scripted

Volume 18, Issue 1, September 2021

NISD2: A Common Framework for Information Sharing Among Network Defenders

*Andrew Cormack**

DOI: 10.2966/scrip.180121.83

Abstract
Sharing information about vulnerabilities and attacks is essential to defend information systems against threats such as malware, phishing and unauthorised access. By identifying this information sharing as a legitimate interest of data controllers, and highlighting the public interests that it serves, the draft Network and Information Security Directive provides a framework to encourage European participation in global information sharing, benefitting all users of the Internet.

Keywords
Data Protection; incident response; information sharing; NIS Directive; security

* Chief Regulatory Adviser, Jisc, Didcot, UK, andrew.cormack@jisc.ac.uk.

1 Introduction

One of the European Commission's aims in proposing an updated Network and Information Security Directive[1] (henceforth "NISD2") is to "facilitate secure, robust and appropriate information-sharing".[2] Those defending networks and information systems need "information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools"; sharing this helps:

> (a) preventing, detecting, responding to or mitigating incidents;
> (b) enhance[] the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats' ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.[3]

Article 26 of the proposed Directive therefore requires Member States to "ensure that essential and important entities may exchange relevant cybersecurity information among themselves",[4] while respecting the General Data Protection Regulation (GDPR).

However, Article 27 recognises that sharing among "essential and important entities" is insufficient. These entities – including digital infrastructures, platforms and some areas of manufacturing, as well as traditional critical infrastructures[5] – may represent the most societally significant **impacts** of

---

1 European Commission, "Proposal for a Directive on Measures for High Common Level of Cybersecurity Across the Union" (COM(2020) 823 final, 16 December 2020), available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166 (accessed 8 March 2021).

2 *Ibid*., p. 3.

3 *Ibid*., art. 26(1).

4 *Ibid*.

5 *Ibid*., arts. 1 and 2.

network and information insecurity, but much of the **threat** to them comes from outside the Directive's scope: from compromised devices in homes, non-NIS organisations, and from outside the EU. Information about these – for example from software and service providers – is essential to prevent, detect and mitigate security incidents. Member States are therefore required to "ensure that…entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses".[6]

This paper examines why and how defenders share network and information security information, and the patchwork of GDPR provisions that currently applies. For information sharing to be trusted to deliver benefits rather than create risks, it needs a clear, simple basis in data protection law, without relying on quibbles, exemptions, or the turning of blind eyes. The new draft Directive suggests how this might be achieved.

2 The Importance of Sharing

NISD2 Recital 67 explains why information sharing is important for network and information security:

> With cyber threats becoming more complex and sophisticated, good detection and prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to increased awareness on cyber threats, which, in turn, enhances the entities' capacity to prevent threats from materialising into real incidents and enables the entities to better contain the effects of incidents and recover more efficiently.[7]

---

[6] *Ibid*., art. 27.

[7] *Ibid*., Recital 67.

Three practical examples illustrate how this happens and, later, how it is addressed by data protection law:

- **Victim notification**. Organisations defending their own networks, systems, information and users often discover signs of security breaches elsewhere. For example, they may detect attacks coming from a compromised machine, find passwords or credit card details during forensic investigations, or on sites where intruders post "stolen" data.[8] Most teams, given sufficient resources, try to notify the victims of such breaches. This mainly benefits the organisation or individual being notified but, by "impeding…threats' ability to spread" (Article 26(1)(b)),[9] it should also reduce malicious activity against the notifying organisation. Typically, notifications are sent to a trusted (or at least self-interested) intermediary such as an internet service provider, organisation or bank. Individual victims are hard to identify from Internet Protocol (IP) addresses, card details and similar pseudonyms and, even where this is possible, sending notification to a victim's compromised account may alert the intruder, so is usually avoided. For large-scale notifications, organisations may send their victim lists to National Computer Security Incident Response Teams (CSIRTs) with facilities for automated processing, but smaller-scale notifications are usually sent direct.
- **Community alerting**. When defenders discover new threats, vulnerabilities or defences they normally share this knowledge to help others protect their own networks, systems, data and users: Article

---

8 European Network and Information Security Agency, "Proactive Detection – Measures and Information Sources" (ENISA, 2020), available at https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources (accessed 8 March 2021).

9 European Commission, NISD2, *supra* n. 1, art. 26(1).

26(1)(a) mentions "information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools".[10] Such sharing normally uses trusted communities because the shared information – even the fact that it is known – would help current attackers evade detection and might help others mount copy-cat attacks.

- **Collaborative analysis**. Understanding and defending the largest, most complex, and most damaging threats requires defenders to collaborate. Attacks that modify global infrastructures – such as naming[11] and routing[12] – may only become apparent when different geographic viewpoints are compared; major threats may require coordinated skills and mitigation measures beyond those of any single team.[13] Global platforms let defenders work together on shared data;[14] services generate feeds of "threat intelligence" by combining individual sources.[15] Both help defenders "collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to

---

10 *Ibid*., art. 26(1).

11 Cloudflare, "What is DNS cache poisoning?" (2021), available at https://www.cloudflare.com/learning/dns/dns-cache-poisoning/ (accessed 8 March 2021).

12 Cloudflare, "What is BGP Hijacking?" (2021), available at https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/ (accessed 8 March 2021).

13 E.g. Catalin Cimpanu, "Microsoft orchestrates coordinated takedown of Necurs Botnet" (ZDNet, 10 March 2020), available at https://www.zdnet.com/article/microsoft-orchestrates-coordinated-takedown-of-necurs-botnet/ (accessed 8 March 2021).

14 E.g. MISP, "MISP – Open Source Threat Intelligence Platform and Open Standards for Threat Information Sharing" (undated), available at https://www.misp-project.org/ (accessed 8 March 2021).

15 E.g. SANS, "Internet Storm Center" (2021), available at https://isc.sans.edu/ (accessed 8 March 2021).

> enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats".[16]

3 Current Law on Sharing

Draft Article 26(1) insists information sharing must be "without prejudice to [the General Data Protection Regulation]". Draft Recital 69 suggests the primary mechanism for this. It first states, copying Recital 49 of the GDPR, that:

> The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security…should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679.

Whereas GDPR Recital 49 identifies attacks whose defence "could" require processing personal data:

> unauthorised access to electronic communications…malicious code distribution…'denial of service' attacks…damage to computer and electronic communications systems

NISD2 Recital 69 defines a complete defensive process – "prevention, detection, analysis and response" – and specific information sharing this "should" involve:

> measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and

[16] European Commission, NISD2, *supra* n. 1, Recital 68.

> configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.[17]

GDPR Recital 49 thus places activities protecting security within the Legitimate Interests framework (GDPR Article 6(1)(f)): by echoing the Recital 49 wording, NISD2 Recital 69 adds information sharing to the same framework.

Several authors have compared Article 6(1)(f)'s requirements with the incentives and practices of those defending networks and systems. Cormack found strong alignment, and suggested relevant factors for the legitimate interests balancing test to ensure users' interests were protected when sharing information. [18] The ACDC project concluded – under the prior Data Protection Directive – that sharing to mitigate botnets might be both a public interest and a legitimate interest of network operators; they also highlighted strict purpose limitation and limiting sharing to data necessary for that purpose.[19] The MISP platform found information about attacks, not victims, was most useful to other defenders.[20] Von Maltzan identified Article 6(1)(f) as appropriate for contributing data to collaborative platforms and suggested a privacy-by-design approach – sharing only structured data, masking or omitting local identifiers, using the

---

17 *Ibid*., Recital 69.

18 Andrew Cormack, "Incident Response: Protecting Individual Rights Under the General Data Protection Regulation" (2016) 13:3 *SCRIPTed* 258-282.

19 Advanced Cyber Defence Centre, "Legal Requirements (second iteration)" (ACDC Deliverable 1.8.2, 31 July 2015), available at https://acdc-project.eu/wp-content/uploads/2015/11/ACDC_D1.8.2_Legal-Requirements-Second-Iteration.pdf (accessed 8 March 2021).

20 MISP, "Information Sharing and Cooperation Enabled by GDPR" (30 January 2018), available at https://www.misp-project.org/compliance/gdpr/ (accessed 8 March 2021), p. 9.

Traffic Light Protocol[21] to express confidentiality – to satisfy the balancing test.[22] Sullivan and Burger examined automated sharing – to give "real-time warning"[23] – favouring public interest (Article 6(1)(e)) because legitimate interest would require notifying attackers, under Article 14.[24] However, according to the Article 29 Working Party, notification that would "seriously impair the achievement of the objectives of that processing" is exempt.[25,26] This would clearly apply if defenders had to try to tell attackers what they knew, their sources and methods. Long before GDPR, Swire identified information sharing within a trusted group of defenders as the best way to address cyber-attacks.[27]

Although the GDPR did not mention information sharing, the draft ePrivacy Regulation[28] provides tacit permission for it, by permitting processing of electronic communications data to protect **any** "electronic communications

---

21 Forum of Incident Response and Security Teams, "Traffic Light Protocol (TLP) – version 1.0", (FIRST, undated), available at https://www.first.org/tlp/ (accessed 8 March 2021).

22 Stephanie von Maltzan, "No Contradiction between Cyber-Security and Data Protection? Designing a Data Protection compliant Incident Response System", (2019) 10(1) *European Journal of Law and Technology*, pp. 10-11.

23 Clare Sullivan and Eric Burger, "In the public interest: The Privacy Implications of International Business-to-business Cyber-threat Intelligence" (2017) 33(1) *Computer Law and Security Review* 14-29, p. 16.

24 *Ibid*., pp. 26-27.

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter 'GDPR'), art. 14(5)(b).

26 Article 29 Working Party "Guidelines on Transparency under Regulation 2016/679" (17/EN WP260, 2017), pp. 25-28.

27 Peter Swire, "A Model for when Disclosure Helps Security: What is Different about Computer and Network Security?" (2004) 3(1) *Journal on Telecommunications & High Tech Law* 163-208.

28 Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)-Mandate for negotiations with EP" (6087/21, 10 February 2021) available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN (accessed 8 March 2021).

networks and services" (Article 6(1)(b)) or "end-users' terminal equipment" (Article 6(1)(c)), not just those within the organisation. Such processing is pointless unless its results are shared with those affected. NISD2 draft Recital 69 moves from permission to active encouragement – "That **should** include…exchange of information" [emphasis added] – and explicitly makes this part of the Article 6(1)(f) Legitimate Interests framework.

Note that both NISD2 and GDPR include "public authorities" among those allowed to use Article 6(1)(f), with its balancing test, even though they would more usually operate under the "public interest" (Article 6(1)(e)) justification, which presumes that individual interests and rights are considered in the enabling legislation. This addresses concerns that sharing between different legal bases may result in safeguards being lost.[29] Public bodies that do use public interest for network and information security can still provide that reassurance by conducting an Article 6(1)(f)-style balancing test as a matter of good practice.

Invoking GDPR Article 6(1)(f) is not, however, a complete solution for GDPR-conformant information sharing. As discussed above, truly effective sharing must include all defenders. Adding sharing outside Europe, or outside the NIS Directive's scope, makes the legal picture more complex.

4 Sharing Among Continents

As well as an Article 6 basis, sharing information outside the EEA must address additional risks according to GDPR Articles 44-49. Under the previous (1995) Data Protection Directive, exporting organisations might themselves assess the

[29] Cormack, "Incident Response", *supra* n 18, p. 268.

benefit and risk to data subjects:[30] victim notification provides immediate benefit to the recipient with very little risk; community alerting includes information about attacks, but attackers try to eliminate any risk of this being linked to them; for collaborative platforms, as Cormack notes, decisions to share based on security risks are usually at least as cautious as data protection requires.[31] But the GDPR removes this option for controllers to "adduce adequate safeguards", leaving only narrower, more prescriptive, options.

These include a legitimate interests basis, in Article 49, which might seem to coincide with the Article 6(1)(f) assessments used within the EEA. However, the export version has significant limitations: Article 6(1)(f) can consider benefits to anyone, but Article 49 only covers "compelling interests pursued by the controller", whereas victim notification and community alerting mainly benefit others; limiting to "not repetitive" transfers of data "concern[ing] only a limited number of data subjects" may exclude the most effective uses of collaborative analysis platforms and services.

Instead, each use case seems to require a different, less than satisfactory, provision. Victim notification might be framed as an Article 14 notification, arguing that the victim's personal data has been obtained from the (unknown) attacker. But this turns a voluntary act – helping others – into a legal obligation, potentially overriding the team's main priority of protecting its own users.[32]

Occasional community notification might be shoe-horned into Article 49 by ignoring its main benefit – to others – and claiming a residual "compelling interest" to the exporting organisation that a more secure Internet represents less

---

30 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 26(2).

31 Cormack, "Incident Response", *supra* n 18, p. 274.

32 Article 29 WP, "Transparency", supra n. 26, pp. 25-28.

threat. But any requirement to "inform the supervisory authority of the transfer" would risk overwhelming those authorities with low-risk notifications, already a problem under breach notification provisions.[33]

A few collaborative analysis services might offer standard contractual clauses under Article 46(2)(c) or (d). But the burden on exporting and receiving organisations is likely to exclude many important data sources and analysis platforms operated as volunteer, community-benefit activities.[34]

Alternatively we might quibble that attackers work hard to ensure they cannot be linked[35] – even using police powers – to the "online identifiers" used in attacks, so those identifiers should not qualify as GDPR Article 4(1) personal data. Or, in a less extreme form, that we are re-exporting identifiers that originate outside the European Economic Area, so do not expect the same level of protection.

But none of these is the "clear, simple basis, within data protection law" (see introduction above) needed for information sharing to be trustworthy.

5 Sharing Among Sectors

Although the NISD2 draft covers more organisations than its predecessor – notably adding public electronic communications networks providers and a wider range of digital services[36] – it still omits significant contributors to

---

33 Sarah Cameron, "ICO warns of over-reporting of data breaches" (Pinsent-Masons, 13 September 2018) available at https://www.pinsentmasons.com/out-law/news/ico-warns-over-reporting-data-breaches (accessed 8 March 2021).

34 E.g. SANS, *supra* n. 15.

35 Wajeeha Ahmad, "Why Botnets Persist: Designing Effective Technical and Policy Interventions" (Internet Policy Research Initiative, MIT, 2019) available at https://internetpolicy.mit.edu/publications-ipri-2019-02/ (accessed 8 March 2021), p. 6.

36 European Commission, "Revised Directive on Security of Network and Information Systems (NIS2)" (16 December 2020), available at https://ec.europa.eu/digital-single-

understanding NIS threats and counter-measures. These include, for example, software providers, researchers and organisations, wider manufacturing, and informal collaborations that address a particular problem.[37] We must not require everyone that wishes to contribute skills or information to submit to the NIS regulatory regime but, as Recital 68 recognises, "actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms".[38]

Article 27's voluntary reporting to national platforms is a good start[39] but, like National CSIRTs,[40] these organisations need to participate in international sharing activities, not just national ones. Important information sharing already occurs within global industry groups such as Information Sharing and Analysis Centres (ISACs)[41] as well as ad hoc problem-based and standing groups such as Emotet,[42,43] Internet Storm Centre[44] and the Forum of Incident Response and Security Teams (FIRST).[45] These may arise to keep commercially sensitive information within a sector, or because national platforms lack appropriate

market/en/news/revised-directive-security-network-and-information-systems-nis2 (accessed 8 March 2021).

37 Ahmad, "Why Botnets Persist", supra n. 35, s. 5.1.

38 European Commission, NISD2, *supra* n. 1, Recital 68.

39 *Ibid*., art. 27.

40 *Ibid*., Recital 26.

41 Wikipedia, "Information Sharing and Analysis Centre" (undated), available at https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center (accessed 8 March 2021).

42 Catalin Cimpanu, "Meet the White-hat Group Fighting Emotet, the World's Most Dangerous Malware" (ZDnet, 29 February 2020), available at https://www.zdnet.com/article/meet-the-white-hat-group-fighting-emotet-the-worlds-most-dangerous-malware/ (accessed 8 March 2021).

43 Europol, "World's Most Dangerous Malware Emotet Disrupted Through Global Action" (Europol, 27 January 2021), available at https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action (accessed 8 March 2021).

44 SANS, *supra* n. 15.

45 FIRST, "Forum of Incident Response and Security Teams" (undated), available at https://www.first.org/ (accessed 8 March 2021).

capacity or, as discussed by Tanczer, to include entities in countries that Government platforms find politically difficult to engage.[46] Any legislation that discouraged this sharing amongst peers would be seriously counter-productive.

Draft Article 5(2), on national cybersecurity strategies, recognises the need for information sharing to go beyond national platforms and collaborations: requiring Member States to "support voluntary cybersecurity information sharing between companies in compliance with Union law".[47] The final section considers whether NISD2 might provide a more consistent legal – as well as policy, procedural and technical – basis for that.

6 Sharing: A Public Interest

Draft NISD2 clearly provides informal support for current global information sharing practices, but it might also contribute to a clear, comprehensive legal basis for them, replacing the current patchwork for international and inter-sectoral sharing.

First, the lists of practices that may be "necessary and proportionate for the purposes of ensuring network and information security" in NISD2 Recital 69 and GDPR Recital 49 should be read together. Information sharing (NISD2) is thus permitted – or, following the Article 29 Working Party Opinion,[48] encouraged – for all data controllers in Europe. Both Recitals invoke Article 6(1)(f) legitimate interests, with its dual safeguards: that information sharing must be necessary for that purpose and satisfy the balancing test to protect the

---

46 Leonie Tanczer, Irina Brass, and Madeline Carr, "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy" (2018) 9(S3) *Global Policy* 60-66, p. 63.

47 European Commission, NISD2, *supra* n. 1, art. 5(2)(g).

48 Article 29 Working Party, "Guidelines on Personal Data Breach Notification under Regulation 2016/679" (WP250rev.01), available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (accessed 8 March 2021), p. 12.

rights and freedoms of data subjects. Article 6(1)(f) should therefore be the standard framework for anyone considering **what** to share. Where an organisation cannot use Article 6(1)(f) – though both Recital 49 and Recital 69 explicitly include "public authorities" – it should still conduct a balancing test as a matter of good practice and trustworthiness.

Second, NISD2 may provide a consistent test and legal framework for **when** to share, replacing the export patchwork described above. Whereas GDPR Recital 49 is motivated by breaches that harm individuals – unauthorised access, malware and denial of service attacks – NISD2 Recital 3 recognises their societal impact: "impede the pursuit of economic activities…generate financial losses, undermine user confidence and cause major damage to the Union economy and society". Thus we might consider whether sharing is "necessary for important reasons of public interest", bringing exports within GDPR Article 49(1)(d). By Article 49(4), such interests must be "recognised in Union law or in the law of the Member State to which the controller is subject". NISD2 appears to provide that recognition, by highlighting the need for international sharing[49] and "actively support[ing] and encourag[ing]" non-NIS entities to participate.[50]

By requiring information sharing to satisfy tests of public interest (via Article 49(1)(d)) and individual risk/benefit (via Article 6(1)(f)) this approach meets the needs of both internet users and internet defenders. Compared to the current patchwork: external victim notification remains a voluntary activity that teams can prioritise among other activities; community notification can consider the benefits to direct recipients and the wider public benefit from more secure systems, networks and data; collaborative analysis can include all relevant partners, using appropriate community rules and safeguards rather than a

---

[49] European Commission, NISD2, *supra* n. 1, Recital 26.

[50] *Ibid*., Recital 68.

complex mesh of bilateral contracts. NISD2 specifically recognises the global Traffic Light Protocol,[51] "used in almost all CSIRT communities" to indicate confidentiality rules.[52] These teams routinely use encryption and strong authentication to protect shared data:[53] another example of the incentive not to assist attackers aligning perfectly with data protection requirements. Even the *Schrems II* obligation,[54] to assess the risk of state interference with transferred data, may be more easily satisfied using an "internet protection" lens than a "data protection" one. Many more states have supported the UN Global Group of Experts' 2015 norm 4 of non-interference with Incident Response Teams than are ever likely to achieve an adequacy decision.[55,56] Further safeguards – such as adequacy decisions and model contracts – can, of course, be added to this basic framework where they are available. But their absence should not be a barrier to sharing.

7 Conclusion: Improvement by Iteration

This iterative approach – using experience of a general data protection law to inform a later, sector-specific one, then reading that refinement back into the general law – is not new. In network and information security alone it has occurred at least three times: the 2009 revision of the ePrivacy Directive gave

---

51 FIRST, "TLP", *supra* n. 21.

52 European Commission, NISD2, *supra* n. 1, Recital 6.

53 Nevil Brownlee and Erik Guttman, "Expectations for Computer Security Incident Response" (Internet Engineering Task Force, RFC 2350, June 1998), available at https://www.ietf.org/rfc/rfc2350.txt (accessed 8 March 2021).

54 *Data Protection Commissioner [Ireland] v Facebook Ireland Ltd and Maximillian Schrems*, Case C-311/18, ECLI:EU:C:2020:559.

55 CCDCOE, "2015 UN GGE Report: Major Players recommending Norms of Behaviour, Highlighting Aspects of International Law" (2015), available at https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/ (accessed 8 March 2021).

56 Tanczer et al, "CSIRTs and Global Cybersecurity", *supra* n. 46, pp. 61-62.

explicit permission for incident response by network operators, whose logic was read back into the Data Protection Directive – at least for website operators – in the case of *Breyer v Germany*.[57] The same revision informed Recital 49 of the GDPR, which extended the permission to "public authorities, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), … and providers of security technologies and services".[58] That permission became a duty on all data controllers and processors, via regulatory guidance on the GDPR breach notification provisions.[59]

In the same way, NISD2 and its Articles 26 and 27 should inform how the GDPR is applied to information sharing to defend networks, systems, data and users. This should ensure all data controllers, data processors and data subjects benefit from, and trust in, the "effective cybersecurity measures" enabled by a coherent, comprehensive information sharing framework.[60]

---

[57] *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, ECLI:EU:C:2016:779.

[58] GDPR, *supra* n. 25, Recital 49.

[59] Article 29WP, "Personal Data Breach Notification", *supra* n. 48. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052, p. 12.

[60] European Commission, NISD2, *supra* n. 1, p. 5.