certificates related to those services.[220]

This definition brings a wide array of actors into its realm including companies specialized in the subject of certification and electronic signatures as well as businesses, "whose core activities lie elsewhere but offer and certification and trust services as value-added services to the benefits of their clients."[221] The use of the phrase "normally provided for remuneration" implies that only services provided on a commercial basis are subject to the legislation although remuneration does not have to be in the form of direct payments.[222] This excludes the provision of trust services, which have no effect on third parties such as "systems set up in businesses or public administrations to manage internal procedures making use of trust services."[223]

In accordance with the precedents of the Court of Justice for the European Union (CJEU), a trust service provider would be considered to have an establishment within the EU, if it has effective and real exercise of activity in a Member State through stable arrangements irrespective of the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality.[224] Furthermore, some trust services provided by trust providers established outside the EEA might be recognized through "an agreement concluded between the Union and the third country in question or an international organization in accordance with Article 218 TFEU."[225] This implies that the requirements of the Regulation will be applicable, through their inclusion in the agreements, to the trust providers established outside the Union.

The eIDAS Regulation regulates the notification of breaches by trust service providers as defined under Article 3(16). The Regulation makes a distinction between qualified and non-qualified trust service

---

220. Regulation 910/2014, 2014 O.J. (L 257) 73 (EU).

221. JOSHUA BUDD ET AL., EUR. NETWORK & INFO. SEC. AGENCY, IMPLEMENTATION OF ARTICLE 15 OF THE DRAFT REGULATION ON ELECTRONIC IDENTIFICATION AND TRUSTED SERVICES FOR ELECTRONIC TRANSACTIONS IN THE INTERNAL MARKET 7 (Dec. 19 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/implementation-of-article-15/at_download/fullReport.

222. Regulation 910/2014, art. 3(16), 2014 O.J. (L 257) 73, 84 (EU).

223. *Id*. at 76.

224. Case 168/84, Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt, 1985 E.C.R. 2251, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61984CJ0168&from=EN.

225. Regulation 910/2014, art. 14(1), 2014 O.J. (L 257) 73, 92 (EU).

providers. Generally non-qualified trust service providers are subject to lighter obligations within the Regulation. However, the breach notification requirement applies to any trust service provider regardless of whether it is qualified or not. In this regard, Article 19 contains two kinds of notifications. The first relates to the notification of risks that might have "adverse effects" to the security of the trust services. This flows form the obligation of the trust service providers to take appropriate measures commensurate to the degree of risk. This requirement is similar to the notification of "particular risk" under the ePrivacy Directive as discussed above. Once the providers are able to identify that a certain security incident might have adverse effect, they have to inform the relevant stakeholders including the users and supervisory authorities.[226] Furthermore, Article 19(2) of the Regulation stipulates that trust service providers:

> [S]hall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.[227]

Notification to National Regulatory Authorities (NRAs)

A further distinction can be made between two kinds of breaches under Article 19(2) of the Regulation. The first breach concerns *any breach of security or loss of integrity that has a significant impact on the trust service provided*. This terminology is similar to Article 13a of the Framework Directive. Therefore, discussion regarding the kind of breach to be notified is equally applicable for this breach. In other words, the focus of the breaches is mainly on the functionality or continuity of the services and the "significance" is determined having regard to the number of customers' affected, geographical coverage, and the length of the incident. However, "breaches affecting trust services" could have more severe ramifications as "they may result in the loss of trust in the digital identity of a natural person or a legal entity."[228] In addition, unlike the notification within the Framework Directive which excludes its application to the physical kit such as telecom equipment, the breaches under the eIDAS Regulation might emanate from breaches affecting, for example, IT equipment (misplaced or stolen equipment laptops or USB sticks).

The second kind of *breach constitutes breach of security or loss of in-*

226. *Id*. art. 19(1), at 95.

227. *Id*.

228. BUDD ET AL., *supra* note 221, at 19.

tegrity that has a significant impact on the personal data maintained. Under the Regulation 611/2013 we have noted that any kind of personal data breach regardless of its significance has to be notified to the relevant authorities. However, Article 19(2) seems to qualify the notification of such breaches only if it has "a significant impact on the personal data maintained."[229] This contradicts the requirements under both the Regulation 611/2013 and the draft GDPR that require notification of any personal data breach, even very small incidents, to data protection authorities. However, Recital 11 of the eIDAS Regulation indicates that the Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council. This implies that once the breach affects personal data, Regulations 611/2013 and the GDPR will have an upper hand on their application. Thus, any breach of personal data has to be notified to the data protection authorities in accordance with the Regulation 611/2013 and draft GDPR regardless of its impact. According to Article 19(2), such notification has to be made both to the competent supervisory authority designated by the Member State to handle matters on trust providers and the Data Protection Authority. This might give rise to multiple notifications by some providers under the eIDAS Regulation, draft GDPR and possibly the NIS Directive. Taking PayPal as an example, a security breach affecting its service might need to be reported under the eIDAS Regulation (as provider of trust services such as DocuSign eSignatures), under the GDPR (as data controller of personal data) and possibly under the NIS Directive (as operator of financial services that are considered critical infrastructure). Such breaches have to be notified to the relevant supervisory body without undue delay but in any event within 24 hours after having become aware of it. This provision in particular makes it clear that the use of the term "undue delay" within the notification regimes represent that the notification should be given immediately.

Notification to individuals or legal person

Paragraph 2 of Article 19(2) states that:

> Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.[230]

This is essentially similar to the requirements under Article 3(1) of Regulation 611/2013. Thus, the assessment of whether a security

229. Regulation 910/2014, art. 19(2), 2014 O.J. (L 257) 73, 95 (EU).
230. *Id*.

breach adversely affects the individual has to be made in the same manner as discussed in Section 3.1.3. This notwithstanding, unlike Article 3(1) of Regulation 611/2013, the adverse effect under the eIDAS Regulation is not only limited to privacy or personal data concerns but also includes breaches affecting loss of trust in the digital identity of a natural person or a legal entity. In addition, the eIDAS Regulation covers the notification of breaches to legal persons.

3.5. NOTIFICATION OF BREACHES WHEN USING THIRD PARTY PROVIDERS

One notable pattern in the emerging breach notification requirements is the introduction of obligations on third party provider to inform and alert actors subject to breach notification requirements. One of the main challenges for enforcement of breach notification requirements is the disclosure disincentive. As noted above, such disincentive is particularly strong when there is third party involvement, such as cloud providers, in undertaking certain operations, for example in relation to billing or management functions, on behalf of the provider. In such a case where a data breach occurs at the third party provider, the third party provider is not under obligation to notify the regulatory authorities or the end users regarding the breach. However, both Regulation 611/2013 and the proposed GDPR try to mitigate by introducing obligations on the third party to inform the provider. For example, Article 5 of Regulation 611/2013 requires the third party provider to "alert and inform the provider with which it has a direct contractual relationship."[231] This applies, for example, in the context of wholesale provision of electronic communications services, when typically the wholesale provider does not have a direct contractual relationship with the end user. In such a case, the wholesale provider should inform the retail provider, which in turn should notify the end users. Similarly, Article 31(2) of the proposed GDPR requires the processor to "alert and inform the controller without undue delay after the establishment of a personal data breach."[232]

It has to be noted that the involvement of a third party provider does not reduce any of the conditions regarding, timeframe, and content to be complied with. Therefore, it is recommended that the obligation of the third party provider to notify the provider immediately if a personal data breach occurs be set out in a contract. Nevertheless, given that many third party providers' offer non-negotiable standard terms of service, it may be difficult to negotiate such notifications into the contracts for many controllers, particularly SMEs. Where contracts are negotiable, such contract should include an obligation on the third party pro-

231. Commission Regulation 611/2013, 2013 O.J. (L 173) 2, 3 (EU).

232. *GDPR*, *supra* note 8, art. 31(2), at 60.

vider to provide any information that the provider is required to provide in its notification to the authorities and affected individuals. To the extent possible, the contract should also address the party responsible to bear the notification costs, legal costs, and investigation costs. The challenge with third party providers, such as cloud providers is that sometimes it might be not easy for the provider to know whether certain breach affects personal data of its customers. For example, providers of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) might not be aware of whether their infrastructure is handling personal data.[233] Furthermore, regarding the requirements under the proposed GDPR, making distinction between controller and processor appears to be a challenging task in cloud computing scenarios. Some commentators suggest that one way of dealing with such challenge is to adopt the "intermediary liability" approach within the e-Commerce Directive where only controllers should be responsible.[234] This would also imply that the obligation to inform the controller might be triggered once the third party provider is aware that it is handling personal data. Furthermore, a survey by ENISA on cloud security incident reporting stresses the importance of anonymity through legal protection or non-disclosure agreements in encouraging breach disclosure by cloud providers.[235] Therefore, further implementing measures from the Commission and Member States on breach notifications should give due consideration of such measures for notifying breaches under certain circumstances.

Although the amendments from the Parliament to the NIS Directive have excluded the application of the Directive to information service providers such as cloud computing providers, cloud service providers might still be subject to the Directive. This could be where the cloud computing services are used by "operators of critical infrastructure to support the delivery of their core services" or where the cloud computing services are critical in themselves.[236] In the first case scenario, the cloud providers have to notify the critical infrastructure operator regarding the breaches so that the latter could notify the relevant authorities. In the second case, the cloud providers themselves have to notify the competent national authorities. Nevertheless, this raises many controversial issues. First, it is often hard for the cloud provider, particularly IaaS and PaaS providers, to know the number of end-users and organizations depending on the cloud services. This means it is "dif-

---

233. DR. MARNIX DEKKER ET AL., EUR. NETWORK & INFO. SEC. AGENCY, CLOUD SECURITY INCIDENT REPORTING FRAMEWORK FOR REPORTING ABOUT MAJOR CLOUD SECURITY INCIDENTS, *supra* note 186.

234. Hon et al., *supra* note 164, at 39.

235. DR. MARNIX DEKKER ET AL., EUR. NETWORK & INFO. SEC. AGENCY, CLOUD SECURITY INCIDENT REPORTING FRAMEWORK FOR REPORTING ABOUT MAJOR CLOUD SECURITY INCIDENTS, *supra* note 186, at 17.

236. *Id.* at 10.

ficult to measure the impact of incidents or the criticality of a service in terms of the number of end-users, because the number of end-users cannot be easily estimated by the service provider" or due to a chain of actors.[237] The reason behind is that the cloud provider might not be aware of what kind of service or data is used over its infrastructure by the customer and how critical such service might be. Second, to the extent that cloud services can be used by the energy, transport, banking, financial market, and health sector, a challenge could be that if a cloud services, which is considered to be critical in itself, offers services for all these sectors, which would be the appropriate organ for the cloud provider to report the breaches to, i.e. Financial regulator, Energy regulator, or "in general the public bodies that have a regulatory mandate that includes networks and information security."[238] Third, the distributed nature of cloud services means many Member States might be involved in the provision of a specific service, making it difficult "to determine where such incidents should be reported."[239]

4. DEALING WITH THE COMPLEXITY OF BREACH NOTIFICATION REQUIREMENTS

One of the rationales for breach notification requirements is to enhance transparency of organization on data security. Transparency is also related to data security and risk management. In the above discussions we have noted that the relevant actors subject to the Regulation 611/2013, the proposed GDPR, the proposed NIS Directive and the eIDAS Regulation are required to take measures that are commensurate to the risks presented. Furthermore, a risk management framework is an essential part of the proposed NIS Directive where organizations are required to have a methodology and criteria for identifying, evaluation, prioritization and treatment of risk as well as for assessing the impact of potential incidents.[240] Similarly, both the Framework Directive and the eIDAS Regulation contain provisions for the notification of particular risks to the users of the services, clearly showing that a risk assessment and an appropriate risk management framework is an important consideration with in such legislations regulating breach notifications. This implies that companies should define in advance appropriate plans to deal with breach notification requirements, which can ensure that they respond quickly and effectively to security incidents.[241] Given that

237. *Id.* at 11.

238. *Id.* at 23.

239. *Id.* at 20.

240. *Proposed NIS Directive*, *supra* note 4, art. 5(2), at 20; *Comm. on Internal Mkt. and Consumer Protection*, *supra* note 187, art. 5(2)(a).

241. RECOMMENDATIONS ON TECHNICAL IMPLEMENTATION GUIDELINES OF ARTICLE 4, *supra* note 97, at 6.

security risk analysis is an integral part of the notification requirements, addressing breach notification requirements in conjunction with the security risk analysis would benefit organizations in a number of ways.

First, risk management enables organizations to identify risks in advance and thereby decrease the possibility of unexpected events to occur.[242] Research shows that it is cheaper for corporations to be proactive in their efforts to prevent data breaches rather than react after it happens.[243] On the one hand, organizations will be able to identify the possible risks and take measures to prevent them, meaning the need to comply with breach notification requirements would not arise. On the other hand, organizations will be better prepared in detecting and reporting the breaches rapidly. More particularly, addressing breach notification requirements in conjunction with security risk analysis would enable organizations for assessing which of the identified security incidents, if materialized, needs notification to the authorities or both to the authorities and individual. Second, the security risk analysis becomes essential when looking at the content of the notification that the regimes require. At least in cases of personal data breaches, the security risk analysis is essential in providing inputs such as the nature of the data that has been breached (financial, health, etc.), nature of the breach (widespread, or an isolated incident; technical, human error, or theft), and security level (has the data been encrypted). Attaching the data breach notification requirement to security risk analysis would enable organizations to import such content easily from the latter. Similarly, the security risk analysis will be useful in making decisions such as whether an incident will have "a significant impact" on the security of networks or services so that the breach notification requirement under the Framework Directive, the NIS Directive, and eIDAS Regulation need to be complied. Related with this, ENISA's methodology for assessing the adverse effect of a breach on the rights of individuals, discussed in Section 3.1.3, would be simpler to use if compliance with the breach notification requirement is aligned with the security risk analysis.

Third, considering data breach notification requirements during security risk analysis is particularly important because such laws require organizations give notice of the breach within a matter of hours or at most a few days. However, if organizations manage to address such compliance issues in advance during the security risk analysis, it would avoid a possible last minute rush and confusion in determining which risks to report once a security breach occurs. Therefore, organizations

---

242. PEDRO VICENTE & MIGUEL M. DA SILVA, A CONCEPTUAL MODEL FOR INTEGRATED GOVERNANCE, RISK AND COMPLIANCE 204 (H. Mouratidis ed., 2011).

243. Michael E. Jones, Comment, *Data Breaches: Recent Developments in the Public and Private Sectors*, 3 J.L. & POL'Y INFO. SOC'Y 555, 580 (2007).

need to "navigate the dense fabric of security breach notification requirements of various locations and jurisdictions and identify the relevant risks."[244] During such risk analysis, measures should be put in place such as establishing a communication channel between the security experts and legal/compliance team when a security breach occurs so that the organization can comply with the notification requirements in the given timeframe.

5. CONCLUSION

The prominence of information technology in day-to-day life means that businesses' ICT infrastructures attract great interest from both cyber-criminals and legislators. Businesses have to deal not only with the increased cyber-attacks, but also with an array of increasingly complex laws dealing with information security. The emergence of a number of regulatory instruments containing breach notification requirements within the EU and around the globe is a reflection of such reality. At present there are four regulatory instruments, which are already in force and two proposed legislations containing breach notification requirements in the EU. This article studies the emerging and existing breach notification requirements in the EU in a way that shows their overlap, areas of conflict, and the resulting complexity in compliance with such requirements. In this regard, the article examines two existing, two newly implemented, and two en route laws containing breach notification requirements. It also highlights the challenges in the effective implementation of such rules. Furthermore, the article underlines the need to adopt a proactive approach to compliance with breach notification requirements. Particularly, given the emergence of legislative instruments requiring for conducting security risk analysis, addressing breach notification requirements in conjunction with security risk analysis would significantly ease organizations' compliance with such requirements in reporting breaches quickly and effectively.

The article also shows that there is significant convergence among the different notification regimes – existing and emerging. More particularly, the breach notification requirements under the Framework Directive, the NIS Directive, and the eIDAS Regulation are essentially similar. Such requirements focus on breaches that affect the functionality or continuity of a network or services and these regimes require such breaches to have significant impact on the network or services, which is determined having regard to the number of customers' affected, geographical coverage and the length the incident lasts. Likewise, the notification regimes under the Regulation 611/2013 and proposed GDPR are essentially similar. They focus on the notification of personal data

244. WORLD LAW GROUP, *supra* note 12, at i.

breach notifications to regulatory authorities and to individuals. Under both regimes, the regulatory authorities should be notified of any kind of personal data breach regardless of its impact. However, the notification to the individuals or subscribers adopts a risk-based trigger which requires a "likely adverse effect" on the rights of the subscriber or individual. In addition, the ePrivacy Directive and the eIDAS Regulation contain provisions for the notification of "risks" to customers that might have an adverse effect on the services of the provider.

In some sense, the convergence among the different regimes contributes positively in the understanding of the breach requirements and in gearing the notification regimes in a similar direction. However, such overlap means that the same breach within a company might have to be brought to the attention of a number of different regulatory authorities, and following different timeframes and procedures. For example, the Commission draft of the NIS Directive applies to information service providers such as cloud providers and online payment services. This significantly overlaps with the draft GDPR, which means information service providers, would be subject to the proposed GDPR as well to Member States' implementation of the NIS Directive. This might create complexity in compliance and considerable administrative costs for providers operating cross-border. Overall, although a greater convergence among the regimes is positive and commendable, more work need to be done in terms of creating stronger collaboration among the different regulatory authorities or creating a single point of contact for notification by providers that are subject to different notification regimes.

In addition, a notable trend among the notification regimes is that third party providers, such as cloud providers, are obliged to inform the main providers subject to the breach notification. Although this is a good approach in mitigating the disclosure disincentive for such providers, sometimes it might be difficult for the third party providers to know that their customers have such an obligation. For example, an IaaS provider might not be aware that its customer is handling personal data on its infrastructure and is subject to the Regulation 611/2013 or the GDPR. So there are suggestions for the "intermediary liability" approach where such third parties would be responsible only based on their actual knowledge. Furthermore, although the need for anonymous notification channels has been underlined by cloud providers, such measure has hardly caught any attention in the notification regimes and need to be explored.