The Proactive Imperative: A Legal Analysis of DPA Enforcement Actions and Lessons from the 23andMe and Carrefour Breaches

1. Introduction

The data protection landscape in the European Union and the United Kingdom continues its rapid evolution, driven by the robust enforcement of the General Data Protection Regulation (GDPR)[1] and its UK equivalent, the Data Protection Act 2018[2]. As personal data becomes an increasingly valuable asset for commerce and innovation—and simultaneously a prime target for malicious actors[3]—national data protection authorities (DPAs), despite justified current criticism of their enforcement,[4] are demonstrating reasonable commitment to holding organizations accountable for their security practices. This report conducts a comparative analysis of pivotal decisions by two prominent DPAs—the UK Information Commissioner's Office (ICO) and the Spanish Data Protection Agency (AEPD)—to illuminate escalating regulatory expectations and the critical importance of effective data protection measures.

The ICO's recent imposition of a £2.31 million fine on genetic testing company 23andMe serves as a stark reminder of the heightened scrutiny applied to entities processing sensitive data special category data, such as genetic information. This decision, following a joint investigation with the Office of the Privacy Commissioner of Canada, underscored 23andMe's profound failings in implementing basic security protocols, most notably the absence of mandatory multi-factor authentication (MFA). The breach, stemming from a credential stuffing attack, exposed sensitive personal

---

[1] 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) [2016] OJ L 119/1.

[2] Data Protection Act 2018, c 12.

[3] European Data Protection Board, 'AI privacy risks and mitigations in LLMs' (April 2025) <https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf> accessed 2 August 2025.

[4] David Erdos, 'Holding the Information Commissioner's Office (ICO) to Account' (Written Evidence submitted to the Data (Use & Access) Bill Committee, 2023) DUAB08; David Erdos, 'UK Regulatory Enforcement of Data Protection: Current Concerns and Pathways for More Effective and Consistent Practice' (*Oxford Business Law Blog*, March 2023) https://blogs.law.ox.ac.uk/oblb/blog-post/2023/03/uk-regulatory-enforcement-data-protection-current-concerns-and-pathways-more accessed 2 August 2025; David Erdos, 'The UK Information Commissioner's Annual Report 2024-25: Surveying a Systematic Trend away from Adequate Enforcement' (*UK Constitutional Law Association Blog*, July 2025) https://ukconstitutionallaw.org/2025/07/22/david-erdos-the-uk-information-commissioners-annual-report-2024-25-surveying-a-systematic-trend-away-from-adequate-enforcement/ accessed 2 August 2025.

and health data of thousands of UK residents, highlighting the irreversible nature of such a compromise when it involves genetic profiles.[5]

Mirroring this rigorous approach, the AEPD's €3.2 million penalty against retail giant Carrefour S.A. provides a compelling Spanish perspective on similar security shortcomings. The Carrefour decision, also triggered by a series of credential stuffing attacks, revealed the company's reactive rather than proactive stance on cybersecurity, with two-factor authentication (2FA) only being implemented after multiple breaches. The AEPD's findings, which also included a violation of Article 33 of the GDRP (breach notification),[6] resonate with the ICO's, emphasizing the critical need for robust authentication mechanisms and timely incident response across all sectors handling significant volumes of personal data.[7]

These two high-profile decisions, occurring in close temporal proximity and addressing analogous security vulnerabilities, collectively illustrate a clear and consistent regulatory message across the UK and Europe. In line with caselaw from the Court of Justice of the EU (CJEU),[8] they underscore that organizations are expected to implement comprehensive technical and organizational measures, anticipate evolving cyber threats like credential stuffing, and ensure transparent communication with data subjects in the event of a breach. This report will first detail these DPA actions and establish the broader legal framework provided by key CJEU jurisprudence, followed by an in-depth analysis of converging regulatory expectations, and finally, present actionable recommendations for enhancing data protection posture.

2. Case Studies: DPA Enforcement Actions and Legal Framework

To understand the practical application of GDPR's data security principles—specifically the requirements for integrity and confidentiality under Article 5(1)(f) and the technical and organizational measures of Article 32—examining recent DPA enforcement actions is crucial. The decisions against 23andMe and Carrefour S.A. offer direct insights into current regulatory priorities and the specific types of security failings that incur substantial penalties.

---

[5] Information Commissioner's Office, '23andMe fined for failing to protect UK users' genetic data' (June 2025) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data/> accessed 2 August 2025.

[6] AEPD, 'AEPD (Spain) - EXP202305979' (2023) <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202305979> accessed 2 August 2025.

[7] Information Commissioner's Office, '23andMe fined for failing to protect UK users' genetic data' (June 2025) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data/> accessed 2 August 2025.

[8] See e.g., Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986 [26]; Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* [2023] ECLI:EU:C:2023:957[3], [5], [56], [59], [66]; Case C-203/22 *CK v Dun & Bradstreet Austria GmbH* [2025] ECLI:EU:C:2025:117 [5], [58].

2.1. ICO Fines 23andMe £2.31 Million for Failing to Protect Genetic Data

The UK Information Commissioner's Office (ICO) fined genetic testing company 23andMe £2.31 million for failing to implement adequate security measures, leading to a large-scale cyberattack in 2023. The penalty follows a joint investigation with the Office of the Privacy Commissioner of Canada (OPC), underscoring the growing importance of international regulatory cooperation.[9]

The breach, which occurred between April and September 2023, was a "credential stuffing" attack that exploited login credentials stolen from unrelated data breaches.[10] This granted unauthorized access to approximately 155,592 UK accounts and up to 7 million customers globally. The breach exposed personal data including names, profile images, birth years, location, race, ethnicity, family trees, and health reports.[11] The ICO noted that genetic information is permanent and cannot be changed, demanding a heightened standard of care.[12]

The joint investigation found that 23andMe violated UK data protection law (Data Protection Act 2018) by failing to implement appropriate technical and organizational measures as mandated by Article 5(1)(f) (integrity and confidentiality) and Article 32(1) (security of processing) of the UK GDPR. Several key failings were identified. First, the company's security measures were inadequate, as multi-factor authentication (MFA) was optional, with less than 22% of users opted in. Furthermore, 23andMe had weak password requirements and did not conduct robust checks for compromised or reused passwords. Second, the company's monitoring was insufficient; its systems failed to detect a login spike that occurred in July 2023, even after receiving direct warnings about stolen data being sold online. Compounding these issues, 23andMe's response was delayed, taking a full month to implement mandatory MFA and disable the raw DNA download feature. Finally, the company's breach notification was inadequate; it failed to inform the ICO of the incident within the statutory 72-hour timeframe and provided incomplete information, violating Article 33 and necessitating multiple follow-ups from the regulator.[13]

---

[9] Information Commissioner's Office, '23andMe fined for failing to protect UK users' genetic data' (June 2025) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data/> accessed 2 August 2025.

[10] *Ibid*.

[11] *Ibid*.

[12] Information Commissioner's Office, 'Statement on 23andMe investigation' (March 2025) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/statement-on-23andme-investigation/> accessed 2 August 2025.

[13] Office of the Privacy Commissioner of Canada, 'Joint investigation into 23andMe Inc' (2025) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/> accessed 2 August 2025.

This case sets a significant precedent for organizations handling highly sensitive personal data. The decision emphasizes that a heightened standard of care is required for information like genetic data due to its immutable nature.[14]

2.2. AEPD Fines Carrefour S.A. €3.2 Million for Repeated Security Failures

The Spanish Data Protection Agency (AEPD) fined Carrefour S.A. €3.2 million for a series of data breaches, providing a key comparison point to the 23andMe case due to similar security failures. The decision, made in March 2025, followed an investigation into five separate breaches that occurred between January and September 2023.[15]

All five breaches were linked to "credential stuffing" attacks.[16] The compromised data included at least the confirmation of valid credentials and likely access to personal information such as full name, contact details, and addresses. The AEPD found that the breaches affected a much higher number of accounts (almost 119,000) than initially claimed by the company.[17]

The Spanish Data Protection Agency found Carrefour S.A. in violation of several GDPR articles following a series of data breaches. The investigation revealed that the company failed to implement proactive and appropriate security measures, a breach of Article 5(1)(f) (integrity and confidentiality) and Article 32 (security of processing). The AEPD's decision specifically criticized Carrefour's significant delay in introducing Two-Factor Authentication (2FA), which was only implemented after the fifth breach, highlighting a reactive rather than preventative security posture. Furthermore, Carrefour was found to have violated its general responsibility as a data controller to ensure compliance under Article 24(1) by not managing security risks effectively. The company also failed to notify the supervisory authority of a breach in a timely manner, a clear violation of Article 33. Finally, Carrefour's communication with its customers was deemed insufficient and in breach of Article 34. The company's email only informed customers of a required password change, without explicitly stating that a data breach had occurred, detailing its severity, or explaining the potential risks to their personal data.[18]

The Carrefour decision is particularly relevant for comparison with the 23andMe case due to the identical attack vector and the focus on the delayed implementation of

---

[14] US House of Representatives Committee on Oversight and Accountability, 'Letter to 23andMe, Inc' (15 April 2025) <https://oversight.house.gov/wp-content/uploads/2025/04/04.15.2025-23andMe-Letter.pdf> accessed 2 August 2025.

[15] AEPD, 'AEPD (Spain) - EXP202305979' (2023) <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202305979> accessed 2 August 2025.

[16] *Ibid*.

[17] *Ibid*.

[18] *Ibid*.

multi-factor authentication as a critical security failure. Both DPAs criticized the companies for a reactive posture.[19] The case highlights that even for large-scale breaches of non-genetic data, regulators will impose significant fines, especially when security is demonstrably inadequate and communication with data subjects is misleading.

3. Analysis: Converging Regulatory Expectations & Jurisprudence

The DPA enforcement actions against 23andMe and Carrefour S.A., when viewed through the lens of recent CJEU jurisprudence,[20] reveal a clear convergence of regulatory expectations regarding data security and accountability. These cases are not isolated incidents but illustrative examples of broader trends in GDPR enforcement.

3.1. Credential Stuffing as a Definitive Security Failing

Both the 23andMe and Carrefour breaches underscore that credential stuffing is a threat demanding appropriate security. The rulings by their respective DPAs, supported by the landmark CJEU judgment in *Natsionalna agentsia za prihodite*[21], established that relying on single-factor authentication constitutes a failure to implement "appropriate technical and organisational measures" under Article 32 GDPR.[22] The Court clarified that the adequacy of these measures must be assessed "in a concrete manner" considering the specific risks, nature, scope, context, and purposes of the processing.[23] It also affirmed that the burden of proof rests with the controller to demonstrate their security was sufficient.[24] Furthermore, the ruling established that a controller is not automatically exempt from liability for a third-party breach (e.g., a hacker), and that a well-founded "fear" of data misuse can constitute

---

[19] Office of the Privacy Commissioner of Canada, 'Joint investigation into 23andMe Inc' (2025) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/> accessed 2 August 2025; AEPD, 'AEPD (Spain) - EXP202305979' (2023) <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202305979> accessed 2 August 2025.

[20] *Ibid*.

[21] Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986 [26].

[22] Office of the Privacy Commissioner of Canada, 'Joint investigation into 23andMe Inc' (2025) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/> accessed 2 August 2025; AEPD, 'AEPD (Spain) - EXP202305979' (2023) <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202305979> accessed 2 August 2025.

[23] Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986 [42], [47], [87]

[24] *Ibid* [52], [56], [57].

compensable non-material damage.[25] This judgment directly empowered regulators such as the ICO and AEPD. The authorities concluded that, despite the external origin of the credential stuffing attacks, the companies' failure to implement robust controls like MFA rendered them "responsible" for the breaches, leading to the imposition of fines.[26]

3.2. The Imperative of Proactive Security and Data Protection by Design

The consistent criticism of both companies for their reactive rather than proactive security postures highlights a fundamental shift in regulatory expectations. The delayed implementation of MFA by both 23andMe and Carrefour, only after multiple breaches or clear warning signs,[27] stands in stark contrast to the Article 25 GDPR principle of "data protection by design and by default." This principle demands that security safeguards, like robust authentication, are integrated from the outset, not as an afterthought.[28] CJEU caselaw, such as *Fashion ID*[29] and *Wirtschaftsakademie Schleswig-Holstein*[30], implicitly requires website operators to embed privacy protections at the design stage, extending their responsibility even to third-party plugins. This proactive design approach is further affirmed in the *Natsionalna agentsia za prihodite*[31] ruling, which demands that the security measures move beyond reactive fixes to be designed with a level of security appropriate to the risk. The AEPD's fine against Caixabank in March 2025, explicitly linked to "poor design of the bank's online banking system," reinforcing that design flaws leading to security vulnerabilities are actionable infringements.[32] Regulators expect organizations to

---

[25] *Ibid* [74], [86].

[26] Office of the Privacy Commissioner of Canada, 'Joint investigation into 23andMe Inc' (2025) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/> accessed 2 August 2025; AEPD, 'AEPD (Spain) - EXP202305979' (2023) <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202305979> accessed 2 August 2025.

[27] *Ibid*.

[28] Information Commissioner's Office, 'Data protection by design and default' (2025) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-default/> accessed 2 August 2025.

[29] Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* [2019] EU:C:2019:629 [76], [101].

[30] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] EU:C:2018:388 [39], [42].

[31] Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986 [38].

[32] AEPD, 'AEPD (Spain) - EXP202213437' (2022) <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202213437> accessed 2 August 2025.

anticipate known threats and build resilience into their systems proactively. This coordinated approach is further supported by the European Data Protection Board's (EDPB) Coordinated Enforcement Framework (CEF), which is focusing on the right to erasure in 2025 to ensure consistent enforcement across the EEA.[33]

3.3. Amplified Risk for Sensitive and Large-Scale Data Processing

The nature of the data compromised significantly influenced the severity of the fines. The ICO's decision against 23andMe vividly demonstrates the magnified risk associated with "special category data" under Article 9 GDPR.[34] Genetic information, being immutable and deeply personal, demands an exceptionally high standard of care justifying a substantial penalty.[35] CJEU jurisprudence, such as *Lindenapotheke*[36] and *Ministerstvo na vatreshnite raboti*[37] reinforces that any data allowing the inference of sensitive characteristics and the indiscriminate collection of genetic and biometric data, requires strict necessity and robust safeguards to be lawfully processed. While Carrefour's breach did not involve genetic data, its large scale and the potential for identity theft and fraud (due to access to personal details) still warranted a significant fine. This illustrates that DPAs are attentive to both the type and the volume/impact of compromised data. Furthermore, the *SCHUFA Holding (Scoring)*[38] and *Dun & Bradstreet*[39] judgments, though not directly security-focused, reflect the CJEU's broad commitment to holding large-scale data aggregators to high standards of accountability and transparency, encompassing not only security but also profiling, data retention, and the right to meaningful information.

---

[33] European Data Protection Board, 'Coordinated Enforcement Framework' (2025) <https://www.edpb.europa.eu/coordinated-enforcement-framework_en> accessed 2 August 2025.

[34] Information Commissioner's Office, '23andMe fined for failing to protect UK users' genetic data' (June 2025) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data/> accessed 2 August 2025.

[35] Information Commissioner's Office, 'Statement on 23andMe investigation' (March 2025) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/03/statement-on-23andme-investigation/> accessed 2 August 2025.

[36] Case C-21/23 *ND v DR (Lindenapotheke)* [2024] EU:C:2024:846 [83], [84].

[37] Case C-205/21 *VS v Ministerstvo na vatreshnite raboti* [2023] EU:C:2023:49 [117], [135].

[38] Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* [2023] ECLI:EU:C:2023:957 [5], [10], [50], [56], [63].

[39] Case C-203/22 *CK v Dun & Bradstreet Austria GmbH* [2025] ECLI:EU:C:2025:117 [3], [70], [74], [75].

3.4. Enforcement of Data Subject Rights and Transparency

Failures in breach communication were a common thread in both the 23andMe and Carrefour incidents. The companies were criticized not only for delayed notification to affected data subjects (Article 34 GDPR), but also for their inadequate transparency in a way that undermined the data subject's fundamental right to be informed (Articles 13 and 14 GDPR).[40] This broader commitment to transparency is underscored by recent CJEU rulings such as *SCHUFA Holding (Scoring)*[41] and *Dun & Bradstreet*[42], which compel controllers to provide "meaningful information" (Article 15(1)(h) GDPR) about automated decisions (Article 22 GDPR), even over claims of trade secrets. This jurisprudence confirms that transparency is a core legal requirement.[43] Combined with the CJEU's *Natsionalna agentsia za prihodite*[44] ruling, it is clear that data subjects' rights to accurate information and redress are highly protected. This places additional pressure on controllers to manage breaches effectively and transparently.

In essence, these cases showcase a regulatory environment that demands not just reactive compliance post-breach, but proactive, designed-in security, robust accountability frameworks, and a firm commitment to data subject rights and transparency across all forms of data processing.

4. Recommendations for Robust Data Protection

Based on these critical lessons, organizations must strengthen their data protection posture to mitigate risks and ensure compliance.

4.1. Mandate Phishing-Resistant MFA and Strong Password Policies

The primary lesson from both 23andMe and Carrefour is to eliminate single-factor authentication. Organizations must mandate MFA for all user accounts, particularly for sensitive data and privileged access. However, while MFA significantly reduces the risk of account compromise—with research by Microsoft showing a 99.22%

---

[40] Office of the Privacy Commissioner of Canada, 'Joint investigation into 23andMe Inc' (2025) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/> accessed 2 August 2025; AEPD, 'AEPD (Spain) - EXP202305979' (2023) <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202305979> accessed 2 August 2025.

[41] Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* [2023] ECLI:EU:C:2023:957 [16], [56], [63].

[42] Case C-203/22 *CK v Dun & Bradstreet Austria GmbH* [2025] ECLI:EU:C:2025:117 [70], [74], [75].

[43] Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* [2023] ECLI:EU:C:2023:957 [5], [56], [59]; Case C-203/22 *CK v Dun & Bradstreet Austria GmbH* [2025] ECLI:EU:C:2025:117 [5], [58].

[44] Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986 [57], [74], [82], [86].

reduction[45]—not all methods are equally effective. To maximize effectiveness, a risk-based approach should be taken to select the most appropriate method. The UK National Cyber Security Centre (NCSC) categorizes MFA types from most to least secure, highlighting the superiority of FIDO2 credentials (often called passkeys) and challenge-based authenticator apps over less secure SMS or email methods.[46] The NCSC emphasizes that the key limitations of MFA stem from its implementation, as sophisticated attackers have developed techniques to bypass weaker forms. [47] Therefore, organizations must guard against vulnerabilities like "MFA fatigue" attacks and implementation flaws such as allowing legacy protocols to bypass MFA or exempting privileged accounts.[48] By combining mandatory, robust MFA with strong password policies, organizations can effectively defend against common cyber threats and meet evolving regulatory expectations.

4.2. Cultivate Proactive Threat Intelligence and Continuous Monitoring

In a rapidly evolving digital landscape, the need for proactive security has never been greater. The international cyber threat intelligence market is a testament to this, with its expected growth to $15.8 billion by 2026, highlighting the global focus on mitigating sophisticated cyber risks.[49] A reactive security posture is no longer acceptable demanding proactive threat intelligence. The failure of both 23andMe and Carrefour to act on early warning signs stresses the necessity of a robust threat intelligence program. Such a program should provide valuable insights and predictions about potential threats, enabling security teams to anticipate, detect, and prevent attacks before they happen. Effective tools should offer real-time data collection, seamless integration with existing security infrastructure like SIEM systems, and utilise automation and artificial intelligence to streamline detection and response.[50] This intelligence can be used at three levels: strategic (high-level

---

[45] Microsoft, 'Announcing Mandatory Multi-Factor Authentication for the Microsoft 365 Admin Center' (Microsoft Tech Community, 2025) <https://techcommunity.microsoft.com/blog/microsoft_365blog/announcing-mandatory-multifactor-authentication-for-the-microsoft-365-admin-cent/42325> accessed 2 August 2025.

[46] National Cyber Security Centre, 'Recommended types of MFA' (2025) <https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/recommended-types-of-mfa> accessed 2 August 2025.

[47] National Cyber Security Centre, 'Not all types of MFA are created equal' (NCSC Blog, 2025) <https://www.ncsc.gov.uk/blog-post/not-all-types-mfa-created-equal> accessed 2 August 2025.

[48] *Ibid*.

[49] MarketsandMarkets, 'Threat Intelligence Security Market' (MarketsandMarkets, 2025) <https://www.marketsandmarkets.com/Market-Reports/threat-intelligence-security-market-150715995.html> accessed 2 August 2025.

[50] Recorded Future, 'Threat Intelligence 101: Tools and Technologies' (Recorded Future, 2025) <https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies> accessed 2 August 2025.

insights for executives), tactical (detailed TTPs for security experts), and operational (real-time insights for incident response). Effective implementation requires a comprehensive approach, including clear goals, adequate staff training, and continuous updates to intelligence feeds.[51]

4.3. Develop and Practice a Comprehensive Incident Response Plan

Prompted by the delayed responses of 23andMe and Carrefour, a well-defined and regularly tested incident response plan is a GDPR cornerstone. An effective plan must outline clear procedures for detecting, containing, and recovering from breaches, while also ensuring it is regularly tested and evaluated for effectiveness, as required by Article 32(1)(b), (c), and (d) of the GDPR. This is underpinned by the CJEU's *VB v Natsionalna agentsia za prihodite*[52] judgment, which places the burden on controllers to prove their security measures were appropriate. The plan must include timely notification to the supervisory authority (within 72 hours, per Article 33 GDPR) and affected individuals (without undue delay, per Article 34 GDPR). Transparent and comprehensive communication with data subjects is essential, as the CJEU's ruling in *BL v MediaMarktSaturn*[53] established that even minor, non-material damage can be grounds for compensation, with no *de minimis* threshold. Finally, regular drills and simulations are crucial. They ensure the plan's effectiveness and serve as vital evidence of an organization's accountability, directly supporting the GDPR's requirement (Articles 5(2) and 24) to demonstrate compliance to regulators.

4.4. Implement Heightened Safeguards for Special Category Data

The 23andMe case unequivocally demonstrated the critical need for enhanced sensitive data protection such as health, biometric, racial, political, or religious information (Article 9 GDPR). The publication of the European Health Data Space (EHDS) Regulation in March 2025 further underscores this, creating a new legal framework specifically for electronic health data that demands robust safeguards for both primary and secondary use.[54] Organizations processing such data must conduct thorough Data Protection Impact Assessments (DPIAs) (Article 35 GDPR). A DPIA is a legal requirement under the GDPR for processing operations likely to

---

[51] *Ibid*.

[52] Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986 [7], [29], [42].

[53] Case C-687/21 *BL v MediaMarktSaturn Hagen-Iserlohn GmbH* [2024] ECLI:EU:C:2024:72 [59], [66].

[54] European Commission, 'European Health Data Space Regulation (EHDS)' (2025) <https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en> accessed 2 August 2025.

result in "high risk" for individuals, serving as a cornerstone for demonstrating accountability and embedding "data protection by design and default" (Article 25 GDPR). Its omission can lead to substantial fines, potentially up to £17.5 million or 4% of global annual turnover.[55] This essential risk-based approach, consistent with CJEU *VB v Natsionalna agentsia za prihodite*[56] and *SCHUFA Holding (Scoring)*[57] cases, should lead to the implementation of robust organizational and technical measures (Article 32 GDPR) like regular risk assessments, comprehensive staff training, and the strategic use of encryption and pseudonymisation. To ensure data integrity, organizations must implement strong physical and cybersecurity measures, including robust backup processes and regular testing like vulnerability scanning. Adhering to recognized frameworks like Cyber Essentials is also a key way to demonstrate compliance.[58]

4.5. Embed Accountability and Data Protection by Design and Default

The 23andMe and Carrefour decisions implicitly underscore the principle of accountability (Article 5(2) GDPR), placing the onus on organizations to demonstrate compliance beyond mere technical fixes. A critical step is to integrate data protection principles into the design of new systems, products, and services at the outset, ensuring that, by default, only the necessary personal data is processed. This involves conducting privacy-by-design reviews at every stage of development, with close collaboration between legal and technical teams.[59] In line with CJEU caselaw that requires the least invasive data protection approach—for example, in judgments like *Koninklijke Nederlandse Lawn Tennisbond*[60] and *HTB Neunte Immobilien Portfolio*[61]—a key part of this process is utilising Privacy Enhancing Technologies,

---

[55] Information Commissioner's Office, 'What is a DPIA?' (2025) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/> accessed 2 August 2025.

[56] Case C-340/21 *VB v Natsionalna agentsia za prihodite* [2023] ECLI:EU:C:2023:986 [7], [29], [42].

[57] Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* [2023] ECLI:EU:C:2023:957 [5], [10], [50], [63], [67].

[58] Information Commissioner's Office, 'A guide to data security' (2025) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/> accessed 2 August 2025.

[59] European Data Protection Supervisor, 'Preliminary Opinion on privacy by design' (31 May 2018) <https://www.edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> accessed 2 August 2025.

[60] Case C-621/22 *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens* [2024] ECLI:EU:C:2024:857 [42], [51], [57], [58].

[61] Joined Cases C-17/22 and C-18/22 *HTB Neunte Immobilien Portfolio geschlossene Investment UG & Co. KG and Ökorenta Neue Energien Ökostabil IV geschlossene Investment GmbH & Co. KG v*

such as differential privacy, synthetic data, homomorphic encryption, zero-knowledge proofs, trusted execution environments, secure multiparty computation, and federated learning.[62] This also involves appointing and empowering a Data Protection Officer (Article 37 GDPR) with sufficient resources and genuine functional independence, as reinforced by CJEU judgments like *X-FAB Dresden*[63] and *KISA*[64]. A proactive, strategic mindset is essential for demonstrating a genuine commitment to data protection.

4.6. Prepare for the AI-Powered Threat Landscape and Multifaceted Extortion

The landmark decisions against 23andMe and Carrefour S.A. underscore a regulatory environment that punishes a reactive security posture.[65] Yet, the threat landscape is rapidly evolving with attackers utilising AI to industrialize their operations, a trend that intensifies the risk of multifaceted extortion, as detailed in the Cybersecurity Forecast 2025 report.[66] To counter this, organizations must fight AI with AI, positioning the technology as the defender's most powerful ally.[67] As highlighted in a recent Google blog, AI agents like "Big Sleep," a collaboration between Google DeepMind and Google Project Zero, proactively discover and foil vulnerabilities before they are exploited.[68] Furthermore, Google DeepMind's paper An Approach to Technical AGI Safety & Security emphasizes the need for robust

---

Müller Rechtsanwaltsgesellschaft mbH and Others [2024] EU:C:2024:738 [51], [59], [73], [74], [76], [78].

[62] Information Commissioner's Office, 'Privacy-enhancing technologies' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/> accessed 2 August 2025.

[63] Case C-453/21 *X-FAB Dresden GmbH & Co KG v FC* [2023] ECLI:EU:C:2023:79 [3], [5], [27], [44].

[64] Case C-560/21 *ZS v Zweckverband 'Kommunale Informationsverarbeitung Sachsen' KISA* [2023] ECLI:EU:C:2023:81 [3], [5], [22].

[65] Office of the Privacy Commissioner of Canada, 'Joint investigation into 23andMe Inc' (2025) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/> accessed 2 August 2025; AEPD, 'AEPD (Spain) - EXP202305979' (2023) <https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_EXP202305979> accessed 2 August 2025.

[66] Google Cloud, 'Cybersecurity Forecast 2025' (Google Cloud, 2025) <https://cloud.google.com/security/resources/cybersecurity-forecast> accessed 2 August 2025.

[67] *Ibid*.

[68] Kent Walker, 'A summer of security: empowering cyber defenders with AI' (Google Blog, 15 July 2025) <https://blog.google/technology/safety-security/cybersecurity-updates-summer-2025/> accessed 2 August 2025.

security and monitoring to mitigate misuse, validating that proactive, AI-driven defence is essential for building a resilient security posture. As systems approach artificial general intelligence (AGI), their ability to influence behaviour and cause harm necessitates proactive safety measures.[69] Embracing these advanced technologies is now critical for meeting the heightened regulatory expectations of the future.

5. Conclusion

In conclusion, the decisions against 23andMe and Carrefour S.A. serve as a powerful and unified message to all data controllers: a reactive, compliance-checklist mentality is no longer sufficient. These landmark cases, reinforced by CJEU jurisprudence, demand a proactive, risk-based approach to data security, with a firm commitment to robust authentication, continuous monitoring, and transparent communication. The significant financial penalties levied by both the ICO and AEPD serve as a potent deterrent, reinforcing that robust data protection is not merely a legal obligation but a fundamental business imperative for maintaining trust and avoiding severe regulatory consequences in the dynamic realm of European data protection law. Indeed, recent DPA enforcement actions, such as the Dutch DPA's investigation into the personal liability of Clearview AI executives, signal a shift towards holding management directly accountable for security failures.[70] As the threat landscape evolves with the advent of AI-powered attacks and multifaceted extortion,[71] a forward-looking data protection strategy is more critical than ever. The imperative for organizations is clear: they must not only learn the lessons of the past but also actively utilise new technologies to build a resilient and accountable security posture for the future, thereby safeguarding personal data and maintaining trust in an increasingly complex digital world.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

In the preparation of this work, the author utilized Google's Gemini to refine the language and enhance readability. The author exercised full human oversight and control over the content, meticulously reviewing and editing all output for accuracy and coherence. The author affirms full responsibility for the entirety of the work.

---

[69] Rohin Shah et al, 'An Approach to Technical AGI Safety and Security' (arXiv, 2 April 2025) [https://arxiv.org/abs/2504.01849] accessed 2 August 2025

[70] DLA Piper, GDPR Fines and Data Breach Survey: January 2025 (DLA Piper, January 2025) [https://www.dlapiper.com/en/insights/publications/2025/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2025] accessed 2 August 2025.

[71] Google Cloud, 'Cybersecurity Forecast 2025' (Google Cloud, 2025) <https://cloud.google.com/security/resources/cybersecurity-forecast> accessed 2 August 2025.

Declaration of Competing Interest

The author declares no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.