EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 4/2024, 23 January 2024
Tags: Case 340/21, Natsionalna agentsia za prihodite
Topics: Data protection and digital governance, data retention, Legal remedies

The GDPR as a cyber risk management system: the ECJ cautiously tackles data breaches in the NAP case

By Maria Grazia Porcedda

When the Bulgarian National Revenue Agency (Natsionalna agentsia za prihodite or the 'NAP') suffered a malicious data leak in 2019, it joined the growing ranks of organizations affected by cyberattacks. With security often being an afterthought in cyberspace, data breaches have become a drawback/reality of networking. Beneath the glitter of digitalization and the data economy lie illicit markets, "the central commodity of which is stolen data". The NAP data breach, which affected 6 million Bulgarians and foreign citizens, sparked several actions to recover damages such as the proceedings that led to the Natsionalna agentsia za prihodite (NAP) case. While *Breyer* was technically the first ECJ judgment linked to a cybersecurity incident, the *NAP* case is the first to deal with data breaches and 'cyberoffending' in the context of the GDPR. Its importance cannot be overstated: proceedings brought by individuals against the Irish Health Service Executive in the aftermath of a 2021 HSE ransomware attack have been stayed pending the outcome of this and similar cases.

That a request for preliminary ruling landed on the Court's registry only in 2021, notwithstanding exposure of data controllers to breaches for two decades, owes to the belated inclusion of cybersecurity within the scope of EU law. Concerning data breaches in particular, discrete provisions have been embedded into existing instruments over the past 15 years, creating an incoherent regulatory patchwork. The first was introduced with the 2009 amendment to the e-privacy Directive, which however had a limited scope of application and no dedicated liability regime, unlike the GDPR, which provides for a horizontal system of civil law remedies. It is the interpretation of this system of remedies that gave rise to a request for preliminary ruling by the Bulgarian Varhoven administrativen

sad (Supreme Administrative Court), together with the rules on the responsibility of data controllers whose data have been breached. The request was made in proceedings brought by VB to claim compensation for non-material damage suffered due to the NAP's alleged failure to fulfil its legal obligations as a data controller.

In a judgment delivered on December 14th, the Court blended literal, systemic and teleological reasoning to find that a cyberattack does not automatically exonerate data controllers from the responsibility incumbent on them under the GDPR, nor that such an attack, on its own, demonstrates the inappropriateness of the technical and organizational measures in place. The controller bears the burden to prove the appropriateness of such measures, which must be assessed by a national court without necessary recourse to expert evidence. Fear of future misuse of personal data can constitute non-material damage giving rise to compensation under Art 82 GDPR.

Partly novel matters, parsimonious reasoning

In answering the partly novel matters raised by the *Varhoven administrativen sad*, the CJEU follows the Opinion to the case, but adopts a more cautious reasoning than AG Pitruzzella's. The AG made statements on cybercrime and commented on the architecture of the GDPR to clarify the nature of its liability regime, distinguishing between upset and inconvenience suffered by data subjects and casting the adoption of Technical and Organisational Measures (TOMs) as a balancing exercise of rights carried out by the controller. The Court's reasoning rests on the reconciliation of the ultimate goal of the GDPR - a high level of protection of the rights and freedoms of data subjects - with the reality of data processing risks and inherent cyber-insecurity.

The GDPR as a (cyber) risk management system (Q1)

The Court finds that, since the GDPR is a risk management system premised on TOMs that was intended to mitigate risks rather than eliminating them (paras 29 and 38), the occurrence of a breach is not enough to demonstrate that TOMs implemented by a data controller under arts 24 and 32 GDPR are inappropriate (para 31). To argue the point, the Court engages in an autonomous and uniform interpretation of Arts 24 on responsibility of the controller and 32 on the security of processing (paras 23-28). These, as supplemented by recitals 74, 76 and 83, provide criteria for the appropriateness of TOMs, which must be assessed concretely, having regard to the needs and risks of processing (paras 30-36).

The literal interpretation is backed by context and teleology: to equate a cyberattack with the inappropriateness of TOMs and assume the controller is obliged to prevent attacks would deprive the controller of its ability to adduce evidence and defy the logic of Arts 24, 32 and 82(2) and (3), with the latter providing an exemption from liability if the controller can demonstrate not to be responsible 'in any way' (paras 31, 37-38).

The protection of the GDPR depends on the security measures adopted by the data controller, who is liable save for no causal link between the breach and damages (Q3i and 4)

The objective of the GDPR to provide a high protection to the rights and freedoms of data subjects supports a broad interpretation of the principle of accountability and an inversely strictly limited interpretation of the controller's exemption from liability (para 73). To preserve the effectiveness of Art 82(1), it is the controller who bears the burden of proving the appropriateness of TOMs in light of the security principle enshrined in Art 5(1)(f) and the rules of general application contained in Arts 24(1) and 32(1) at stake in actions for damages (paras 50-52). Although controllers cannot be expected to prevent attacks, they must be encouraged to do everything in their powers because 'the protection of the GDPR depends on the security measures adopted' (para 55).

An infringement of the GDPR caused by a 'third party' within the meaning of Art 4(10) – such as cybercriminals responsible for breaching personal data– can be made possible by the controllers' failure to comply with their obligations (para 71). Under a strictly limited interpretation of the clause 'in any way' within Art 82(3), the controller is exempt from liability if there is no causal link between a possible breach and the damage suffered (paras 70-72).

TOMs' appropriateness is to be *substantively* checked by a national court and cannot be deduced from an expert report (Q2 and 3ii)

Although the controller has discretion in the adoption of TOMs, the evaluation of the appropriateness of the 'level of safety' of a TOM (para 41) to the risk of processing is liable to a two-stepped substantive assessment by a national court aimed at ensuring effective protection (paras 42, 44). Based on the wording of Art 32 and with a nod to Portuguese written observations (note 17), a review begins with a concrete assessment of the likelihood and severity of a data breach and potential consequences for the rights and freedoms of natural persons (para 42). It is followed by an assessment of the appropriateness of TOMs based on composite factors (state of the art, the costs of

implementation and the nature, scope, context and purposes of that processing) (para 42). The need for a substantive assessment that takes account of circumstances, evidence and statutory criteria is supported by a purposive reading of the GDPR in light of expectations for effective protection and availability of judicial remedies contained in recitals 11, 74, Art 79 (1) and recital 11 (paras 45-46).

Since the national Court's concrete analysis must encompass the risks associated with the processing and suitability of the nature, content and implementation of TOMs, it is not surprising that the ECJ finds against a national procedural rule systematically requiring an expert report (para 64). In keeping with the principle of procedural autonomy discussed in Österreichische Post AG, it is for the legal system of Member states to discipline the admission and probative value of evidence in the absence of relevant EU provisions (para 60). A national rule systematically requiring the production of an expert report violates the principle of effectiveness, whereby it cannot be excessively difficult or impossible to exercise a right, as established in Österreichische Post AG (para 59, 61). A report may be superfluous, for instance vis-à-vis a recent review of compliance with the TOM by a supervisory authority, or else detrimental to a court's objective assessment (para 62). With the objective in mind of the right to an effective judicial remedy, an impartial tribunal 'cannot confine itself to…a deduction' (para 63).

Well-founded and specific fear of future data misuse can be classed as non-material damage (Q5)

The Third Chamber judges also uphold the three conditions for compensation identified in Österreichische Post AG (para 77) and find that the fear of potential, future misuse of data following a hack can, in light of the ultimate objective of the GDPR, constitute non-material damage. A broad interpretation of the concept of damage is supported by the wording of Art 82(1), which does not distinguish between actual and potential damage, and of recitals 146 and 85, which specifically refers to the loss of control of one's data (paras 79-82). The finding of fear as non-material damage rests on national courts (para 84). Unlike the AG, the ECJ does not suggest how to distinguish between upset and inconvenience, but solely notes that fear must be well-founded in a specific case and for a specific data subject (para 84).

Establishing 'well-founded' fear in practice may prove contentious. Ireland's written observations (note 39) point to the significant impact of granting compensation to every person affected by a public sector data breach, in light of limited resources that should be directed, among other, to the improvement of personal data security – a relevant remark in light of the 2021 HSE cyberattack.

Notable absences: privacy and Charter-based considerations on the essence

The judgment should contain few surprises to those familiar with the security requirements of the GDPR, insofar as the analysis is parsimoniously grounded in the wording of the Regulation. The judgment contains measured remarks on the relationship between the GDPR, safety and security premised on the impossibility of eliminating cybercrime, a well-founded stance in face of the technological reality. While the preservation of the rights and freedoms of data subjects features prominently in the judgment, neither *The Varhoven administrativen sad* nor the ECJ rely on the Charter of Fundamental Rights (CFR). Shunning the Charter may help against 'privacy thinking', but could also constitute a missed opportunity.

There are open questions as to the centrality of 'security' to the right to the protection of personal data enshrined in Art 8 CFR and its essence. Following *Digital Rights Ireland* and *Opinion 1/15*, the essence is upheld by the presence of rules intended to ensure, inter alia, the security, confidentiality and integrity of processed personal data, and to protect it against unlawful access and processing. This appears to be a procedural understanding of the essence disconnected from the appropriateness of rules –and, down the line, TOMs– to ensure the security, confidentiality and integrity of data emphasized instead by the NAP case. The disconnect is fundamental insofar as a breach of the essence constitutes an automatic violation of the right to data protection, whereas the adoption of inappropriate TOMs constitutes a breach of the GDPR exposing the controller to penalties. What link can be established between the inclusion of rules on security, integrity and confidentiality in a legal basis and the adoption of appropriate TOMs by a data controller? This invites an analysis that exposes a dangerous loophole in the architecture of data protection law.

On the GDPR, TOMs and loopholes: appropriate TOMs should be chosen on a coordinated basis at EU level

Among the points of the AG not taken up by the ECJ are comments on the nature of the 'state of the art' (SoA) and 'certification'. The SoA appears in Art 25 on data protection by design and Art 32 on security of processing and the Opinion refers to the 'solutions that the state of the art in science, technique, technology and research offers at the time, also taking into account… the implementation costs' (para 32). The SoA refers to the most advanced state of technology and is undefined, yet crucial to TOMs and the architecture of the GDPR.

In a nutshell (with a full explanation in a monograph and a concise article), TOMs must be chosen according to the SoA. However, there is no catalogue of TOMs compliant with the SoA, primarily for two reasons: because of the paradigm of technology neutrality central to the GDPR, and because the GDPR addresses technological use, rather than technology development. Technical measures tend to be software-based, and software has traditionally not been part of the New Legislative Framework, which has historically set parameters for technology development, further contributing to delays in dealing with integrity and confidentiality concerns notwithstanding their importance to safety. Think of cyberattacks against critical infrastructure and cybercrime-as-a-service, which has significantly lowered the barriers to entry for cyber-offenders.

The SoA rests entirely on the market-based mechanism of standardization in which Big Tech companies, including major addressees of the GDPR, play a central role. The burden of choosing TOMs rests on controllers; note that major tech-developers are likely to have contributed to both the creation of standards and TOMs, while other controllers will simply be TOM-adopters. Selection of TOMs appropriate for security is especially challenging given expert opinion that cybersecurity is a market for lemons. The EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification have been reportedlymet with criticism for the divide between regulatory expectations and industry practice.

Note that, because the GDPR is not part of the New Legislative Framework, any standards adopted, including the 2021 CEN-CENELEC standard, are not European Mandatory Standards, are not for publication in the OJ and do not create a presumption of conformity. Certification against such standards should therefore be treated with caution as should the ability of related certification to fulfill data controllers' accountability requirements. This is separate from supervisory authority-based certification mechanisms, which suffers from specific challenges.

Against this background, to task exclusively national courts with the decision of what TOMs are appropriate to ensure security of processing on a case-by-case basis appears to be particularly problematic and liable to creating fragmentation in the implementation of the GDPR. While the solution does not have to be tech-specific at legislative level, the evaluation of technological appropriateness in the face of security risks would best be coordinated by Member States at EU level, by a new mechanism that involves authorities with expertise across legislative frameworks with cybersecurity relevance.

In the meantime, to the extent that rules on the security, integrity and confidentiality of data - the meaning of which are determined by the market - are disconnected from the appropriateness of the TOMs they are supposed to incentivise, the essence of the right to the protection of personal data will remain market-driven, to the detriment of a high level of protection of the rights and freedoms of data subjects.