# Remedying Data Vulnerability in a Global World: A Comparison of the European Union and Japan's Approach to Compensation for Data Breaches


**Barbara Milillo**

**Abstract** The notion of digital vulnerability can be defined as the exposure of individuals to risks arising from their engagement with online activities. The dissemination of personal information in the digital realm, often resulting from the misuse or violations of privacy, underscores the need for an understanding of digital vulnerability as a multifaceted phenomenon that perpetually shapes the landscape of privacy protection. This has led to privacy being recognized as an essential and vital right, continuously shaped and challenged by technological developments and judicial interpretations across various legal traditions. The purpose of this paper is to explore the data protection remedies developed by the Japanese legal system, and to investigate the relevant insights for the data protection policy and the safeguard of vulnerable subjects that Japanese judicial decisions can offer to Europe. To this purpose, the paper will highlight key elements of the Japanese and European approach in mitigating privacy-related vulnerabilities and will survey their respective limitations, focusing in particular on the impact of tort law on privacy rights and on data protection policy.

**Keywords** Data protection · Tort law · Japanese law · EU law · GDPR

## 1 Introduction

A growing body of literature recognizes the significance of the right to privacy amidst technological developments. In the digital realm, the right to privacy is continuously subject to a growing number of threats (such as data mining, automated decision-making, profiling). In this context, institutions across many legal systems have recently been working to guarantee a broader protection of personal information. However, in a world of increasing digital interactions, which at the same time

B. Milillo (✉)
Department of Legal Science, University of Udine, Udine, Italy
e-mail: barbara.milillo@phd.units.it



C. Crea and M. Infantino (eds.), *Remedies to Digital Vulnerability in European Private Law*, https://doi.org/10.1007/978-3-032-19720-7_15

increase the risks associated with the misuse of data, it can be argued that, inasmuch as privacy is concerned, every individual is vulnerable. The protection of digital privacy therefore calls for new and flexible legal solutions.

This is how privacy and vulnerability are interconnected in the digital world. The notion of digital vulnerability has recently received considerable critical attention. The idea of vulnerability is part of the data protection environment, but it is usually employed to refer to specific categories of individuals, such as the elderly, children or people affected by disabilities. Nevertheless, the notion that vulnerability is an inherent characteristic of all data subjects, including in the perspective of data protection, is currently growing in the state-of-the-art research.[1]

The specific objective of this paper is to examine the role of vulnerability in the data protection realm by performing a comparative analysis between the European Union (EU) and Japan's different approaches to the issue. More in particular, the main purpose of the paper is to investigate how the EU and Japanese law address the harm caused by data breaches through tort law.

The paper is composed of three parts. Section 2 will briefly examine the existing legislation in the data protection field within the context of both the EU and Japan. Section 2.1 will outline the main EU legal text on privacy, that is, the General Data Protection Regulation (EU) 2016/679 (GDPR). Section 2.2 will then analyse the Japanese approach to privacy and to data protection, with particular emphasis on the Japanese Act on the Protection of Personal Information (APPI). After this brief comparison, Sect. 3 will explore the history and contents of the Adequacy Decision (AD) on Japan adopted by the European Commission in 2019. The AD recognized that the Japanese legislation guarantees a level of data protection similar to the European standard, as a direct consequence of the 'Brussels Effect'.[2] As it will be highlighted, the decisional process underlying the AD was characterized by a significant amount of institutional dialogue between the European Commission and the Protection of Personal Information Committee of Japan. Finally, Sect. 4 will offer a comparative analysis of the Japanese Supreme Court's Benesse Case in connection with the decisions of the Court of Justice of the European Union (CJEU), formerly known as the European Court of Justice (ECJ), on compensation in cases of infringements of data protection law. The comparison will shed light on the three core aspects that are central in the Japanese Supreme Court's judgment on the case: firstly, the recognition of mental distress as a compensable harm; secondly, the factors considered in determining the award; thirdly, the reliance on apology as a form of compensation. Section 5 concludes by reflecting on the key elements that the EU can learn from the Japanese tort-based approach and its flexibility vis-à-vis cultural expectations. While EU law has so far emphasized proof of harm and the need for a uniform interpretation of the GDPR across Member States, Japan places a higher value on a social responsive form of redress. Nevertheless, the comparative analysis of the EU and Japanese legal approach to privacy harms also shows a considerable convergence

[1] *See* Malgieri (2023).

[2] *See* Bradford (2020).

in their recognition of the individual as a vulnerable subject worthy of increased protection vis-à-vis the new digital threats.

## 2 Data Protection Legislation in the EU and in Japan

This section offers a preliminary overview of data protection regulation within the EU and Japan, serving as a foundation for the subsequent analysis of the relevant case law on tort liability and data breaches. More in particular, Sect. 2.1 will summarise the main contents of the GDPR, with a focus on the most important provisions pertaining to data breaches and the compensation of the harm caused by them. Section 2.2 will subsequently examine the right to privacy in Japan and the Japanese data protection regime, in particular after the reform that followed the AD of 2019.

### *2.1 The EU: Setting the Global Standard of Data Protection*

European national jurisdictions developed their own approach to privacy, particularly through tort law remedies, since the 1950s. The protection of the private sphere has been widely recognized by European private laws through tort law litigation, even if the foundation for the right to privacy and its declinations (such as the right to be forgotten, the right to one's imagine, and so on) has been varied across legal systems.[3] Nowadays the current European regime of protection of personal data has been largely built by the EU and finds its most important source in the GDPR.

The GDPR confirmed and replaced the approach of the Data Protection Directive 1995/46/EC previously into force. The Directive 1995/46/EC, which was significantly inspired by the principles set out by the OECD Privacy Guidelines of 1981 and by the Council of Europe's Convention of Privacy of 1980, was the first legislation in the European context that focused on the protection of personal data.[4] The Directive 1995/46/EC already obliged all Member States to enact data protection frameworks in line with its provisions, as to remove the obstacles to the free flow of information within the EU and, at the same time, to promote the protection of the fundamental right to data protection.[5] In 2000, the Charter of Fundamental Rights of the EU recognized both the right to the respect of personal life[6] and the right to the protection of personal data and their fair processing[7] as fundamental rights within the EU. But it was the GDPR that established a global standard for the protection

[3] Brüggemeier, Colombi Ciacchi, O'Callaghan (2010, 569–570).

[4] Casagran (2017, 37).

[5] McGeveran (2016, 969).

[6] Charter of Fundamental Rights of the EU (2012), Article 7.

[7] Charter of Fundamental Rights of the EU (2012), Article 8(1)(2).

of personal information, initiating a worldwide reform of data protection regulation. This push towards a global standard in privacy regulation has been notoriously considered one of the most powerful illustrations of the EU's so-called 'Brussels Effect'. The Brussels Effect refers to the ability of the EU legislation to influence sectorial regulation on a global scale, by relying on the market power of the EU and on the interest of multinational foreign companies to adopting standards adapted to the European market, even if more stringent.[8]

The central focus of this section is the treatment in the GDPR of data breaches and of the right to compensation in cases of privacy infringement. This is necessary to appreciate the legal bases of the decisions of the CJEU on these matters that will be examined in Sect. 4.

The first key aspect concerns the regulation of data breaches. The definition outlined by the GDPR is found in article 4(12), which refers to 'personal data breach' as: "[a] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". In the event of a personal data breach, the GDPR imposes a specific obligation on the data controller to notify the breach to the supervisory authority (Article 33); the same obligation arises vis-à-vis data subjects, but only if there is a "[a] high risk to the rights and freedoms of natural persons" (Article 34).[9] In accordance with the minimum content required by law, the notification must include the measures taken by the data controller to mitigate the risks associated with the breach and must be submitted within 72 h of becoming aware of the breach.[10] An exemption may be applied in the instance where it is deemed unlikely that the breach will produce any adverse effect to fundamental rights and freedoms.[11] In the absence of any of these measures being implemented to mitigate the adverse effects from the data breach, the potential consequences could result in physical, material or non-material damage to individuals affected by the data breach.[12]

A second fundamental feature of the GDPR is the principle of accountability, mentioned in Article 5(2) and then further operationalized by Article 82. Under Article 82(1), "[a]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered".[13]

This provision provides the plaintiff with the right to claim compensation directly against the data controller or data processor, thereby avoiding the necessity to resort to national law.[14] Further, it opens the door to the possible intervention of CJEU

[8] Bradford (2020).

[9] Kiesow Cortez (2020, 244).

[10] Regulation (EU) 679/2018, Article 33.

[11] Regulation (EU) 679/2018, Article 33(1).

[12] Regulation (EU) 679/2018, Recital 85.

[13] Regulation (EU) 679/2018, Article 82(1).

[14] Knetsch (2022, 138).

whenever a doubt arises before national courts as to its application or interpretation, since the CJEU has jurisdiction over the interpretation of the EU law.[15]

A noteworthy element of Article 82(1) GDPR is the incorporation of a provision for compensatory damages in the EU legal framework—something that is a rarity within EU legislation.[16] In the context of the EU Member States, where legal traditions embrace different visions of tort law and of damage compensation,[17] the application of the provision has sparked a significant debate.[18] The Court of Justice in the latest years has developed a robust *corpus* of case-law on article 82(1) GDPR, with the aim of establishing a consistent interpretation across Member States.

By establishing clear obligations for data controllers and a mechanism to address data breaches, the GDPR empowers individuals to seek compensation in case of data breaches and strengthens the enforcement of data protection as a fundamental right. At the same time, the GDPR lays the groundwork for a uniform legal approach across EU Member States, guided by the evolving case law of the CJEU.

## *2.2 Japan: Data Protection Between Hard and Soft Law*

In Japan, the development of several branches of the law has been shaped less by statutory reforms than by the interpretations adopted by the Japanese Supreme Court and by lower courts.[19] This is the case for the fundamental principles about the existence of a general right to privacy and the right to obtain compensation in case of its infringement, that were established by the Supreme Court over the course of several decades, as Sect. 2.2.1 will show.

Japanese data protection law is more recent and has largely evolved because of external pressures. In recent years, and especially after the AD on Japan by the European Commission in 2019, the Japanese government has enacted significant reforms in this sector. Other than statutory law, the Japanese data protection law also includes additional significant sources such as the guidelines adopted by ministries and the guidelines enacted by the Japanese supervisory authority, the Personal Information Protection Commission (PPC). The aforementioned factors collectively delineate a data protection framework that provides protection for the personal data in a manner that aligns with the Japanese sensitivity regarding privacy.

[15] Knetsch (2022, 138).

[16] Knetsch (2022, 141).

[17] Infantino and Wang (2018, 59–60).

[18] Knetsch (2022, 141).

[19] Matsumoto (2021, 359).

### 2.2.1 The Right to Privacy in Japan

The right to privacy is not explicitly established by the Japanese Constitution or by the data protection law. The real recognition of the right to privacy in Japan lies outside these boundaries, since its definition was firstly outlined in civil litigation.[20] Japanese courts have played a crucial role in shaping the law of privacy, most of all through tort law, which has historically served as the primary basis for privacy infringement litigation.[21]

In particular, the Japanese Supreme Court has derived the right of privacy from article 13 of the Japanese Constitution, which states: "[a]ll of the people shall be respected as individuals".[22] Though in Japan constitutional provisions are not directly applicable to private law claims, nevertheless they may provide solutions to problems of legal interpretation. In the context of privacy infringement, the Japanese Supreme Court has read the said constitutional provision in combination with the tort law provisions in the Civil Code to infer the right to limit unauthorized access to private information without a lawful reason.[23] Over the past half century, Japanese courts have protected the right to privacy as the right of the individual to not have private information be known to the public, more specifically to let them be free from government interference.[24] If one considers the Japanese society from a historical perspective, it then becomes clear that the characteristics of such a right to privacy are deviant from the long-standing Japanese tradition to sacrifice the private sphere for the public interest, under which the needs and interests of the society were always considered to be of greater importance than those of the individual.[25]

The most significant shift in the approach in this regard occurred in the second half of the last century, when several decisions of the Japanese Supreme Court fundamentally altered the traditional perspective on privacy.[26] These rulings recognized that private matters must not be made public without a valid justification.[27] Moreover, the Supreme Court's decisions established that in the event of any personal information being made public and causing mental distress to the victim, the latter has the right to claim damages under article 709 of the Civil Code, which is the general provision on tort in Japan.[28] Therefore, the Japanese Supreme Court found the main legal remedy to the infringement of the right to privacy in the general provision on tort.

Furthermore, the court determined that the applicable standard of tort is based on the sensibility of an 'ordinary person' in Japan. In this regard, the circumstances to be evaluated by courts in privacy infringement cases are: 1) if the facts made

[20] Pardieck (2024, 5).

[21] Oda (2009, 42).

[22] Judgment of the Supreme Court, 6 March 2008, *Minshu* vol.62 n.3.

[23] Miyashita (2016, 117).

[24] Miyashita (2016, 117).

[25] Adams et al. (2009, 8).

[26] Pardieck (2024, 10).

[27] Pardieck (2024, 10).

[28] Pardieck (2024, 10).

public are related to the private life of the victim; 2) whether the disclosure of personal information would cause mental distress to an ordinary person; and 3) if such information could not have been known to the public.[29]

Even before the data protection law was drafted, the Japanese Supreme Court assumed a pivotal role in defining the right to privacy and its protection. This had been achieved through the application of tort law and the interpretative use of constitutional principles on statutory law. Japanese courts have always remained aligned with the sensitivity of the Japanese people, even when they introduced a right that was never considered as such before.

### 2.2.2 The Act on the Protection of Personal Information (APPI)

As a response to the Directive 1995/46/EC, Japan enacted in 2003 the Act on the Protection of Personal Information (APPI), that became effective in 2005.[30] Besides the Directive, the APPI was drafted following the OECD Privacy Guidelines of 1981 and its eight fundamental principles as a point of reference.[31] Actually, the APPI aligned more closely with the OECD Privacy Guidelines of 1981 than with the protection standards set forth by the Directive 1995/46/EC.[32]

This partially explains why the APPI has undergone several amendments over time. A first round of amendments was implemented in 2015, and further amendments were made in 2020 and 2021 (coming into effect in 2022), after the AD of 2019 on Japan was adopted.

The 2015 reform brought the Japanese data protection law closer to EU law regarding various aspects, such as the incorporation of the notion of pseudonymised personal data[33] and the establishment of an independent supervisory authority on data protection, the Personal Information Protection Commission (PPC), which played a significant role in drafting the AD of 2019.

The PPC is an independent supervisory authority that currently oversees the data protection matters related to business operators. While at the beginning its competence was limited in the private sector,[34] with the 2021 amendments it was expanded to the public sector too.[35] Prior to its establishment, a substantial part of the data protection enforcement involved guidelines from each Ministry and from local governments, that had a role in complementing the data protection law in force.[36] Since the main objective of these guidelines was to ensure the adherence to the provisions of the APPI, these measures were addressed to different types of business operators

[29] Pardieck (2024, 11).
[30] Suda (2020, 513).
[31] Miyashita (2011, 232).
[32] Suda (2020, 514).
[33] Suda (2020, 515).
[34] Suda (2020, 516).
[35] Miyashita (2022, 136).
[36] Miyashita (2016, 111).

and were specific to each industry sector.[37] Yet, there was often an overlap between different guidelines, and business operators found themselves bound to comply with many guidelines stemming from different ministries at the same time.[38] This situation gave rise to a considerable degree of perplexity and difficulty among the business operators, who were uncertain about which rules they needed to abide by, without infringing any of them. The establishment of the independent authority led to the dissipation of such doubts, because the PPC assumed a centralized role in enforcing Japanese data protection law.

In this regard, the amendments of 2015 also introduced some measures which constitute the primary enforcement mechanism of the PPC.[39] In particular, the revised APPI gave to the PPC the exclusive power to draft guidelines on the protection of personal information,[40] such as those containing supplementary and enforcement rules.[41] Furthermore, the PPC became the only authority with the power to issue recommendations and orders to business operators in the event of a violation of the APPI.[42] Currently, such violations are limited to a few cases per year, but should these recommendations and orders not be followed through, the PPC retains the power to impose administrative sanctions on non-complying subjects.[43] Although this has yet to happen in practice,[44] the PPC's approach exerts a considerable influence on the application of data protection rules and shapes the manner in which legal principles are applied and interpreted by Japanese courts, not only in the data breaches cases, but also in ordinary cases in which data protection matters.

It should nevertheless be noted that, even after the amendments to the APPI to better align it with the EU standard (especially after the AD of 2019), substantial disparities between the Japanese and the EU approach to personal data protection still persist. Besides the issue of enforcement, which in Japanese data protection framework remains much more rooted in soft law measures and cultural norms, another significant disparity stems from the definition of sensitive data. The later amendments to the APPI introduced a broader definition of sensitive data by introducing new categories of information called 'special care-required information'.[45] However, some information that could be considered sensitive in the EU, for example sexual orientation and trade union membership, are still considered not to be so in Japan.[46]

---

[37] Greenleaf and Shimpo (2014, 142).

[38] Miyashita (2022, 136).

[39] Wang (2020, 675).

[40] Japanese Act on the Protection of Personal Information (2003), Article 54.

[41] PPC, Enforcement Rules for the Act on the Protection of Personal Information, https://www.ppc.go.jp/files/pdf/PPC_rules.pdf; PPC, Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU and the United Kingdom based on an Adequacy Decision, https://www.ppc.go.jp/files/pdf/Supplementary_Rules_en.pdf.

[42] Japanese Act on the Protection of Personal Information (2003), Article 148.

[43] Japanese Act on the Protection of Personal Information (2003), Chapter VIII Penal Provisions.

[44] Kuroda, Nakayama, et al. (2025)

[45] Miyashita (2022, 134–135).

[46] Suda (2020, 520).

This demonstrates how variable the sensitivity on different kinds of data in Japan and in the EU still is.

In sum, despite the considerable efforts made by Japan to bring the data protection regime closer to that of the EU, significant differences remain, primarily due to the distinct legal traditions and cultural conceptions of privacy. Unlike the EU, where the right of privacy is nowadays considered to be a fundamental right, the recognition of privacy in Japan has evolved through judicial interpretation, simultaneously influencing its perception by society.

## 3 The Adequacy Decision on Japan by the European Commission

In order to understand the relationship and interconnection of the data protection laws between the EU and Japan, it is essential to take a closer look at the Adequacy Decision (AD) of 2019.

As illustrated above, the AD constituted the starting point of the most recent reforms of the Japanese data protection law, which took the Japanese APPI closer to the EU regime. However, Japan adapted its legislation following the principles of its own legal system and the characteristics of its legal tradition.

The impact made by the AD on Japan shows the GDPR's great influence outside the European borders, as a direct consequence of the 'Brussels Effect'. Specifically, the GDPR set a global standard on data protection, as multinational companies find it easier to adapt to a stricter standard set by a major economic force such as the EU, instead of imposing different ones across several countries.[47]

The legal foundation for this mechanism is article 45 of the GDPR. The article establishes the procedure which the EU is required to follow in order to recognize a third country as having an *adequate level of protection*[48] and therefore to facilitate the transfer of personal data to that country without further authorizations.[49] The formulation of article 45 makes it clear that the objective of an adequacy decision is not to impose identical level of protection based on the GDPR, but to oblige a third country to guarantee a protection for personal data similar to the one provided by the European standards.

The European Commission has so far recognized Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zeeland, the Republic of Korea, Switzerland, Uruguay, the United Kingdom and the USA, only for some commercial organisations participating in the EU-US Data Privacy Framework.[50]

---

[47] Rustad and Koenig (2019, 391).

[48] Regulation (EU) 679/2018, Article 45(1).

[49] Regulation (EU) 679/2018, Article 45(3).

[50] Kiesow Cortez (2020, 242).

### *3.1 The Path to the Adequacy Decision: The Role of the Guidelines*

The AD marked the culmination of a two-year long effort made by both Japan and the EU. The final agreement between the two countries, shaped by the dialogue between the Commission and the PPC, was reached in July 2018, and the AD took effect in January 2019.[51]

The process leading to the decision proved to be a challenging one for both the EU and Japan, implying several rounds of drafts prepared by the Japanese PPC and followed by recommendations by the European Commission.[52] The role of the PPC was of utmost importance, as their intervention with the Supplementary Rules and non-binding guidelines on international transfer constituted the basis for the implementation of the safeguards in practice.[53]

During the negotiation process, it soon became evident that Japan needed to make substantial amendments to the APPI.[54] The issues were accentuated by the profound gap between the two legal traditions: one crucial aspect of the discussion was the effectiveness of guidelines in enforcing the protection of European personal data in Japan.[55] As discussed in Sect. 2.2, the Japanese approach to data protection relied primarily on guidelines enacted by different ministries and on the spontaneous adherence to them by enterprises and public bodies. In the EU context, by contrast, measures such as guidelines were perceived as lacking the necessary authority to compel individuals and entities to abide by the legal framework.[56]

In collaboration with the PPC, the Japanese legislator worked to build a bridge to overcome these discrepancies. In particular, the PPC adopted in 2018 the Supplementary Rules to the APPI, which are explicitly recognized in the AD as having a legally binding effect on Japanese business operators.[57] The result is that the PPC guidelines are now deemed to be binding for business operators, since failure to comply with them is to be considered as a violation of the APPI itself.[58]

Thanks to this solution, agreement on the AD was reached. The EU now acknowledges that Japan guarantees an adequate level of data protection, aligned with the

[51] Suda (2020, 511).

[52] Suda (2020, 521).

[53] Wang (2020, 672).

[54] Suda (2020, 517).

[55] Wang (2020, 674–675).

[56] Wang (2020, 675).

[57] European Commission (2019) Decision 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, Recital 15.

[58] Wang (2020, 676).

standard set forth by the GDPR. The agreement enables the flow of personal information between businesses in both directions without requiring additional authorisation from business operators located in Japan.[59]

The Commission is obliged to review the AD every two years, as per its underlying agreement.[60] One relevant aspect of the latest report on Japan, which was published on 4th of April 2023, is that it concluded with a positive evaluation from the European Commission.[61] The Commission explicitly recognized the effort of the PPC in contributing to ensure an adequate level of protection after the final agreement was reached. Moreover, the Commission acknowledged once again Japan's preference for soft law measures and distinctly recognized the ability of these in guaranteeing the protection of personal data. In the report it can be read that "[t]he Commission notes that the PPC has made more use of its non-coercive powers of guidance and advice, than of its coercive powers in the period following the adoption of the adequacy decision".[62]

Overall, the AD of 2019 between the EU and Japan constitutes an essential development in facilitating cross-border data flows by recognizing the Japanese data protection regime as essentially equivalent to that of the EU. The agreement required Japan to reform some part of its data protection law, notably amendments to the APPI, in order to align the legal framework closer to EU requirements under Article 45 of the GDPR. Central to this was the role of Japan's PPC, whose guidelines addressed EU concerns over their enforceability. Despite structural and cultural differences—in particular the reliance of Japan on soft law –, the European Commission recognized the level of data protection in Japan to be similar to that of the GDPR.

## 4 Data Breach and Tort Law: A Comparative Analysis

After the overview of the data protection frameworks in the EU and Japan, especially with regard to the respective courts' interpretations of the right to privacy, it is now important to verify these courts' approach to data breach cases framed in tort. Courts indeed often address the challenges posed by digital vulnerability by hearing and adjudicating claims where plaintiffs complain of harm suffered because of the infringement of their privacy allegedly realized by the defendants. The aim of this section is therefore to explore the factors that are considered by the Japanese

[59] European Commission (2019) Decision 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, Recital 4.

[60] European Commission (2019) Decision 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, Recital 181.

[61] European Commission (2023) Report on the first periodic review of the adequacy decision for Japan: 6.

[62] European Commission (2023) Report on the first periodic review of the adequacy decision for Japan: 5.

Supreme Court and by the CJEU when assessing the harm caused by the unlawful use of data resulting from a data breach and providing the plaintiffs with a remedy.

Section 4.1 will therefore introduce the Benesse Case, through which the Japanese Supreme Court established significant principles and introduced new factors for assessing tort liability in data breach litigation and determining the amount of damages to be awarded. Section 4.2 will examine the elements identified by the Japanese Supreme Court as relevant in comparison with the most recent decisions of the CJEU on compensation for harm caused by data breaches.

## *4.1 The Benesse Case*

The Benesse case concerned a data breach in 2014 that compromised the personal information of 30 million customers of the Benesse Corporation. The data breach was caused by a sub-contractor engineer who stole the customer's information from the database of the company and subsequently sold it on the market to a number of data brokers. This resulted in the victims of the data breach being subject to unsolicited advertisements after the incident.[63]

In the aftermath, the Benesse Corporation issued a public apology and offered affected customers a 500-yen coupon as a compensation for the inconveniences of having their personal information leaked to the public. However, these measures did not prevent around 12.000 customers from filing claims for damages.[64]

The case passed through the first two levels of judicial reviews before reaching the Japanese Supreme Court, that remanded the case back to the Tokyo Appellate Court for the final judgment on the merit.[65] At the first instance, the Kobe district court declared that no evidence of negligence on the part of Benesse was found and therefore held that there was no civil liability in this case.[66] On appeal, the Osaka Court upheld the lower court's ruling, concluding that the anxiety caused by the data leakage did not amount to a sufficient injury to justify a legitimate claim for damages.[67]

While these decisions were being adopted, an investigation on the incident carried out by the Ministry of Economy, Trade and Industry (METI) revealed evidence of Benesse's infringements of the APPI provisions on security measures and on the duty to supervise contractors. In addition, the plaintiffs obtained further evidence of Benesse's negligence regarding the security measures required to protect personal information.[68]

---

[63] Ishii and Komukai (2016, 89).

[64] Pardieck (2024, 18–19).

[65] Pardieck (2024, 23).

[66] Pardieck (2024, 20).

[67] Pardieck (2024, 20).

[68] Pardieck (2024, 20).

This explained why the Japanese Supreme Court overturned the prior rulings and upheld the plaintiffs' claim. The Court found that the company had failed to implement adequate security measures to protect the personal data in its custody, and that the failure constituted negligence. Taking into account the supervisory obligations outlined in the METI guidelines, the Court concluded that such conduct constituted a tort under article 709 of the Japanese Civil Code.[69] Ultimately, the Tokyo Appellate Court's subsequent decisions recognized the negligence of the Benesse Corporation resulting in a compensable harm to the plaintiffs, and so, by holding it liable, the court awarded damage to the victims.[70]

## *4.2 The Comparative Analysis: Elements of Tort Law in Cases of Data Breaches*

After outlining the essential contents of the Benesse case, this section will analyse three key elements highlighted by the court: (a) the legal relevance of the mental distress arising from the loss of control over one's personal information; (b) the factors considered in determining the award; (c) the issuance of an apology as a form of compensation for non-material damages.

The element (a) concerns the legal relevance of the non-material damage resulting from the loss of control over personal information, particularly if the harm consists of psychological distress and fear associated with the loss. As anticipated above, in the Benesse decision, the Japanese Supreme Court recognized that mental distress caused by the unauthorized disclosure—and the consequent loss of control over one's personal information—constitutes an injury in itself, even in the absence of material damage.[71] The court determined that the sensation of loss of control over and the consequent feeling of uncertainty surrounding the status of personal information could constitute relevant harm.

A comparable issue was addressed by the CJEU litigation in the recent case C-590/22. In this judgment, the Court acknowledged that, under Article 82(1) of the GDPR, a data subject's concern for their personal data following a data breach may entitle them to redress.[72] However, the CJEU also clarified that the fear of the potential negative consequences must be proven in its entirety.[73] In doing so, the CJEU fully aligned with its own previous and subsequent case-law insisting that a mere infringement of the GDPR provisions is not sufficient for compensation and that

[69] Saikō Saibansho [Sup.Ct.] Oct. 23, 2017, Hei 28 (uke) no. 1892, (appeal from Osaka High Ct., Heisei 28 (ne) no. 37).

[70] Pardieck (2024, 24).

[71] Saikō Saibansho [Sup.Ct.] Oct. 23, 2017, Hei 28 (uke) no. 1892, (appeal from Osaka High Ct., Heisei 28 (ne) no. 37).

[72] Case C-590/22, *PS*, EU:C:2024:536 [20 June 2024], § 32.

[73] Case C-590/22, *PS*, EU:C:2024:536 [20 June 2024], § 36.

the material and non-material damage must be fully proven.[74] Merely proving the infringement of the GDPR is not enough to succeed, since the CJEU has repeatedly established that the following three cumulative conditions are necessary to give rise to the right to compensation: (1) the existence of the harm, (2) the infringement of the regulation and (3) the causal link between the two.[75] This implies that, although the CJEU adopted a broader definition of non-material damage, that includes the loss over one's personal information due to the possibility of data misuse,[76] the CJEU also emphasized that the existence of a concrete fear must be supported by specific evidence.[77]

The element (b) concerns the criteria to be addressed in determining the sum to be awarded to compensate the damage resulting from the violation of data protection provisions. In the Benesse decision, the Japanese Supreme Court identified five factors that must guide this assessment: *(i)* the nature of the information disclosed, along with the scope of the disclosure; *(ii)* the nature of the privacy rights infringed; *(iii)* the presence or absence of actual damage; *(iv)* the countermeasures adopted by the data controller; and *(v)* the previous disclosure of personal information.[78]

Some of these factors, such as the countermeasures taken after the breach by the data controller, bear some similarity with the duties imposed by Article 33 of the GDPR and surveyed above in Sect. 2.1 (consider for example the fact that, under Article 33 GDPR, the notification of the data controller must list the measures taken immediately after the breach).

Ultimately, in the aftermath of the Benesse case, the Tokyo Appellate Court issued against the Benesse Corporation a symbolic award of 1000-yen per plaintiff, intended as an expression of apology for the mental distress caused by the data breach. However, the court did not specify the factors that it took into consideration in the assessment.[79]

In the EU legal framework, the GDPR does not contain any specific provision on the assessment of damages. In the case C-300/21, the CJEU stated that, in the event of an infringement of the GDPR, European national judges must rely on their domestic legislation when determining compensation.[80] However, the CJEU also clarified that national courts' discretion in this regard is limited by two key principles: the principle of equivalence (according to which national rules used to enforce rights derived from EU law cannot be less favourable than those applied in an equivalent domestic situation) and the principle of effectiveness (according to which national rules cannot make the exercise of the rights conferred by the EU law excessively

[74] Case C-300/21, *Österreichische Post AG*, EU:C:2023:370 [4 May 2023], § 42; Case C-507/23 Patērētāju tiesību aizsardzības centrs, EU:C:2024:854 [4 october 2024], §29.

[75] Case C-300/21, *Österreichische Post AG*, EU:C:2023:370 [4 May 2023], § 32.

[76] Case C-340/21, *Natsionalna agentsia za prihodite,* EU:C:2023:986 [25 January 2024] § 20.

[77] Case C-590/22, *PS*, EU:C:2024:536 [20 June 2024], § 34.

[78] Saikō Saibansho [Sup.Ct.] Oct. 23, 2017, Hei 28 (uke) no. 1892, (appeal from Osaka High Ct., Heisei 28 (ne) no. 37).

[79] Pardieck (2024, 23).

[80] Case C-300/21, *Österreichische Post AG*, EU:C:2023:370 [4 May 2023], § 53–59.

difficult or impossible).[81] Nonetheless, in light of these principles, the CJEU retains the power to verify whether an award issued under domestic law is adequate to compensate in its entirety the damage suffered.[82]

The element (c) is compensation through apology. As illustrated, the Japanese Supreme Court has long affirmed that damages under tort law should be determined taking into consideration all the circumstances of the case and the sensibility of an 'ordinary person'.[83]

In Japan, courts attach great importance to the actions undertaken after the breach by defendants, including apologies released via public media or the adoption of measures to avoid causing further harm.[84] In particular, the issuance of a public apology is highly valued in the Japanese culture, because for Japanese companies the loss of a customer's trust and the reputational damage resulting from a data breach are considered to be more impactful than the obligation to pay fines or compensate for the damages caused.[85] Especially in cases of defamation and intellectual property infringement, plaintiffs often explicitly request, and courts often accept, that, as a form of redress, defendants are obliged to issue apologies, which are then published in newspapers.[86]

In the Benesse case, the Benesse Corporation issued a formal public apology for the data breach immediately after the news broke on the mainstream media, in the absence of any external pressure or legal obligation to do so. Alongside this notification, the company also divulged the measures implemented to prevent potential secondary harm and to increase the security of their data protection systems.[87] The prompt issuance by the Benesse Corporation of a public apology outlining the remedial actions undertaken, reflected the respect for a cultural norm under which the apology serves both a symbolic and a practical role.

The role of an apology as a potential form of compensation has also been recognized in the European context. In the recent case C-507/23, the CJEU expressly stated that an apology may fully compensate for the harm suffered.[88] Yet, the court further asserted that, when determining the compensation under Article 82(1) of the GDPR, neither the attitude nor the motivation of the data controller are to be considered, since the purpose of such a provision is to ensure redress for any material and non-material harm directly caused by the data protection violation.[89] This interpretation clearly limits the rationale for issuing apologies in case of corporate data breaches.

On a conclusive note, there is a growing acknowledgment in the EU context about the positive impact of an apology—especially for victims of non-pecuniary

[81] Case C-300/21, *Österreichische Post AG*, EU:C:2023:370 [4 May 2023], § 53.

[82] Case C-300/21, *Österreichische Post AG*, EU:C:2023:370 [4 May 2023], § 58.

[83] Pardieck (2024, 11).

[84] Pardieck (2024, 43).

[85] Miyashita (2016, 107).

[86] Lee (2005, 38–39).

[87] Benesse Holdings Inc (2014).

[88] Case C-507/23, *Patērētāju tiesību aizsardzības centrs*, EU:C:2024:854 [4 october 2024], §36–37.

[89] Case C-507/23, *Patērētāju tiesību aizsardzības centrs*, EU:C:2024:854 [4 october 2024], §43–44.

harm.[90] On the other hand, in the Japanese legal and cultural framework, a public apology often holds greater meaning for victims than any monetary compensation, as it directly addresses the breach of trust between them and the company that caused them harm.[91]

Overall, the analysis of these three elements demonstrates that the Japanese and EU approaches to remedies for data breaches are shaped by their respective legal traditions but are also converging on a broader understanding of harm from data breaches in the digital age.

## 5 Conclusion

The above study showed that, in Japan as well as in the EU, courts predated and complemented data protection legislation in addressing data breaches through the adjudication of civil liability cases. The Supreme Court of Japan and the CJEU both recognized that the mental distress from the unauthorized disclosure of personal data may be a compensable harm, even though the Japanese Supreme Court found that a data breach may constitute an injury per se, while the CJEU requires the proof of the concrete existence of the fear. Both courts acknowledge the possible role of apologies as a form of compensation. Yet, apologies play in Japan an important cultural and legal role as both a symbolic and compensatory measure, as also demonstrated by the objective and subjective factors that courts are required to take into account when determining the compensation owed, while the CJEU held that an apology can be a form of compensation only if it allows it to compensate the damage fully.

The analysis therefore showed that, in spite of many similarities, the approaches adopted by Japan and the EU to remedy data vulnerability through tort law also differ. In the EU, the GDPR establishes a regulatory framework based on the respect of data protection as a fundamental right and provides for compensation in the event of concrete harm resulting from the infringement of the regulation. In addition, the CJEU has taken steps to define the scope of protection by requiring a demonstrable harm, while at the same time recognizing that mental distress can constitute non-material damage. In contrast, the Japanese legal framework for data protection tends to rely on softer provisions, with courts showing a deep sensitivity to the cultural expectations of the general public and demonstrating substantial flexibility in shaping the remedies for privacy violations, including through public apology and repair of reputational damage. Japanese courts seek to balance the rights of the victims of data breaches with the interests of the companies concerned, even when the latter are found liable for failing to take proper protective measures.

Despite these differences, a common ground between the two legal systems is that digital vulnerability is recognized by both of them as a key concern in the field of data protection, especially in a context constantly shaped by technological advances.

[90] De Rey (2021, 205–206).

[91] Wang (2020, 681).

While the European approach emphasises clear evidence of damage, the Japanese's one places greater importance on contextual and reputational factors. Nevertheless, they both strive to protect data subjects by offering the remedies that reflect what each legal tradition considers most significant.

**Funding Information** This contribution has benefited from support co-funded by the European Social Fund Plus of the Autonomous Region of Friuli Venezia Giulia.

## References

Adams A, Murata K, Orito Y (2009) The Japanese sense of information privacy. AI Soc 24:327–341

Benesse Holdings, Inc. (2014) Notice and apology regarding leakage of customer's personal information. https://pdf.irpocket.com/C9783/o1Tt/faNa/DxxF.pdf

Bradford A (2020) The Brussels effect: how the EU rules the world. Oxford University Press, New York

Brüggemeier G, Colombi Ciacchi A, O'Callaghan P (2010) Personality rights in European Tort law. Cambridge University Press, Cambridge

Casagran CB (2017) Global data protection in the field of law enforcement: an EU perspective. Routledge, New York

De Rey SE (2021) Court-ordered apologies under the law of torts? Non-monetary relief for emotional harm. A comparative outlook from a western legal perspective. In: Brutti N, Carroll R, Vines P (eds) Apologies in the Legal arena, a comparative perspective. Bonomo Editore, Bologna, pp 203–249

European Commission (2019) Decision 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information

European Commission (2023) Report on the first periodic review of the adequacy decision for Japan

European Union (1995) Directive 95/46/EC

European Union (2012) Charter of Fundamental Rights of the EU

European Union (2018) Regulation 679/2018 General Data Protection Regulation

Floridi L (2016) On human dignity as a foundation for the right to privacy. Philosophy & Technology 29:307–312

Greenleaf G, Shimpo F (2014) The puzzle of Japanese data privacy enforcement. International Data Privacy Law 4(2):139–154

Infantino M, Wang W (2018) Algorithmic torts: a prospective comparative overview. Transnational Law & Contemporary Problems 29(1):1–68

Ishii K (2020) Advancements in the personal information protection system in Japan. Global Privacy Law Review 1:164–172

Ishii K, Komukai T (2016) A Comparative Legal Study on Data Breaches in Japan, the U.S., and the U.K. In: Kreps D, Fletcher G, Griffiths M (eds) Technology and Intimacy: Choice or Coercion. HCC 2016. IFIP Advances in Information and Communication Technology 474. Springer, Cham, pp 86–105

Japanese Act on the Protection of Personal Information (2003)

Kiesow Cortez E (2020) Data Breaches and GDPR. In: Holt T, Bossler A (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham, pp 239–256

Knetsch J (2022) The compensation of non-pecuniary loss in the GDPR infringement cases. Journal of European Tort Law 13(2):132–153

Kuroda Y, Nakayama T, et al. (2025) Data protection & privacy 2025—Japan. Chambers and Partners

Lee I (2005) The law and culture of the apology in Korean Dispute settlements (With Japan and the United States in Mind). Michigan J Int Law 27(1):6–53
Malgieri G (2023) Vulnerability and data protection law. Oxford University Press, Oxford
Matsumoto E (2021) Tort law in Japan. In: Bussani M, Sebok AJ (eds) Comparative tort law: Global perspectives. Edward Elgar, Cheltenham, pp 373–396
McGeveran W (2016) Friending the privacy regulators. Ariz Law Rev 56:960–1025
Miyashita H (2011) The evolving concept of data privacy in Japan. International Data Privacy Journal 1:229–238
Miyashita H (2016) A tale of two privacies: Enforcing privacy with hard power and soft power in Japan. In: Wright D, De Hert P (eds) Enforcing Privacy. Springer, Cham, pp 105–122
Miyashita H (2021) Human-centric data protection laws and policies: a lesson from Japan. Comput Law Secur Rev 40:1–9
Miyashita H (2022) Data protection law in Japan. In: González G, Van Brakel R, De Hert P (eds) Research handbook on privacy and data protection law. Edward Elgar, Cheltenham, pp 128–139
Oda H (2009) Japanese law. Oxford University Press, Oxford
Pardieck AM (2024) Privacy matters: data breach litigation in Japan. Washington International Law Journal 33:1–32
Rustad ML, Koenig TH (2019) Towards a global data privacy standard. Florida Law Review 71:365–452
Suda Y (2020) Japan's personal information protection policy under pressure. Asian Surv 60:510–533
Wang FY (2020) Cooperative data privacy: the Japanese model of data privacy and the Eu-Japan GDPR adequacy agreement. Harvard J Law Technol 33:661–691