INTERSECT POLICY BRIEF 4

Security measures in the GDPR & the NAP judgement (C-340/21)

Date 17/12/2024
Authors Suzanne Nusselder

Tilburg University
Understanding Society

Publication

Tilburg Institute for Law, Technology, and Society (TILT)
www.tilt.nl

Contact

Suzanne Nusselder
S.c.nusselder@tilburguniversity.edu

1 The security of personal data: setting the scene

In the early beginnings, cybersecurity and data protection were addressed together.[1] Over time, they evolved into separate domains and regulatory frameworks with cybersecurity being established as its own policy domain in 2013.[2] Nevertheless, they remain closely related and can be mutually reinforcing. (Cyber)security is a core principle of the EU's data protection legal framework that has stood the test of time. In addition to the array of cybersecurity specific legal instruments that have been adopted in recent years, data protection law, and more specifically the security requirements laid down therein, can play an important role for strengthening cybersecurity as well.

Similar to its predecessor the Data Protection Directive (DPD)[3], the GDPR includes security as one of the data protection principles.[4] The integrity and confidentiality principle (also referred to as the security principle) is further concretised in Section 2 of Chapter IV GDPR which consists of three provisions regarding the security of personal data: Article 32 GDPR which concerns the security of processing; Article 33 GDPR regarding the notification of a personal data breach to the supervisory authority; and Article 34 on the communication of a personal data breach to the data subject.

2 Appropriate technical and organisational measures

2.1 Article 32 GDPR

Article 32 GDPR lays down an obligation for both data controllers and data processors to implement "appropriate technical and organisational measures to ensure a level of security appropriate to the risk"[5], thereby stipulating the general rules for ensuring the security of personal data processing. Rather than providing a list of specific technical and organisational measures (TOMs) that must be implemented, Article 32(1) GDPR provides some minimum guidance and some examples of TOMs. It specifies key factors to be taken into account when deciding on appropriate TOMs to implement, such as "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons".[6] Examples of TOMs are provided in Article 32(1)(a)-(d) GDPR and include the pseudonymisation and encryption of personal data; measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of TOMs for

[1] Commission of the European Communities, 'Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security, COM(90) 314 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990DC0314; Maria Grazia Porcedda, 'The EU Cybersecurity Policy', *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis* (Bloomsbury Publishing 2023), p43.
[2] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', JOIN(2013) 1 final.
[3] 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 (repealed), OJ L 281/31, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
[4] Article 5(1)(f) of the Regulation (EU) 2016/679 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), OJ 2016 L 119 (hereafter GDPR).
[5] Article 32(1) GDPR.
[6] Article 32(1) GDPR.

ensuring the security of the processing.[7] Overall, the data controller thus has quite some leeway when selecting TOMs. Notwithstanding, TOMs ought to be chosen in accordance with the 'state of art'. However, no lists of TOMs compliant with the state of the art exists.

2.2 The NAP judgement

In December 2023, the Court of Justice of the European Union (CJEU), for the first time, ruled on a case specifically dealing with the security requirements laid down in Article 32 of the GDPR in *Natsionalna agentsia za prihodite* (NAP case).[8] The importance of this long-anticipated judgement is not easily overstated.

Let us first take a closer look at the circumstances leading to the NAP case. In 2019, the Bulgarian National Revenue Agency (Natsionalna agentsia za prihodite, NAP) was the victim of a hacking attack leading to a massive data breach.[9] The NAP data breach affected around 6 million Bulgarian and foreign nationals whose personal data, including home addresses, tax and social security information, was leaked. In the aftermath, several hundreds of them brought legal action against the NAP seeking compensation for non-material damages suffered following from the unauthorised disclosure of their personal data. One of these proceedings for damages led to the NAP case in which the Bulgarian court referred several preliminary question to the CJEU.

The CJEU ruled that the mere occurrence of a personal data breach, in this case the unauthorised access to or disclosure of personal data by a third party, is not in itself sufficient for finding that the TOMs implemented by the data controller are not appropriate.[10] The CJEU stressed that the GDPR establishes a risk management system reliant on TOMS which is intended to mitigate personal data breaches rather than alleging to eliminate them altogether or purporting that this can even be done.[11] In essence, the GDPR establishes an obligation of means rather than an obligation of result.[12] Thus, the occurrence of a personal data breach does not necessarily entail that an infringement of the GDPR ensued. However, the fact that the personal data breach occurred as a consequence of a cyberattack does not absolve the data controller from their responsibilities under the GDPR either. Rather, the exemption of liability is strictly limited to those instances where the data controller can establish that there is no causal link between the possible breach of the GDPR and the damages suffered by the data subject.[13]

Furthermore, the CJEU held that the (in)appropriateness of TOMs must be assessed *in concreto*.[14] The national court must carry out a substantive assessment in order to evaluate the substance and appropriateness of the TOMs implemented by the data controller.[15] This two-step substantive assessment starts with a concrete assessment of the likelihood and severity of a data breach and the

[7] Article 32(1)(a)-(d) GDPR.
[8] Case C-340/21, VB v Natsionalna agentsia za prihodite, 2023, ECLI:EU:C:2023:98. The discussion of the NAP judgement is based on a previously published case note: S Nusselder, 'A Closer Look at the GDPR's Security Requirements and Assessing the (In)Appropriateness of Technical and Organisational Measures (TOMs)' (2024) 10 European Data Protection Law Review 111.
[9] Catalin Cimpanu, 'Hacker steals data of millions of Bulgarians, emails it to local media', ZDNET (15 July 2019), available at: https://www.zdnet.com/article/hacker-steals-data-of-millions-of-bulgarians-emails-it-to-local-media/
[10] C-340/21, VB v Natsionalna agentsia za prihodite, para 39.
[11] Ibid, para 29.
[12] Lee A Bygrave, 'Security by Design: Aspirations and Realities in a Regulatory Context' (2022) 8 Oslo Law Review 126, 167.
[13] C-340/21, VB v Natsionalna agentsia za prihodite, para 72.
[14] Ibid, para 47.
[15] Ibid, para 45.

potential consequences for the rights and freedoms of the data subjects.[16] Next, the appropriateness of TOMs is evaluated by looking at factors such as the state of the art, the cost of implementation and the nature, scope, context and purposes of the data processing in question.[17] The assessment encompasses both the nature and the content of the measures, the manner in which they were applied as well as the practical effect on the level of security.[18] Importantly, the burden of proof for demonstrating the appropriateness of the implemented TOMs lies with the data controller in question, following the principle of accountability.[19] The appropriateness of TOMs cannot be deduced from an expert report.[20]

Rooted in the wording of the GDPR, the NAP judgement contains few surprises. It provides some additional clarity on the GDPR's security requirements and the (in)appropriateness of TOMs implemented by the data controller and processor to ensure security. Nevertheless, some open questions persist, such as the notion of 'state of the art', a crucial component for the (in)appropriateness of TOMs, which remains underdefined. Finally, the NAP judgement makes an important contribution to the developing strand of jurisprudence concerning non-material damages, which will be discussed in the Section 3.

3 Non-material damages for security breaches

3.1 The NAP judgement

The final issue under consideration in the NAP case concerned the question of non-material damages following a personal data breach. The CJEU recalled its previous jurisprudence on non-material damages and reiterated the three cumulative conditions for the right to compensation laid down in Article 82(1) GDPR put forth in *Österreichische Post*.[21] These cumulative conditions entail, 1) the existence of damage which has been suffered; 2) the existence of an infringement of the GDPR; and 3) a causal link between that damage and the infringement.[22] The CJEU also reaffirmed that the compensation for non-material damage cannot be subject to the condition that the damage has reached a certain level of seriousness.[23]

In the NAP case, the CJEU ruled that the fear, anxiety, and emotional distress experienced by a data subject concerning the possible (future) misuse of his or her personal data by third parties following an infringement of the GDPR can constitute non-material damage.[24] The data subject negatively affected by the infringement is required to demonstrate that those consequences constitute non-material damage. Importantly, the data subject's fear must be well-founded and specific, which is to be checked by the national court.[25]

[16] Ibid, para 42.
[17] Ibid, para 42.
[18] Ibid, para 46.
[19] Ibid, para 57.
[20] Ibid, para 64.
[21] Case C-300/21, *Österreichische Post*, 2023, ECLI:EU:C:2023:370.
[22] Case C-300/21, *Österreichische Post*, para 32.
[23] C-340/21, VB v Natsionalna agentsia za prihodite, para 78.
[24] Ibid, para 86.
[25] Ibid, para 85.

3.2 The MediaMarktSaturn judgement

Shortly after the NAP case, the CJEU again considered the question of non-material damages in relation to Article 32 GDPR in the MediaMarktSaturn case.[26] This case concerns the question of compensation for non-material damages allegedly suffered by the data subject following the disclosure of their personal data to an unauthorised third party due to an error made by an employee of the data controller. The MediaMarktSaturn judgement confirmed several key elements of the NAP judgement.

The CJEU reaffirmed that the appropriateness of TOMs implemented by the controller must be assessed in a concrete manner, taking into account the various criteria outlined in Article 32 GDPR as well as the data protection needs specifically inherent in the processing concerned and the risks arising therefrom.[27] The CJEU also reiterated that the obligation on the data controller is to mitigate the risks of personal data breaches rather than an obligation to prevent all personal data breaches.[28] Again, the mere occurrence of the unauthorised disclosure of or access to personal data is not sufficient, in itself, for finding the TOMs implemented by the data controller to be inappropriate.[29]

Furthermore, the CJEU held that Article 82 GDPR, and the right to compensation for material and non-material damages provided for therein, fulfils a compensatory function, and not a punitive one.[30] As such, the severity of the GDPR infringement causing the damage in question does not impact the amount of compensation granted.[31] The amount of financial compensation to be awarded based on Article 82 GDPR is such as to allow for the damage actually suffered as a result of the infringement to be compensated in full.[32]

3.3 Going forward

On a positive note, the broad interpretation of non-material damages by the CJEU in the NAP case will offer redress to data subjects following a data breach. On the flipside, data breaches may become increasingly expensive for data controllers. As such, there is a need for a reasonable threshold for controllers to demonstrate that they have complied with the security obligations laid down in the GDPR. The mere occurrence of a personal data breach does not necessarily entail that the data controller failed to comply with the GDPR's security obligations. Instead, compliance with Article 32 GDPR and thus the appropriateness of the TOMs implemented by the data controller is to be evaluated in a concrete manner by national courts. The notion of 'state of the art' plays a crucial role when it comes to the appropriateness of TOMs. As detailed in Article 32(1) GDPR, data controller has to select TOMs according to, inter alia, the state of the art. This remains a challenging task, at least in part due to the lack of much needed guidance regarding state-of-the-art security measures and the role that codes of conduct, certification and technical standards can play.

[26] Case C-678/21, BL v MediaMarktSaturn Hagen-Iserlohn GmbH, 2024, ECLI:EU:C:2024:72.
[27] Ibid, para 38; C-340/21, VB v Natsionalna agentsia za prihodite, paras 30-32.
[28] Case C-678/21, BL v MediaMarktSaturn Hagen-Iserlohn GmbH, para 39; C-340/21, VB v Natsionalna agentsia za prihodite, paras 33-38.
[29] Case C-678/21, BL v MediaMarktSaturn Hagen-Iserlohn GmbH, para 40; C-340/21, VB v Natsionalna agentsia za prihodite, para 39.
[30] Case C-678/21, BL v MediaMarktSaturn Hagen-Iserlohn GmbH, para 47.
[31] Case C-678/21, BL v MediaMarktSaturn Hagen-Iserlohn GmbH, para 48; C-667/21, ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, 2023, EU:C:2023:1022, para 86-87.
[32] Case C-678/21, BL v MediaMarktSaturn Hagen-Iserlohn GmbH, para 50.

According to Article 32(3) GDPR, "adherence to an approved code of conduct as referred to in Article 40 [GDPR] or an approved certification mechanism as referred to in Article 42 [GDPR] may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of [Article 32 GDPR]". To date, there are no approved codes of conduct or certification mechanisms regarding the security requirements pursuant Article 32 GDPR.[33]

4 Notification of personal data breaches

In the case of a personal data breach, the GDPR lays down provisions regarding the notification of such a breach to the supervisory authority (Article 33 GDPR) and the communication of the personal data breach to the data subject (Article 34 GDPR). Pursuant to Article 33 GDPR, the data controller shall notify the competent supervisory authority of the personal data breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it". Notification is not required when the personal data breach is "unlikely to result in a risk to the rights and freedoms of natural persons". Furthermore, the data controller is required to document any personal data breaches including its effects and the remedial action taken.[34] According to Article 34 GDPR, if the personal data breach is likely to result in a "high risks to the rights and freedoms of natural persons", the data controller is obliged to communicate the personal data breach to the affected data subjects.

There is extensive guidance on the topic of data breach notifications.[35] For instance, the EDPB guidelines 9/2022 is a valuable resource when it comes to personal data breach notification under the GDPR explaining when to notify, what information to provide and how to document personal data breaches.[36] The 01/2021 EDPB guidelines provides more "practice-oriented, case-based guidance" addressing practical issues arising with personal data breach notification.[37]

It is important to note that, in addition to and separate from the notification requirements laid down in Article 33 and 34 GDPR, cybersecurity incidents may need to be notified to the relevant competent authorities pursuant to other applicable legislation, such as for instance the NIS 2 Directive.

[33] EDPB codes of conduct register, available at: https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en?page=1
EDPB certification mechanisms register, available at: https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en
[34] Article 33(5) GDPR.
[35] Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, available at: https://ec.europa.eu/newsroom/article29/items/612052.
EDPB, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, adopted on 14 December 2021, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en.
EDPB, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, adopted on 28 March 2023, available at: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.
[36] EDPB, Guidelines 9/2022.
[37] EDPB, Guidelines 01/2021, p5.