Summary
Data breach notification duties: Enhancing the protection of personal data under the General Data Protection Regulation

By Lina Jasmontaitė-Zaniewicz

The obligations to notify personal data breaches, as outlined in Article 33 (*Notification of a personal data breach to the supervisory authority*) and Article 34 (*Communication of a personal data breach to the data subject*), upon their introduction in the General Data Protection Regulation (GDPR), joined the extensive list of attempts by legislature to secure individuals' rights and their (personal) data (Chapter 1). The current understanding of these obligations is rather narrow and limited to an often-pragmatic business perspective.

In my attempt to provide a comprehensive understanding of these obligations, I conducted an extensive review of literature, EU policy documents and Court of Justice of the EU case law. In addition, I examined 45 decisions by data protection authorities (DPAs) from different EU Member States and Norway in cases concerning personal data breaches which were issued from May 2018 to July 2022. The analysis of the latter allowed me to make some observations regarding trends and challenges faced by controllers and DPAs, which can serve as building blocks for future research.

Beginning with a historical context in which the obligation to notify competent authorities and individuals regarding personal data breaches, first emerged in the EU, I analysed EU policy documents and the ePrivacy Directive, as amended in 2009 (Chapter 2). The historical context laid the foundation for the discussion of the definition of a personal data breach under the GDPR. In general, a broad definition is preferred to an overly narrow one in order to capture a wide spectrum of personal data breaches (Chapter 3). I propose that the key elements in the definition are: 1) processing; 2) negative effects (on personal data), and 3) personal data.

I examine the objectives assigned to personal data breach notifications to DPAs and individuals by key stakeholders, including the European Commission, the European Data Protection Supervisor, the Article 29 Working Party (replaced by the European Data Protection Board (EDPB)) and DPAs (Chapter 4). They range from high level, policy orientated objectives (e.g., reduce information asymmetry) to practical implications (e.g., enhance transparency over processing operations). These multiple objectives feed into the role that data breach notifications play in the EU data protection framework. However, they lack a supporting structural governance mechanism.

While commonly thought to be a data security measure, I argue that the reach of notification duties extends beyond the security obligations laid out in Article 32 (Chapter 5). I explain that data breach notification obligations enhance personal data protection indirectly (e.g., through measures controllers are advised to implement in advance) and that they are designed to relate to security measures. After analysing the guidelines issued by the EDPB (Chapter 6) and controller practices (Chapter 7) concerning disclosure requirements concerning personal data breaches, I observe that there is evidence which allows for the argument that controllers often interpret their obligations which arise in the aftermath of personal data breaches differently than the regulators, despite the existence of a reasonably solid post-breach risk assessment framework (e.g., communication to individuals remains rare). I demonstrate that there are specific situations where the non-adherence to the core principles of the GDPR results in a personal data breach (Chapter 8).

The legal debates on the meaning of personal data breaches and their notifications are set to continue in light of other GDPR provisions. In particular, Article 82 which grants individuals the right to compensation for GDPR infringements (Chapter 9). In conclusion, I posit that in today's complex world, information concerning personal data breach notifications and subsequent DPA decisions could enhance the protection of individuals and their personal data long into the future (Chapter 10).

***