

The economic costs of weakening privacy and data protection

Full Report

September 2026



About this study

In light of the European Commission's proposed Digital Omnibus package, BEUC asked Assembly to conduct an economic analysis of the impact on European consumers and businesses of a failure to protect existing EU privacy and data protection regulation.

Research correct as of September 2026.

About Assembly

Assembly produces custom and subscription-based research on regulatory, policy, and legislative developments in communications markets and the digital economy.

For more information visit assemblyresearch.co.uk

About BEUC

BEUC – The European Consumer Organisation – is the umbrella group for 42 independent consumer organisations from 31 countries, representing them to the EU institutions and defending the interests of European consumers.

For more information visit beuc.eu

Disclaimer

BEUC is co-funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority (EISMEA) can be held responsible for them.

Contents

Executive summary	3
Quantifying the economic costs of weakening Europe's privacy and data protection	4
Key messages	5
Introduction	6
The cost to consumers of inadequate privacy and data protection measures	8
Analysing the secondary data market	20
The costs to companies of failing to properly implement privacy safeguards	28
The potential economic benefits of higher standards of data protection	41

List of figures and tables

Figure 1: The top five violations of the GDPR

Figure 2: Fraudulent uses of personal data perceived by individuals in the last three years

Figure 3: Estimated values of different personal data items

Figure 4: The data value gap

Figure 5: Post-breach declines in share prices

Figure 6: The six largest fines under the GDPR to date

Table 1: Common violations of the GDPR

Table 2: Examples of data brokers and providers in Belgium

Table 3: Risks associated with eight types of data brokers and providers

Table 4: Cost of non-compliance with the GDPR

Table 5: Analysis of cyberattack portfolio companies against S&P 500 returns

Executive summary

The Charter of Fundamental Rights of the European Union was declared in December 2000, underlining privacy and the protection of personal data as fundamental rights that reflect the bloc's universal values of human dignity, freedom, equality and solidarity.¹ In the years since, and in response to the growth in concerns around consumer data, privacy legislation has become a central component of the regulatory landscape, shaping the development of the modern digital economy. The General Data Protection Regulation (GDPR) set out a bold vision for consumer rights in the digital age and is widely considered the gold standard in data protection legislation. However, the 'Digital Omnibus' proposal, published by the European Commission (EC) in November 2025, risks weakening it in pursuit of regulatory simplification, which could have significant consequences for consumers.

Businesses increasingly rely on consumer data for decision-making and personalised services. While consumer consent is usually required for businesses to collect and use their personal data, it is often further processed and resold downstream without the consumer's knowledge. We estimate the market for the secondary resale of consumer data to be worth around €40.5bn, highlighting the scale of this further use of data. Data protection regulation should better enable consumers to exercise more control over their personal data and stop it from being used without their consent if they wish.

The implementation of robust data protection regulation has economic implications for both businesses and consumers. Consumers would benefit from having more control over their personal data, making them more confident in their online interactions. Stronger protections could similarly limit the harmful impacts of the increasingly relevant "attention economy". While businesses may feel burdened by stronger protections, they would benefit from the improved regulatory clarity and certainty over how they can use and process consumer data.

¹ [The Charter of Fundamental Rights of the European Union](#), EUR-Lex

Quantifying the economic costs of weakening Europe's privacy and data protection



€1.9bn

The annual cost to consumers of not being able to exercise their rights of access, erasure and data portability



€40.5bn

The estimated value of the secondary data market



€406m

The annual cost to consumers due to the lack of involvement or appointment of a data protection officer



€107.57

The annual cost per European citizen of the resale of their personal data in the secondary data market



€103bn

The annual cost to consumers of organisations' non-compliance with information security rules



€25bn

The annual cost to organisations in the EU of downtime as a result of privacy breaches



€508m

The potential annual cost to consumers of Meta's 'pay or consent' model

Key messages

- While the processing of data can promote competition and innovation in the development of new services, it can pose significant risks for consumers. Breaches of protections provided for by the GDPR, from the use of data without sufficient legal basis to the inability of consumers to exercise their rights, can cause billions of Euros worth of harm per year.
- Cybersecurity-related data breaches potentially represent the most severe and financially consequential incidents for consumers. Despite the regulation's requirements, we estimate that organisations' non-compliance carries a cost to consumers in the EU of €103bn per year, with implications for their future engagement with, and trust in, digital services generally.
- The secondary data market trades valuable consumer data for businesses across the economy, often without the prior knowledge, understanding or meaningful consent of consumers. We estimate the market to be worth approximately €40.5bn, with close to €108 of value being extracted from every EU citizen each year.
- Though there are accepted costs related to meeting the requirements of the GDPR, they are far outweighed by the costs to organisations and the wider European economy of non-compliance. Potential operational, economic and regulatory costs indicate why ensuring a strong level of data protection must be a first-order priority.
- Strengthening the EU's data protection framework with a selection of targeted amendments would allow consumers to more meaningfully control and consent to how their data is used, which would improve their own online experiences. New measures in certain areas would further benefit the wider economy through increased competition and greater regulator certainty for businesses.

Introduction

In May 2016, the EU adopted the GDPR, outlining explicit protections for the personal information of European citizens while ensuring that the free movement of personal data is neither restricted nor prohibited. Prior to this milestone, the Charter of Fundamental Rights had outlined – under Articles 7 and 8 – the right of citizens to privacy and to the protection of their personal data, including that it is processed fairly for specified purposes. The EU Data Protection Directive had also attempted to set a common minimum standard for data protection between Member States. However, as a directive, it was transposed differently across the EU, resulting over time in a fragmented and increasingly complex regulatory landscape.

The GDPR's application from May 2018 set a new and consistent benchmark for data protection, providing individuals and organisations legal clarity in how personal data could be used, influencing the shape of data protection frameworks globally. Its success also made it an integral part of the EU Digital Single Market, which had emerged around the same time in order to remove regulatory and trade barriers in the digital space.

On 19 November 2025, the EC presented its Digital Omnibus, a package of measures covering the GDPR, ePrivacy Directive, AI Act and Data Act, which outlines various proposals to clarify or amend the application, articulation and obligations of the relevant legislative texts. The reaction from across the political spectrum to the Omnibus has been mixed, with European Parliament group Renew warning the EC against straying from the GDPR's core principles, while several EU Member States (including Austria, Estonia, France, Slovenia) have stated firm opposition to any rewrite of the regulation.²

In pursuit of regulatory simplification, the EC has put forward a broad set of changes to the GDPR and ePrivacy Directive, which would enable companies, for example, to:

- No longer have to treat information as personal data if they cannot reasonably identify the natural person to whom the information relates;
- More easily implement cookies and tracking technologies; and

² [The EU's digital simplification package](#), Assembly Research, 2025

- Rely upon the use of legitimate interest as a means of processing personal data, e.g. to train and run AI systems.

Michael McGrath (Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, EC) has stated that the GDPR remains the global benchmark for privacy regulation and that there is no appetite within the EC to reopen the framework in its entirety.³ In his view, the Digital Omnibus proposal includes balanced and targeted measures to clarify GDPR provisions, upholding the regulation's core principles while cutting red tape and accounting for technological developments as well as new legislation, opinions and case law.

While the EC's proposed amendments and adjustments to the GDPR seek to ensure appropriate safeguards are implemented, including for the collection and processing of special categories of personal data, they may nevertheless have the potential to impact the privacy rights of European consumers, and in turn their ability to safely participate in the digital economy. Whereas compliance with, and enforcement of, privacy and data protection regulation delivers positive outcomes for consumers, companies and the economy, there are economic costs on each count from non-compliance, from ex-post financial penalties to loss of customers, which could be exacerbated should rules be weakened or relaxed.

³ [Event debrief: The 15th Annual European Data Protection and Privacy Conference](#), Assembly Research, 2026

The cost to consumers of inadequate privacy and data protection measures

Note on structure and interpretation

The analysis below is organised by categories of GDPR infringements commonly reflected in enforcement statistics and fine classifications. This structure is used for analytical clarity and to support economic assessment. However, it should not be read as implying that these categories operate independently under the GDPR.

In practice, the economic harms described typically arise from failures to realise the GDPR's core principles set out in Article 5 (in particular, fairness, transparency and purpose limitation), with specific obligations (e.g. on consent, transparency, data subject rights or security) functioning as operational mechanisms through which those principles are given effect. Accordingly, individual infringement categories often overlap in practice, and the same underlying conduct may engage multiple obligations while reflecting a single, principles-level failure.

Estimating the costs to citizens of privacy breaches

With the digital transformation of the European economy, the collection and use of consumer data are now central to the activities of many business models and companies – not least large-scale online platforms. Within data-driven economies, consumers – who make economic choices in a market – are also “data subjects” within the meaning of data protection, whose “informational self-determination” is protected by the GDPR.⁴ In parallel, personal data protection has been found to be a “parameter of quality” that consumers take into account when making their consumption choices.

While the processing of data can promote competition and innovation in the development of new services, it can pose significant risks for consumers, which may be especially acute absent appropriate protections. The potential costs of data breaches driven by inadequate privacy and data protection measures differ from those harms caused by cybercriminality in that they do not necessarily involve data that was compromised.⁵ Instead, they often involve the collection or use of data in ways that consumers did not consent to or were

⁴ [Competition and personal data: a common ambition](#), Autorité de la concurrence and CNIL, 2023

⁵ The EU has adopted a portfolio of legislation to protect the bloc from cyberthreats, including the Cybersecurity Act, the Cyber Resilience Act and the NIS2 Directive. The aims of these pieces of legislation differ from the security-related provisions of the GDPR, which focus on the protection of personal data and notification and communication obligations in the event of a breach.

not notified about. Even where legislation is in force, there are various ways in which data rules can be breached and rights to privacy violated – see *Table 1*. In fact, since (and indeed despite) the GDPR’s application, a number of major incidents have occurred that have led to the inappropriate use or exposure of citizens’ data.

Table 1

Common violations of the GDPR

Based on number of fines issued

Violation	Example	Relevant GDPR article(s)
Insufficient legal basis for data processing	Meta (Ireland, 2023): Incorrect reliance on the contract legal basis for processing operations	Article 6
Non-compliance with general data processing principles	Acea Energia (Italy, 2025): Reuse of data for unexpected marketing purposes	Article 5
Insufficient technical and organisational measures to ensure information security	Marriott International (UK, 2020): Data breach following the acquisition of Starwood	Articles 32-34
Insufficient fulfilment of data subjects rights	Google (Sweden, 2020): Failure to remove search result listings	Articles 15-22
Insufficient fulfilment of information obligations	Facebook (Ireland, 2021): Failure to be transparent about the sharing of WhatsApp data	Articles 13 and 14
Insufficient cooperation with supervisory authority	TIMSHEL (Poland, 2022): Lack of responses to the national supervisory authority	Article 31
Insufficient fulfilment of data breach notification obligations	Psykoterapiakeskus Vastaamo (Finland, 2021): Failure to report a security breach on time	Article 33

Source: Assembly, CMS.Law

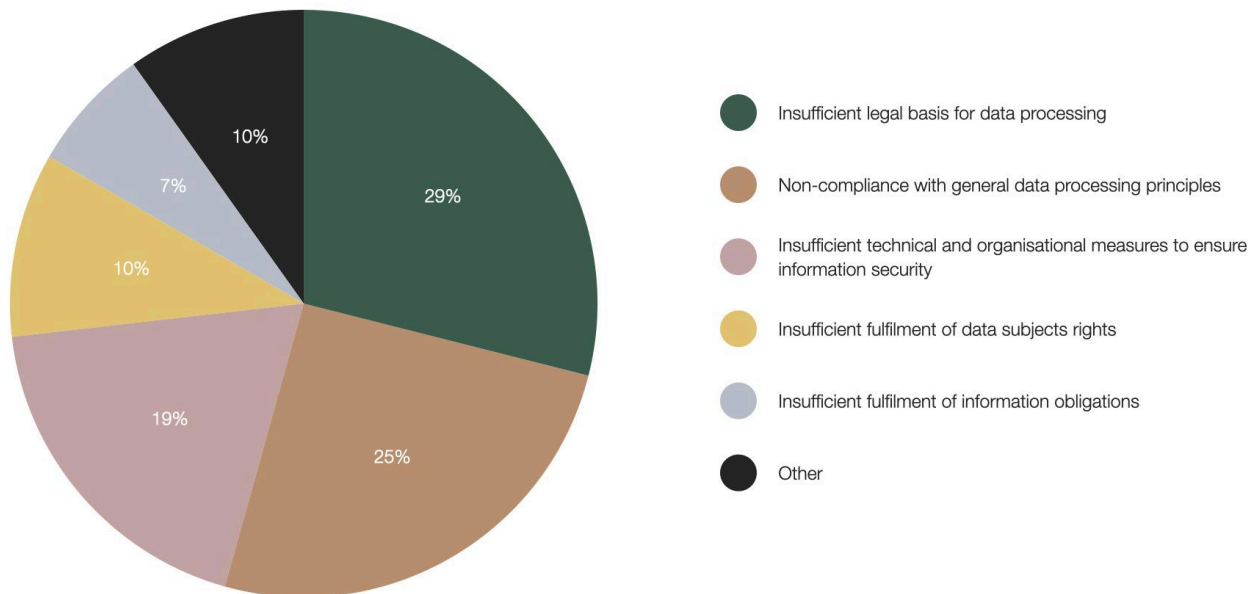
Though breaches of the GDPR may not always lead to fines, and in turn those fines are not always made public, the application of financial penalties provides an indication of how consumers’ privacy has been violated since the regulation came into force. Five types of breach account for just over 90% of all fines (close to 3,000) issued under the GDPR to date – see *Table 2*.⁶ Such incidents may give rise to a wide range of material economic risks and costs for consumers, which can be compounded by the fact that once leaked, data is difficult to recover or invalidate, and misuse can continue for years.

⁶ [GDPR Enforcement Tracker](#), CMS.Law (correct as of 19 May 2026)

Figure 1

The top five violations of the GDPR

Share of total, based on number of fines issued



Source: Assembly, CMS.Law

Insufficient legal basis for data processing

Article 6 of the GDPR⁷ requires every processing activity to have a lawful basis. Pre-ticked checkboxes and bundled consent forms that are acceptable in different countries outside of the EU can violate GDPR consent requirements. The same goes for cookies that force users to accept tracking.

In October 2023, the European Data Protection Board (EDPB) issued an urgent binding decision banning Meta's use of personal data for behavioural advertising across its Facebook and Instagram platforms, in particular prohibiting the firm from citing the use of personal data in pursuit of "legitimate interests".⁸ Later that month, Meta responded by announcing the rollout of a paid subscription plan for Facebook and Instagram users in the EU, which became available for purchase from November 2023.⁹ The result of this 'pay or consent' (alternatively, 'pay or okay') model is that consumers within the EU must either accept that their information is used for personalised advertising or pay a monthly subscription fee of between €5.99 and €7.99. Based on the number of active users across the two platforms and academic research on willingness to pay,¹⁰ the model implies a new source of revenue generation for

⁷ [Regulation \(EU\) 2016/679 of the European Parliament and of the Council](#)

⁸ [GDPR: Meta required to change behavioural advertising practices](#), Assembly Research, 2023

⁹ [Double-dipping in the moderation of Meta](#), Assembly Research, 2024

¹⁰ Research suggests that 99% of users of online news services choose the tracking option when confronted with a pay-or-tracking wall. See [Paying for Privacy: Pay-or-Tracking Walls](#), Müller-Tribbensee, Miller & Skiera, 2024

Meta – or a potential new cost to consumers in the EU to protect their privacy – of up to **€508m** annually.

BEUC and national consumer agencies have argued that Meta's model is not compliant with the GDPR, EU consumer law or the Digital Markets Act (DMA).¹¹ Similarly, Forbrukerrådet (the Norwegian Consumer Council) has filed a complaint with Datatilsynet (Norway's data protection authority, DPA) that news publisher Shibsted's introduction of a NOK49 (€4.45) pay or okay model violates consumers' right to privacy.¹²

€508m

**The potential annual cost to consumers of
Meta's 'pay or consent' model**

Non-compliance with general data processing principles

One of the principles under Article 5 GDPR is 'fairness' – i.e. an organisation should not process personal data unlawfully, unfairly or in an untransparent manner. In September 2023, the Irish Data Protection Commission (DPC) adopted its final decision regarding its inquiry into TikTok, finding that between 31 July 2020-31 December 2020, the platform had breached principles contained within Article 5 as a result of:

- The profile settings for child user accounts were set to public by default, meaning anyone (on or off the platform, including non-TikTok users) could view content posted by child users;
- The 'Family Pairing' setting allowed non-child users (who could not be verified as a parent or guardian) to pair their account to a child user's account and enable Direct Messages for child users aged 16+, posing severe possible risks to child users; and
- TikTok used 'dark patterns' by nudging users towards choosing privacy-intrusive options during the registration process and when posting videos.¹³

The findings were communicated alongside findings that TikTok had also breached aspects of Articles 12, 13, 24 and 25 of the GDPR. The DPC subsequently imposed an administrative fine of €345m, while ordering the platform to take steps to ensure compliance with the GDPR within a three-month period. Further, the Italian DPA (Garante per la protezione dei dati personali – known as the Garante) has repeatedly fined companies for

¹¹ [BEUC assessment of Meta's latest pay-or-consent policy for Facebook and Instagram users](#), BEUC, 2025

¹² [The Norwegian Consumer Council complains about Schibsted's demand for payment for privacy protection](#), Forbrukerrådet, 2026

¹³ [Irish Data Protection Commission announces €345 million fine of TikTok](#), DPC, 2023

excessive data collection and reuse for marketing purposes that went beyond what consumers were told or could reasonably expect.

Such practices lead to direct costs for citizens who are subjected to unexpected uses of their data, including profiling, behavioural advertising or secondary marketing that may disadvantage them financially. Consumers must also invest time trying to understand opaque data practices or exercising rights to limit misuse – something made all the more difficult by the vast quantity of personal data collected and shared nowadays.¹⁴ The Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv) has called for new EU legislation to ban tracking and profiling for advertising purposes, stating that they lead to manipulation, discrimination and loss of trust.¹⁵ Further, dark patterns that manipulate consumers into accepting excessive data collection increase their long-term exposure to profiling and misuse, raising the likelihood of future harm (e.g. price discrimination, erosion of privacy) while solely benefitting the organisation carrying out this behaviour. Research has highlighted how tech firms have used dark patterns and default settings – which most consumers do not change – to nudge users towards the least privacy friendly options to a degree that may be unethical, while giving those same users an “illusion of control” over how their data is used.¹⁶

Insufficient fulfilment of data subjects rights

Chapter 3 of the GDPR, spanning Articles 15-22, sets out provisions covering rights of the data subject, effectively granting consumers rights to access, rectify, erase and port their data within a specified time window. In particular, Article 17 outlines the right to erasure (i.e. the right to be forgotten), incorporating a long-standing principle under European data protection laws and codifies the landmark ruling by the Court of Justice of the European Union (CJEU) in the 2014 “Google Spain” case.

In March 2020, the Swedish DPA (Integritetsskyddsmyndigheten, or IMY) imposed a fine of SEK75m (€6.9m) on Google for failure to comply with the GDPR.¹⁷ The IMY stated that Google, as a search engine operator, had not fulfilled its obligations in respect of the right to request delisting, criticising the fact that Google did not properly remove two of the search result listings that the authority had ordered the firm to remove in 2017.

Based on fines issued under the GDPR, we estimate that there were over 16,500 privacy breaches relating to data subjects rights in 2025.¹⁸ We have focused on three specific rights within the regulation (access, erasure and data

¹⁴ [Surveillance advertising, privacy & data protection](#), Sveriges Konsumenter, 2021

¹⁵ [Personalised Advertising: Overdue Regulation](#), vzbv, 2025

¹⁶ [New analysis shows how Facebook and Google push users into sharing personal data](#), Forbrukerrådet, 2018

¹⁷ [Swedish Authority for Privacy Protection imposes administrative fine on Google](#), IMY, 2020

¹⁸ This figure uses the share of fines issued for breaches of data subject rights as a proxy to estimate the number of breaches related to this type of violation in the latest full year. Data sourced from [GDPR Enforcement Tracker](#), CMS.Law (correct as of 19 May 2026) and [Personal data breaches in Europe reach 443 per day in dramatic 22% jump](#), DLA Piper, 2026

portability), assuming that each accounts for a third of the total number of violations. Leveraging upper bound and lower bound costs for the three rights, reflecting the monetary values surveyed individuals place on them,¹⁹ we have estimated a mean harm to affected consumers, which has subsequently been multiplied by the average number of records exposed per breach. This calculation suggests that the failure of organisations to comply with Articles 15, 17 and 20 is equivalent to an annual economic cost to consumers in the EU of just below **€1.9bn**.

€1.9bn

The annual cost to consumers of not being able to exercise their rights of access, erasure and data portability

However, this figure does not represent the full harm to consumers of non-compliance with data subjects rights. For instance, there can be direct costs to consumers if they do not know what data an organisation holds on them (such as the risk of identity fraud or potentially unclaimed compensation) or if they have to spend their own time chasing organisations for access, erasure or portability. Further, where organisations breach the accuracy principle of the GDPR (Article 5(1)) and consumers do not exercise their right to rectification under Article 16, inaccurate or outdated data that continues to be used in decisions affecting credit, services or employment. In light of estimates that nearly one in three people (32%) who checked their credit report in the past five years found a mistake,²⁰ there is a clear risk for the majority of consumers of incorrect credit scores affecting their ability to buy a property or take out car insurance. The potential costs only build over time the longer a credit report goes unchecked. Such concerns can also persuade consumers of the need to sign up to premium credit monitoring services, fuelling a rapidly expanding market. This poses a further burden on consumers' finances.

Insufficient fulfilment of information obligations

Within the same Chapter, the GDPR aims to ensure that people have insight into how businesses are handling their data. As such, individuals should have a right to know what data an organisation is collecting and what they are doing with it. Specifically, under Articles 12-14, organisations must explain data collection and processing in clear and plain language. Fines often target privacy policies that omit details about third-party sharing or do not accurately reflect the processing activity on an organisation website.

¹⁹ [Research and analysis to quantify the benefits arising from personal data rights under the GDPR](#), London Economics, 2017

²⁰ [Credit reports mistakes widespread – is your score wrong?](#), Which?, 2024

For example, in January 2019, the Commission nationale de l'informatique et des libertés (CNIL) handed out the first major sanction under the GDPR after ruling that Google had not given users sufficiently clear, transparent information about advertising personalisation, and that consent for personalised advertising had not been validly obtained.²¹ Information was buried across multiple pages and required up to five or six clicks to surface. In September 2021, the Irish DPC then issued its first significant financial penalty under the regulation, fining Facebook €225m for failing to comply with transparency requirements on how it uses personal data gathered by WhatsApp and shared across other Facebook platforms.²²

Breaches of Articles 12-14 can lead to costs for citizens as when data processing is not transparent in practice, individuals cannot make informed choices about engaging with a given service, while behavioural advertising and profiling are able to operate without meaningful awareness. In turn, this can lead to distorted purchasing decisions, exposure to targeted, differential pricing or nudging, and/or a reduced ability to compare services on a fair basis. In addition, because processing is not fair or transparent, consumers must invest time trying to decipher long and complex privacy documentation. It has been estimated that just reading all the privacy policies of the apps downloaded on the average smartphone, excluding browsed websites, would take the best part of a day (22.4 hours).²³ Exercising data rights therefore becomes harder because individuals do not know what to object to, with the cost of transparency effectively shifted from the controller to the consumer. Further, a lack of substantive transparency allows profiling to persist unchallenged, data to be reused across advertising and analytics ecosystems, and long-term consumer profiles to develop without effective scrutiny. These profiles influence how individuals are treated across services over time, creating cumulative and difficult-to-reverse economic effects.

Additional breaches of the GDPR

In the “Other” <10% of fines issued since the GDPR came into effect are relatively rare instances of penalties occurring as a result of the lack of appointment of a data protection officer (DPO). Under Article 37, data controllers and processors are required to designate a DPO, who – under Article 39 – undertakes tasks, including advising on and monitoring compliance with the regulation, and training of staff involved in processing operations.

Based on fines issued under the GDPR, we estimate that there were 1,350 privacy breaches relating to the lack of involvement or appointment of a DPO in 2025. Leveraging upper bound and lower bound estimates for the costs of a data breach in Europe and the expected share of those costs borne by

²¹ [The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC](#), EDPB, 2019

²² [Ireland issues its first large GDPR fine](#), Assembly Research, 2021

²³ [Eliminating Deceptive Privacy Practices: Building Trust by Addressing Privacy Dark Patterns](#), ISACA, 2023

consumers,²⁴ we have focused on the expected benefit of designating a DPO in terms of reducing the risk that one type of activity (phishing) results in a data breach.²⁵

Given the reduction in successful phishing attacks as a result of DPO training, we are able to calculate high and low estimates for the benefit to consumers of the involvement or appointment of a DPO – i.e. the harm incurred if a DPO is not designated. This calculation suggests that the failure of organisations to comply with Articles 37, 38 and 39 is equivalent to an economic cost to consumers in the EU of **€406m** per year. In other words, it is the value consumers are unable to benefit from due to the lack of a DPO. As this figure focuses on phishing, we would expect additional harm to be realised by organisations without a DPO, including costs relating to cooperation with the relevant supervisory authority as well as general data protection practices.

€406m

The annual cost to consumers due to the lack of involvement or appointment of a DPO

The impacts of cybersecurity incidents

Beyond unlawful practices under the GDPR, cybersecurity-related data breaches potentially represent the most severe and financially consequential incidents for consumers. As people increasingly rely on new data-driven services and products, they have also become more vulnerable to theft, hacking and misuse (including the sale of stolen profiles on the dark web) – particularly where data protections are inadequate. The GDPR subjects the processing of personal data to security obligations, principally:

- Article 32: The obligation to implement measures safeguarding an appropriate level of security; and
- Articles 33 and 34: The obligation to notify the competent authority in case of a personal data breach or, when there is a high risk, to communicate the breach to the affected individuals.

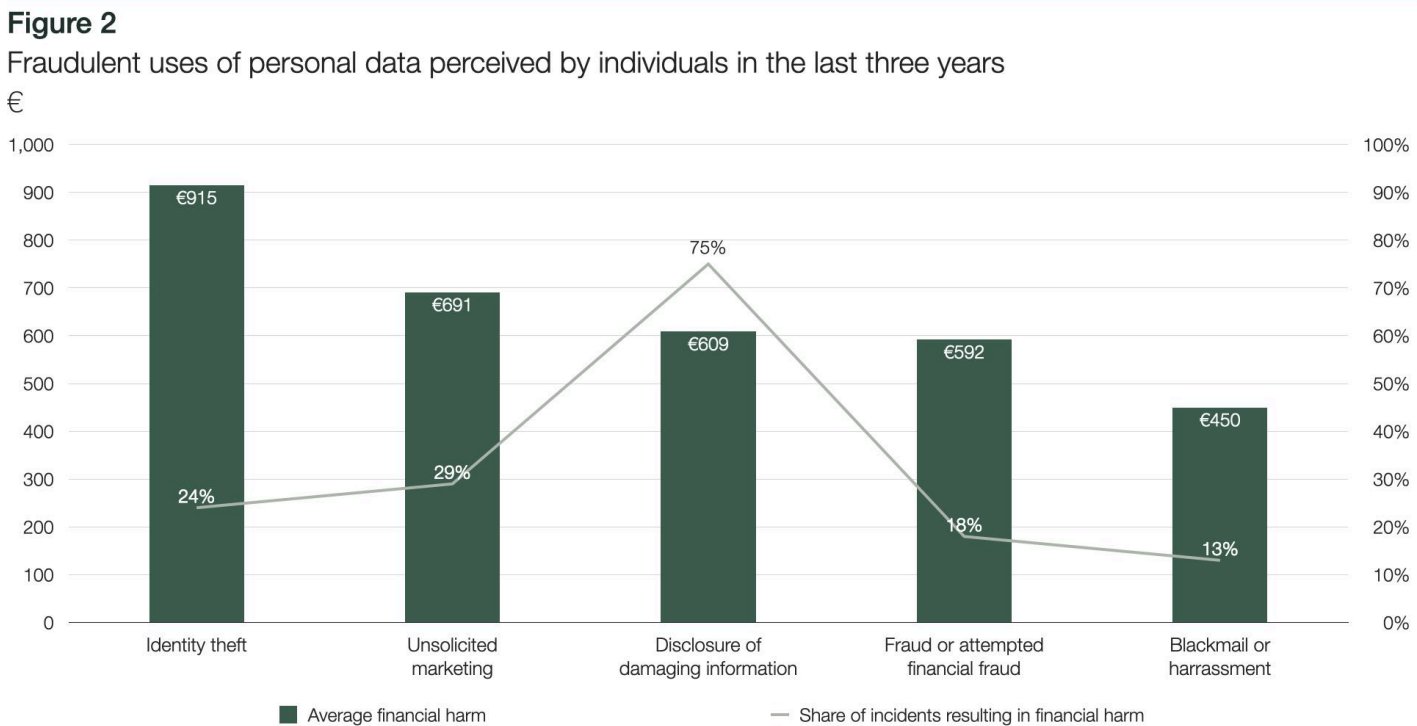
In this context, the level of cybersecurity protection an organisation deploys depends on the investment it makes into doing so, which is weighed against its cost and the risk of cyberattacks. However, this calculation overlooks externalities, the impacts of that investment on wider society, which lead to suboptimal investment in security in the absence of regulation (such as the GDPR). For criminals, underinvestment increases the profitability of cybercrime, particularly through ransomware (attacks that aim to extort a ransom), with their attacks more likely to succeed. The result is a vicious cycle, in which higher success rates strengthen criminals' ability to demand higher ransoms and

²⁴ [Cost of a Data Breach Report 2025](#), IBM, 2025

²⁵ [What are the economic benefits of having a DPO for a company?](#), CNIL, 2025

ultimately boost both the profitability and the severity of their malicious activities.

Equally concerning are the externalities affecting consumers, with data breaches enabling the launch of subsequent cyberattacks against individuals (such as phishing, identity theft, credential stuffing), who may not always be able to identify which company is responsible for the leak of their personal information.²⁶ While cybercrime is a well-known phenomenon, it has been considered that its actual impact for individuals remains difficult to quantify, imposing both financial and non-financial harms. According to research, over a fifth of consumers in France that have experienced fraudulent use of their data have suffered financial damages as a result.²⁷ The average declared financial loss is €740 – a tangible impact that would disproportionately affect lower-income individuals (see *Figure 2*). Identity theft stands out as the type of breach leading to the highest financial damage, with an average loss of €915. Further, the research suggests that a minority of consumers (14%) suffered damages exceeding €1,000, highlighting the highly uneven distribution of cybercrime-related harms.



Source: Assembly, CNIL

²⁶ [Cybersecurity: The Economic Benefits of GDPR](#), CNIL, 2025
²⁷ [Cybercrime: what risks and consequences for personal data?](#), CNIL, 2025

Based on fines issued under the GDPR, we estimate that there were over 30,500 privacy breaches relating to poor information security in 2025. We have focused on the five fraudulent uses of personal data identified in *Figure 2*, calculating their likelihood of occurring as a result of security incidents and the prospect such instances would lead to financial harm for consumers. Leveraging the average financial harms experienced, we have estimated a cost to affected consumers per use, which has subsequently been multiplied by the average number of records exposed per breach. This calculation suggests that the failure of organisations to comply with Articles 32, 33 and 34 is equivalent to an annual economic cost to consumers in the EU of over **€103bn**.

These events have significant non-financial consequences' according to the CNIL, 67% of consumers become more risk averse, altering their behaviour to reduce their perceived risk of harm reoccurring. Cybersecurity incidents also have a lasting impact on individuals' trust; they lead to greater distrust and to the abandonment of certain digital services, particularly online shopping. 57% of individuals who suffered harm over the past three years reported giving up using a digital service out of fear that their personal data might be misused, compared with 35% for the general population.²⁸

57%

The share of consumers that no longer use a digital service due to concerns over misuse of their personal data

Additionally, people may be at an increased risk of psychological harm due to emotional distress (e.g. anxiety, fear, embarrassment) following a personal data breach. For instance, the disclosure of patient records or similar sensitive information could exacerbate an individual's existing trauma, affecting their mental health and potentially leading to impacts on their physical well-being.²⁹ Alarming, 30% of victims report emotional distress, yet 25% receive no support from the organisations responsible.³⁰

Case studies on breaches of the GDPR

Cyberattacks can affect firms regardless of the sector in which they operate, as well as public institutions of all sizes. Below we provide case studies of four recent, criminally-engineered data breaches since the application of the GDPR, considering the privacy and financial impacts on consumers.

²⁸ [Cybercrime: what risks and consequences for personal data?](#), CNIL, 2025

²⁹ [Identifying the harms and impact of a personal data breach](#), ICO, 2024

³⁰ [Ripple effect: the devastating impact of data breaches](#), ICO, 2024

Eurail

In December 2025 and February 2026, European rail pass operator, Eurail, suffered a major data breach that reportedly exposed 1.13TB of data.³¹ It has been reported that approximately 309,000 people may have been affected, with their personal data being offered for sale on the dark web. These datasets include names, dates of birth, passport numbers, email addresses, phone numbers, home addresses and travel information. In the UK, some consumers who had used the Eurail service were advised to replace their passports, costing each person £102 (€117.46).³² The attack has additionally impacted the DiscoverEU programme, a publicly funded travel scheme that is part of the Erasmus programme. Participants in the programme were notified of the data breach and warned that their personal data may have been exposed.

Odido

In February 2026, Odido, a mobile telecoms operator in the Netherlands, suffered a cyberattack that stemmed from multiple voice phishing calls to its customer service team, with the attackers pretending to be members of Odido's IT staff.³³ Although the attackers' access to Odido's IT systems was quickly revoked, the attack was reportedly very sophisticated, leading to data exfiltration. The data breach impacted approximately 6.39m customers of Odido or Ben (an Odido sub-brand). The data affected included information such as names, addresses, mobile numbers, email addresses, IBAN numbers, dates of birth, identification details, nationalities and genders.

³¹ [The Biggest Cyber Attacks Year by Year](#), Amtivo, 2026

³² [Some Interrail travellers told to cancel passports as hacked data posted online](#), The Guardian, 2026

³³ [Update about cyberattack](#), Odido, 2026

EC

In March 2026, one of the EC's Amazon Web Services (AWS) accounts was compromised. CERT-EU, the EU institutions' cybersecurity service, found that a malicious actor had acquired an AWS application programming interface (API) key that gave them access to one cloud account associated with the EC.³⁴ The hackers stole approximately 92GB of data, 2GB of which mostly consists of sent email messages. CERT-EU has stated that most of these messages were automated and did not include material content, but cautioned that in instances where messages bounced back, the personal data of recipients may have been put at risk, and confirmed that such data has been exposed. ShinyHunters, the cybercrime group behind the hack, has claimed to have stolen "data dumps of mail servers, datavases [sic], confidential documents, contracts, and much more sensitive material".

Council of Europe

In June 2026, the Council of Europe, an international human rights organisation, suffered a data breach that reportedly exposed documents³⁵ containing personal employee details such as:

- Full names;
- Addresses;
- Phone numbers;
- Dates of birth (DOB);
- Salaries;
- Bank details;
- Tax and social security information; and
- Medical records.

Due to the sensitive nature of the Council of Europe's human rights casework, exposing employees' personal data creates significant security risks, such as potential targeting by hostile actors.

³⁴ [European Commission cloud breach: a supply-chain compromise](#), CERT-EU, 2026

³⁵ [Hackers claim massive Council of Europe breach: troves of personal data exposed](#), Cyber News, 2026

Analysing the secondary data market

According to the European Data Protection Board (EDPB), the secondary data, or data broker, market refers to the market where personal data is bought and sold by data brokers, which “collect, aggregate, analyse, and resell personal data, often without any direct interaction with the individuals concerned”.³⁶ This data is acquired in a variety of ways by brokers such as by purchasing it from private companies and government agencies, extracting information from publicly available sources such as property records, voter registrations, and court documents, and by scraping social media platforms.

This collection of personal data is often conducted without the consent or knowledge of consumers, who are also usually unaware of how this data is being collected and used by brokers. The aggregation and analysis of collected personal data allow brokers to develop consumer profiles, detailing information originating from multiple different sources about individuals. These profiles are then monetised via their sale to third parties, who use the profiles for a variety of purposes such as targeted advertising.

Identifying the key secondary data market players in Europe is challenging given the market’s relatively obscure nature and operation, with limited information available on turnover and often on number of employees. However, the EDPB’s report identified eight different types of data providers and brokers in the Belgian market, highlighting relevant organisations based on the use of targeted keywords in online searches (see *Table 2*).³⁷

³⁶ [Data brokers market study](#), EDPB, 2026

³⁷ [Data brokers market study](#), EDPB, 2026

Table 2
Examples of data brokers and providers in Belgium

Name	Type	Turnover	Employees
GeoPostcodes	Personal data broker	Not available	19
DPG Media Datalab	Data pool and data cleanroom	€550m	1,206
Kinesso (IPG Mediabrands)	Data pool and data cleanroom	€32.5m	8
MoodMe	AI platform integrating personal data	€14,485	1
Bonex	Data provider of self-generated data (individual level)	Not available	66
OpenTheBox	Business data broker	€88.5m	289
Altares.be	Business data broker	€13.4m	33
Cegeka (UrbanSense and Mobilize)	Data provider of aggregated data with reidentification risk	€390m	1,064

Notes: 1. Some organisations selected based on the availability and size of turnover and number of employees 2. Data from 2023 or 2024
Source: EDPB

For each of the eight types of data brokers and providers, the EDPB then identified the severity of the associated privacy risks, with four considered to be in the high-risk category (see Table 3).

Table 3
Risks associated with eight types of data brokers and providers

	Data collection	Data processing	Monetisation	Control by individual	Preliminary privacy risk
Personal data broker	Multiple public and private sources	Processing, aggregation, profiling	Sold or exchanged	No	High
Data pool and data cleanroom	Collaboration between firms	Processing, aggregation, profiling	Sold or exchanged between partners	Yes	High
AI platform integrating personal data	Multiple public and private sources	AI algorithm training, profiling	Technology product	No	High
Data broker with user control	Multiple public and private sources, user provided	Processing, aggregation, profiling	Sold or exchanged	Yes	High
Data provider of self-generated data (individual level)	Generated by the firm	Raw data processing and/or profiling	Sold or included as part of technology product	Varies	Medium
Business data broker	Multiple public and private sources	Database of raw data	Sold or exchanged	No	Medium
Data marketplace	Platform for data providers and data consumers	Raw data	Sold or exchanged on the marketplace's platform	Varies	Medium
Data provider of aggregated data with reidentification risk	Multiple public and private sources	Processing and aggregation	Sold or exchanged	No	Medium

Source: EDPB

Estimates show that the European secondary data market could be worth as much as €40.5bn

The estimated value of the global data broker market (secondary data market) in 2026 is approximately \$345.1bn (€294.2bn)³⁸, which adjusted by the EU's proportion of world GDP³⁹ or trade⁴⁰ for the same year, would value the bloc's data broker market between €26.7bn and €40.5bn. This estimate closely reflects the EC's own assessment of the EU's wider data market, in its 2024-2026 European Data Market Study (which is still ongoing).⁴¹ The EC's initial study forecasts the 2026 value of the EU market for 'data monetisation' – defined as "the revenue that data suppliers get from selling data. In the data economy" – at approximately €40bn. Although this forecast aligns closely to the higher-end estimated value of the EU's data broker market, the EC is clear that it considers data monetisation "as an additional direct impact, generated at the level of supplier companies", rather than being generated by brokers, who resell this data from supplier companies.

Despite this distinction between the data monetisation and data broker markets, it is likely that much of the latter acquires its data from the former, before continuing to resell or repackage (into products such as consumer profiles) and resell this data. As a result, the estimated €26.7bn-€40.5bn range of the EU's data broker market seems justified, given its resale of data that originates from these supplier companies.

€40.5bn

The estimated value of the secondary data market

It is worth noting that a number of other, larger downstream markets rely on the secondary data market. Most notably, the digital advertising market is notorious for its use of personal data to strengthen the targeting of its advertising. In 2024, the digital advertising market was valued at €118.9bn.⁴² Across advertising as a whole, estimates show that about two-thirds of all spending is now focused on digital rather than traditional advertising. This significant market size and clear focus on digital advertising highlights the importance and monetary value of personal data, which plays an essential role in the digital advertising market.⁴³ Personal data is similarly important to other markets such as credit and financial risk scoring, insurance pricing, and wider consumer intelligence services.

³⁸ [What are data brokers?](#), Incogni, 2025

³⁹ [Share of global GDP adjusted for PPP in the EU from 1980 to 2031](#), Statista, 2026

⁴⁰ [Share of the EU in world trade](#), EU, 2024

⁴¹ [The European Data Market study 2024-2026](#), EC, 2025

⁴² [2024 AdEx Benchmark Report](#), IAB Europe, 2025

⁴³ [Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers](#), EC, 2023

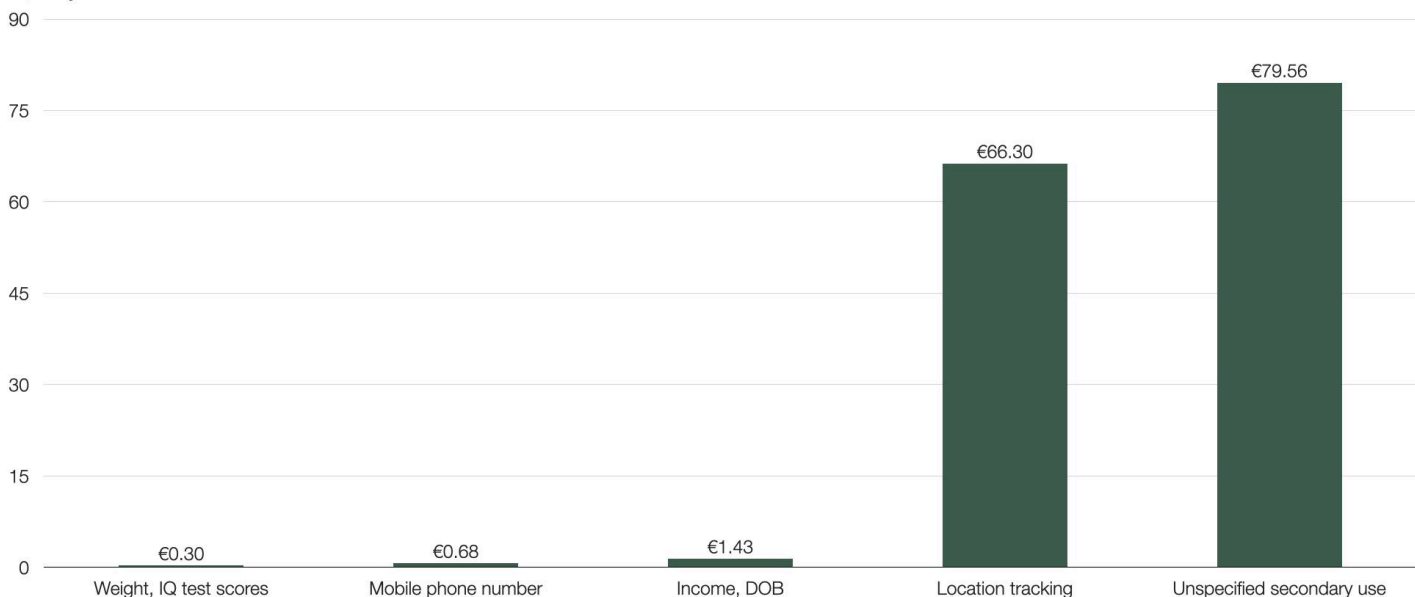
The secondary resale of personal data may cost over €100 per EU citizen every year

The market for personal data is opaque; we know little about the supply and demand, the prices, the buyers, or the sellers involved, making it difficult to find the prices at which consumer profiles are traded at.

When applying our upper and lower-bound estimates for the value of the secondary data market to the EU’s population of those 15 or older,⁴⁴ the value extracted per citizen is between €69 and €105 per year. Taking a median of these figures, the cost per EU citizen of the resale of data in the secondary market could be estimated at €87 per year.

A UK Government-commissioned report on the benefits arising from personal data rights under the GDPR utilises a collation of data on the values attributed to different types of personal data that have been estimated by previous academic research.⁴⁵ The research shows that certain data items are far more valuable than others, for example, individuals’ personal mobile phone numbers are only valued at approximately €0.50 (2012)⁴⁶, while location tracking data is valued more highly, at between €40.10 and €48 (2006) – see *Figure 3*.⁴⁷ The highest valued data item (€47.35 in 2002) falls under the category of “unspecified secondary data use”, which refers to the more general, unknown further use and sale of personal data in the secondary data market.

Figure 3
Estimated values of different personal data items
€, adjusted for inflation



Notes: All figures are estimates from academic and institutional research
Source: Assembly, UK Government

⁴⁴ [Population structure and ageing](#), Eurostat, 2026
⁴⁵ [Research and analysis to quantify the benefits arising from personal data rights under the GDPR](#), London Economics, 2017 and [The Value of Personal Information: Evidence from Empirical Economic Studies](#), Godel, Litchfield & Mantovani, 2012
⁴⁶ [Study on monetising privacy](#), ENISA, 2012
⁴⁷ [A study on the value of location privacy](#), Cvrcek, Kumpost, Matyas & Danezis, 2006

When adjusted for inflation and collated together into a de facto consumer profile, we estimate that this would be valued at approximately €148.27. As a cost per EU citizen of the resale of data, this figure seems quite high, but does reflect an example value of an individual consumer profile product that may be traded in the secondary data market. Taking an average of this figure alongside our upper and lower bound estimates based on the secondary data market's value, we could also estimate the cost per citizen at €107.57 each year.

€107.57

The annual cost per European citizen of the resale of their personal data in the secondary data market

Cost to consumers of lack of clarity and transparency over the value of the resale of their data

The lack of transparency and clarity over how personal data is traded and then used in the secondary data market leaves consumers with little to no understanding of the value of their data. In November 2025, France's data protection authority, the CNIL, published results from a survey it commissioned into public understandings around the monetisation of personal data.⁴⁸

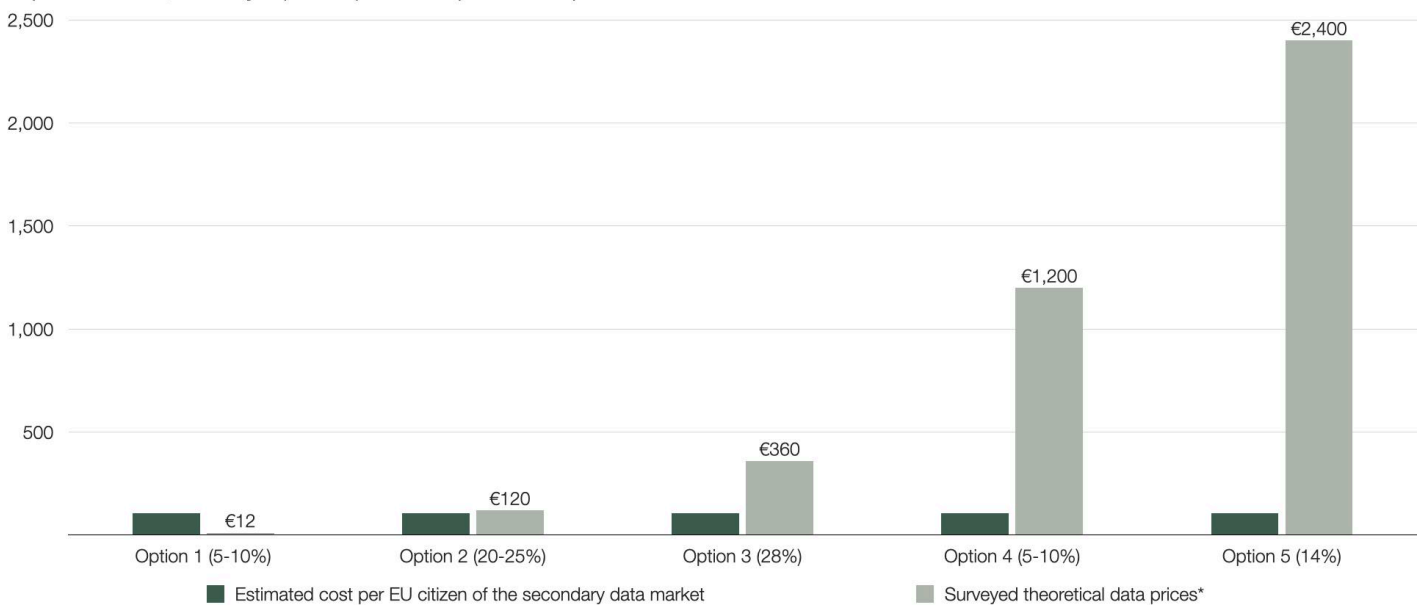
Based on its survey and other academic research on the demand for personal data from advertisers, the CNIL estimates an approximate market price for personal data of around €40 per month – this is perceived as the maximum price advertisers would be willing to pay for personal data per individual, equating to €480 per year. When comparing this annual theoretical market price per individual (€480) with our estimated annual cost per EU citizen of the resale of their data in the secondary market (€107.57), a clear discrepancy arises between how consumers value their data, and how much it is actually traded for (see *Figure 4*).

⁴⁸ [Monetisation of personal data: how much is our data worth?](#), CNIL, 2025

Figure 4

The data value gap

€ per annum, survey option (% of respondents)*



Notes: 1. Some instances are estimated ranges as full CNIL data is unavailable 2. Represents consumer expectations for the price of their data if they were to monetise it
Source: Assembly, CNIL survey

The value gap signals that consumers may not fully understand how their data is traded in the secondary market, and what it is then being used for. One reason for this may be that consumers perceive a higher value for their data due to the harms they consider the secondary data market is causing them that they are not compensated for. This signals that many consumers are aware that within the secondary data market, value is created without their oversight, understanding or influence, leading to a number of indirect consumer harms. In many cases, these harms are not just a redistribution of money within the market, but a systematic weakening of the consumer's position in digital markets.

Imperfect information and a lack of transparency about the onward use of consumer data once resold can cause a range of economic harms

In most cases, consumers are required to provide their personal data to use “free” digital services and platforms. While consumers are made aware of the data they are consenting to being used by the firms running these services and platforms, they are not made aware of their data’s future use and resale. For example, consumers do not know how many times their data is resold, to whom, for what purposes it is then used, or how much value it generates downstream as it is sold on. Brokers in the secondary data market do have this information though, and are more or less in control of it. This **information asymmetry** bars the consumer from negotiating better terms, choosing less invasive alternatives, or ultimately, deciding whether or not the “free” service is worth the hidden price of their data. With these consumer issues arising from this asymmetry, the information gap could be characterised as a market failure

due to data brokers' ability to exploit consumers by utilising and reselling their data without their full understanding.

Similarly, consumers experience a **loss of control through invisible onward use** of their data. For example, after consenting to their data being collected, it may be shared externally with an ad-tech partner and later used to target the consumer across unrelated apps and websites. Consumers cannot realistically track or reverse this spread of where their data ends up or meaningfully exercise their choices about its future use, therefore experiencing a permanent loss of agency over their digital footprint.

Economic value is created from individuals' data in secondary markets and further downstream when it is purchased and used in a variety of sectors such as ad-tech and credit scoring, but none of that value accrues to the consumers themselves. This represents **value extraction without consumer participation or compensation**. The current operation of the secondary data market results in a continued, systematic value capture by market intermediaries, with consumers structurally excluded from the monetary upside. While this does not cause any direct financial harm to consumers, it highlights the monetary value that could be available to them under a stronger regulatory framework for data protection.

Consumers usually compare services based on price and features, rather than on data extraction intensity, largely due to this being a relatively hidden and indirect cost, leading them to **distorted "free" service choices**. Two free digital services may appear equivalent to consumers, even though one service may rely more on the resale of data into the secondary market, subjecting their data to further, unclarified use. Without adequate transparency about these differences in digital services, but also about how resold data may be used, consumers are unable to factor them into their choices, pushing them towards more intensive data collection ecosystems by default. This distorts competition in the data market too, with these services able to extract more data, gaining an unfair advantage over their competitors with more privacy-respecting models.

Secondary data reuse can have further **downstream impacts consumers never agreed to**. Consumer data may be resold in the secondary data market to businesses which may use it in areas such as credit scoring and insurance pricing, potentially leading to higher prices or even an exclusion from certain offers for these consumers in other sectors. For example, if data on a consumer's shopping behaviour is resold and used for credit scoring, their position when looking to borrow money may be weakened at a future point. Even where data collection and secondary resale is lawful, these downstream use cases can still have negative economic and social consequences for consumers.

These consumer harms tend to stem from consumer's lack of understanding about how their data is used once resold, which is due to the obscurity of this

resale and further use in the secondary data market. According to Article 5(1)(a) of the GDPR, personal data should be processed in a “transparent” manner. While secondary data resale may often be lawful as consumers consent to their data being collected and processed when prompted with terms and conditions for each service or site they use, these do not explicitly detail how this data may be used once resold, leaving consumers without the transparency enshrined in the GDPR.

The costs to companies of failing to properly implement privacy safeguards

Estimating the costs to the European economy of privacy breaches

The introduction of the GDPR in 2018 strengthened the EU's existing privacy rulebook, elevating the level of data protection consumers can expect while imposing a host of new obligations on organisations as data controllers. While the regulation carries significant financial penalties for breaches of its provisions, there are costs too of ensuring ongoing and effective compliance.

The cost of compliance

The requirements of the regulation are manifold, covering a range of protections, including the appointment of a DPO, ensuring sufficient information security and reporting instances of data breaches without undue delay. Naturally, the implications of the adoption of the GDPR for organisations has been widely discussed. Companies have had to invest in compliance and data protection measures, which may have increased their cost base, including due to enhanced reporting duties, as well as investments in consent mechanisms and data minimisation processes – with the effects often especially pronounced for small and medium-sized enterprises (SMEs) and startups.⁴⁹ Given the extraterritoriality of the GDPR, its impact stretches beyond the EU, with firms in other jurisdictions required to comply with it where they handle the data of European citizens. One survey estimated that Global 500 companies would spend a combined **\$7.8bn (€6.7bn)** on GDPR compliance between 2017-2018, or **\$15.8m (€13.6m)** on average per firm.⁵⁰

The cost of non-compliance

While in no way trivial, the costs of ensuring – and then maintaining – compliance with the GDPR are likely to pale into insignificance when considered relative to the costs to companies of failing to implement the requisite measures to comply with privacy and data protection regulation – see *Table 4*.

⁴⁹ [GDPR's economic footprint: rising costs, falling investment, and shifting data quality](#), Amazon, 2025

⁵⁰ [Global 500 Faces GDPR Compliance Costs of \\$7.8 Billion](#), CPO Magazine, 2017

Table 4
Cost of non-compliance with the GDPR

Type	Cost	Details
Operational	Downtime	Annual cost of non-compliance is worth more than €45bn, with organisations in the EU directly shouldering almost €25bn of the impact
	Rectification	Patching and improving privacy practices and security processes, and/or implementing corrective measures represents a major opportunity cost
Economic	Share prices	Impacts on the value of publicly-traded companies varies by sector and size of breach, but is almost always negative – and in some cases long-lasting
	Loss of customers	Breaches damage consumer trust and confidence, with an estimated 60% of small businesses closing down within six months of an incident
Regulatory	Enforcement	Greater non-compliance with the GDPR increases complaints, data breaches and regulatory enforcement, increasing budgetary requirements of DPAs
	Litigation	Violations of the regulation can trigger lawsuits and compensation payouts, while unsuccessful legal challenges further raise the cost impact

Source: Assembly

Downtime

One operational cost of non-compliance with privacy regulation is the extensive downtime that organisations can experience as a result of a data breach or cybersecurity incident, having internal impacts on staff as they try to work through the breach and investigate the root cause, halting productivity, delaying projects and resulting in missed opportunities. They also have external impacts on the organisations’ customers and users of its service(s), as well as relevant regulatory bodies.

While research finds that the mean time to contain a data breach has fallen by nearly 10% since 2017, this period still lasted 60 days in 2025.⁵¹ Based on upper and lower bounds for the cost of downtime per minute, and assuming an average working day of eight hours, provides a cost per day range. Using the average number of fines per year since the GDPR came into force as a proxy for the number of organisations that have suffered a data breach in a given year, we are able to calculate a range for the cost of downtime per breach. Multiplying the average by the 60-day mean duration and rationalising by the likelihood of a business suffering operational downtime as a result of an incident, we therefore estimate that the annual cost of downtime caused by non-compliance could be worth more than **€45bn**. Organisations in the EU directly would shoulder the majority – almost **€25bn** – of the impact, a figure that outweighs the cost of ensuring upfront compliance.

⁵¹ [Cost of a Data Breach Report 2025](#), IBM, 2025

Rectification

Efforts and resources to resolve a data breach, cyberattacks or perceived misuse of data also expose companies to a considerable remedial cost – again, with around 55% of the financial impact of a breach absorbed by the affected organisation.⁵² Rectification costs therefore represent a major operational impact, involving work by management, legal and compliance teams to patch and improve privacy practices and security processes, and/or to implement (usually within a short timeframe) any corrective measures imposed by regulatory bodies in order to ensure that similar incidents do not reoccur in the future. The net effect is that a breach can set an organisation back dramatically, consuming resources that could otherwise be directed towards fuelling growth.

As cyberattacks have become more pervasive, many companies have sought to offset recovery costs after a security-related breach by obtaining cyber liability insurance coverage. However, the cost of coverage has risen considerably over time. The increasing frequency, scale and impact of cyberattacks has led insurance providers to raise concerns regarding high-risk profiles, leading to higher premiums, decreasing coverage and the exclusion of entire industries. Providers are analysing companies' cybersecurity readiness and closely tying coverage availability to implementing strong cybersecurity safeguards.

Share prices

A notable economic cost worth highlighting relates to the often measurable, sometimes sudden impact a publicised data breach can have on a company's value, as reflected in its share price. The effect of a data breach on the stock market is inherently unpredictable, varying across industries and by the scale and severity of the violation. Those that have a direct bearing on people's lives and wellbeing, or usually affect millions of individuals at a time may be the most financially consequential. Any stock price change is likely to be influenced by a multitude of factors, including the reactions of shareholders, fines levied against the company and the prospect of class action lawsuits.⁵³

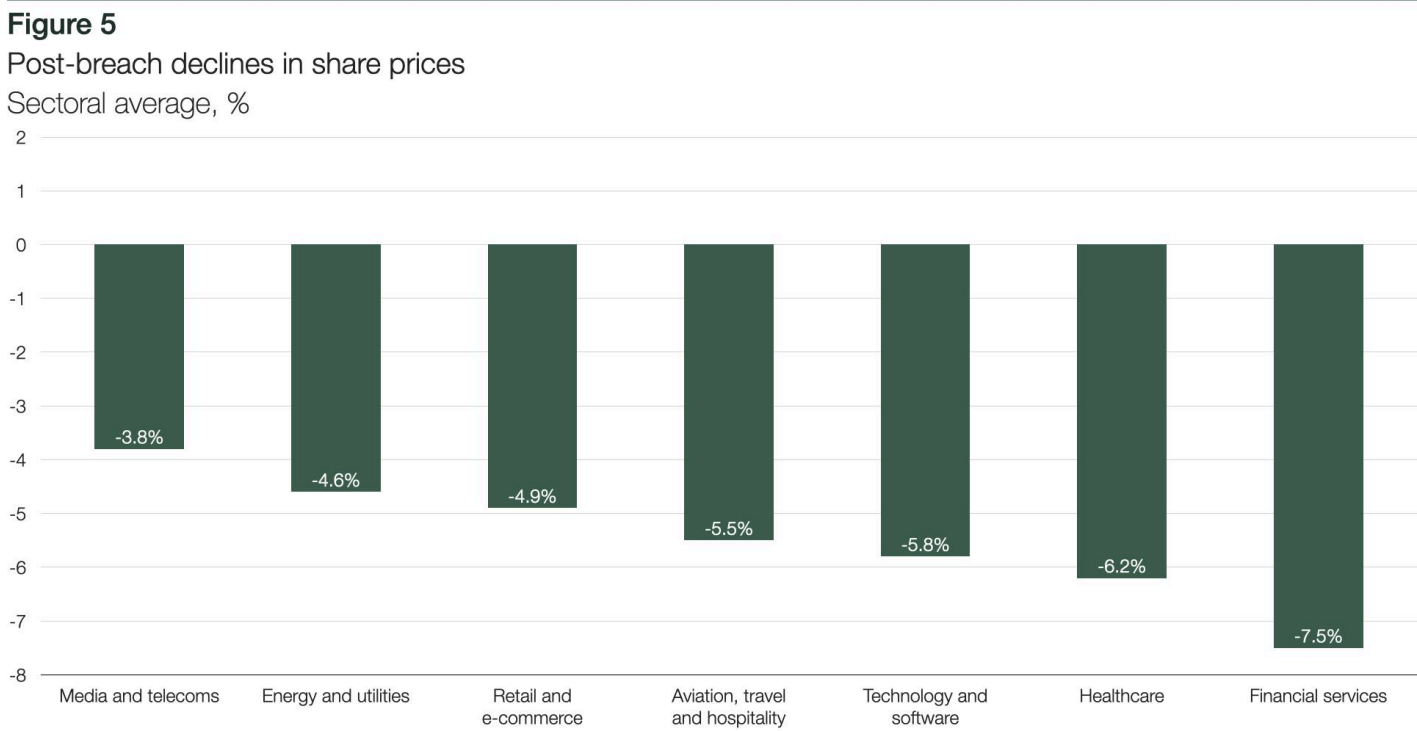
As such, research in this area provides for a mixture of findings. Studies have found that on the day after a cyberattack, stock returns decreased by 0.24%, but that the effect reverses after about two weeks have elapsed.⁵⁴ However, other studies have pointed to more statistically significant harm, stating that cybersecurity incidents resulted in an average share price decline of 5.3% within days of disclosure, with long-term underperformance against sectoral

⁵² Based on the share of organisations that did not report increasing the costs of their products or services following a data breach. See [Cost of a Data Breach Report 2025](#), IBM, 2025

⁵³ [The Impact of Data Breaches on Stock Performance](#), Islam, 2020

⁵⁴ [HACKED: Understanding the stock market response to cyberattacks](#), Akyilodrim, Conlon, Corbet & Hou, 2024

benchmarks reaching up to 15%.⁵⁵ The average decline varies across sectors, with financial services and healthcare the worst affected – see *Figure 5*.



Source: Assembly, Westbourne + Partners

Regardless of the level of impact, the causal relationship between data breaches and share prices is clear, reinforcing the importance of compliance. Research has also indicated that not only do companies’ stock prices fall immediately following a cyberattack, but that they continue to underperform one year on – see *Table 5*.⁵⁶

⁵⁵ [The Financial Impact of Cybersecurity on Stock Price and Corporate Valuation](#), Westbourne + Partners, 2025
⁵⁶ [The Hidden Costs to Business of Overlooking Data Privacy, Cybersecurity and ESG](#), Morningstar Sustainalytics, 2022

Table 5

Analysis of cyberattack portfolio companies against S&P 500 returns
Before and after cyberattack incidences

	Annualised returns	
	One year before incident	One year after incident
Incident portfolio (a)	7.82	-0.65
S&P 500 (b)	14.44	11.58
Sector benchmark portfolio (c)	11.73	10.15
Difference to S&P 500 = (a)-(b)	-6.62	-12.23
Difference to sector = (a)-(c)	-3.90	-10.80

Source: Assembly, Morningstar Sustainalytics

Loss of customers

Beyond the direct, immediate financial losses associated with operational downtime and rectification costs, another major economic impact relates to the implications of lost consumer confidence and trust, which can be difficult to regain, taking years in some instances. When a company suffers a data breach due to negligence, it can suggest to customers that their personal information is not sufficiently protected. The short-term impact is often customer attrition, with some consumers reluctant to continue doing business with a company following a major breach, which translates directly into lost revenue. In fact, it has been estimated that 60% of small businesses close their doors within six months of a data breach.⁵⁷

In addition, privacy or security incidents can damage a company's reputation, and repeated events erode the value of its brand and identity, impacting how customers trust it and who wants to do business with it moving forward. For example, cybercrime fosters a climate of mistrust toward the digital economy, discouraging online transactions, thereby amplifying its overall impact on both individuals and companies. According to a survey by the vzbv, 87% of consumers consider it very or somewhat important to be able to trust companies with the handling of their personal data before using their services.⁵⁸ Customers who do not leave a given organisation or service may hesitate to share data or do business as freely as before, limiting opportunities for growth,

⁵⁷ [The Effect of Data and Privacy Rights on Small Business](#), Fuller, Gauntlett, Oehlers, & Frankel, 2026

⁵⁸ [Digital Omnibus: European Commission puts consumer trust at risk](#), vzbv, 2026

while companies themselves must often invest heavily in customer notifications, credit monitoring for victims, and security improvements to try to repair their image. Even without a breach, the perception that a company has poor data protection practices could be damaging.

Enforcement

The enforcement and investigation activities of regulatory bodies also represents a significant cost for organisations and DPAs themselves, which is intrinsically linked to the degree of compliance with the GDPR. The entry into force of the regulation will have carried an inevitable investment burden; the EC, for example, has provided funding to national authorities to finance projects that support the implementation of the GDPR, including awareness-raising campaigns, training programmes and the development of practical tools and materials that can facilitate small and medium-sized enterprises' (SMEs) compliance with the GDPR.⁵⁹

As data has become increasingly pivotal to organisations and to economies more broadly, such levies as well as enforcement action and oversight functions will have increased organically over time. The EC's first evaluation report on the application of the GDPR noted, among other things, a significant rise in the amount of work for DPAs, due to increases in the number of complaints, notifications of data breaches, investigations and cross-border cases.⁶⁰ The GDPR directs Member States to provide DPAs with the necessary human, technical and financial resources, premises and infrastructure to carry out their duties effectively. However, these costs are directly related to the state of compliance with the regulation (particularly where cost recovery from fines imposed is capped at a certain level), with poor data practices requiring own-initiative investigations or interventions to respond to complaints. The EC's second report highlighted the trend in more robust enforcement activity by DPAs in recent years, such as the rising use of corrective measures and adoption of infringement decisions.⁶¹ This issue is compounded by the fact that while many DPA budgets have increased over time or in specific years, some have contracted,⁶² potentially putting the ability of supervisory authorities to fulfil their responsibilities at risk, with knock-on effects for the protection of citizens' privacy.⁶³

Litigation

The financial impacts do not end with regulatory interventions, with data breaches often triggering lawsuits and compensation payouts to affected customers – which can then be compounded by the effects of protracted legal

⁵⁹ [Data protection](#), EC

⁶⁰ [EU data protection rules empower citizens and are fit for the digital age](#) Commission report: EU data protection rules empower citizens and are fit for the digital age, EC, 2020

⁶¹ [Second report on the GDPR](#), EC, 2024

⁶² [Overview on resources made available by Member States to the Data Protection Supervisory Authorities](#), EDPB, 2022

⁶³ [Budget cuts incapacitate Austrian DPA: NGOs complaint to the EU Commission](#), EDRI, 2025

challenges, with companies such as Spotify appealing against fines imposed on them (unsuccessfully in this case⁶⁴) for GDPR violations. For example, in May 2018, two associations (None Of Your Business, 'NOYB', and La Quadrature Du Net) filed complaints to the CNIL against Google. The claims disputed Google's legal basis to process the personal data of the users of its services, in particular for the purpose of targeted advertising. The CNIL identified two problems: breach of transparency obligations, by not making essential information easily accessible; and failure to provide a legal basis for personalised advertising, which was not relying on "specific" and "unambiguous consent" – and as a result imposed a fine of €50m.⁶⁵

On 19 June 2020, France's Council of State rejected Google's appeal against the CNIL's decision, confirming that Google did not deliver sufficiently clear and transparent information to the users of the Android OS. The Council also agreed with the CNIL's conclusions about the lack of specific consent, because information related to targeting advertising was not presented in a sufficiently clear and distinct manner. In addition, consent was collected by means of a pre-ticked box, which does not meet the requirements of the GDPR.⁶⁶

While the settlement reached in July 2021 between BA and affected customers was not made public, it has been reported that the HSE Ireland will offer the approximately 620 people taking legal action against it €750 each. They will also be offered €650 towards their legal costs.⁶⁷ If correct, and confirmed, the figures would imply a total compensation of **€868,000** for victims of the cyberattack.

Case studies on the largest GDPR fines to date

In the digital age, personal data holds significant economic value, being used by businesses and organisations to gain new customers and make a profit. Large tech companies such as Amazon, Google and Meta can offer their services to users (typically for free) and benefit in return from the personal data of their customers. These companies have the world's largest databases of personal information, which they can share with others for marketing reasons, such as for advertising purposes and sending exclusive emails to customers to gain further engagement. One of the most immediate consequences of poor data protection practices is the risk of financial penalties. Under the GDPR, EU authorities can impose maximum fines of €20m or 4% of worldwide turnover, whichever figure is higher. We have therefore analysed the five largest GDPR fines,⁶⁸ including by:

- Outlining the penalties imposed for the breach, including agreed future investments;

⁶⁴ [Spotify AB must pay a penalty fee](#), Court of Appeal in Stockholm, 2025

⁶⁵ [French DPA issues €50m GDPR fine on Google](#), Assembly Research, 2019

⁶⁶ [Google loses appeal against GDPR fine in France](#), Assembly Research, 2020

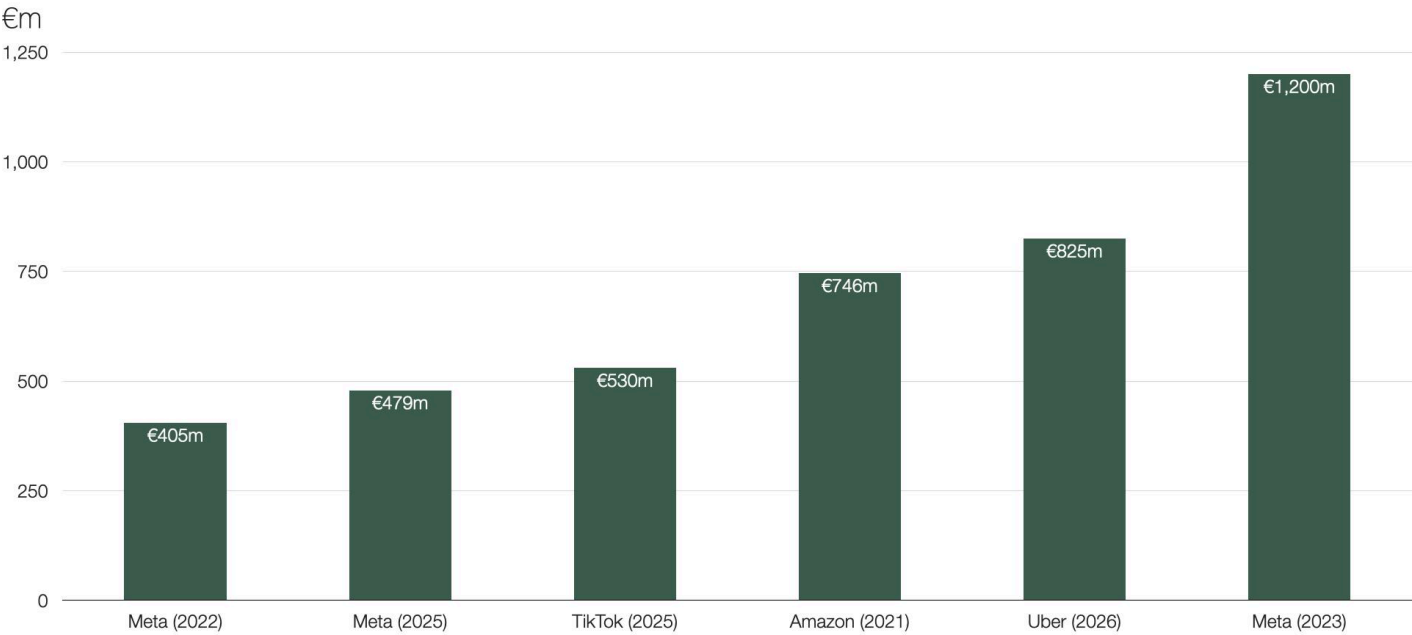
⁶⁷ [HSE begins offering €750 compensation to victims of cyberattack](#), RTE, 2025

⁶⁸ [Privacy and Data Protection Tracker](#), Assembly Research, 2026

- Outlining any compensation paid to victims; and
- Estimating the resourcing costs incurred by DPAs.

Of the largest six fines, three have been imposed on Meta, one on Amazon, one on TikTok and one on Uber (see *Figure 6*), although several further sanctions in the hundreds of millions of Euros have been handed out to tech firms since the regulation came into effect.

Figure 6
The six largest fines under the GDPR to date



Source: Assembly

∞ Meta €1.2bn (2023)

In May 2023, Ireland's Data Protection Commission (DPC) imposed a record fine for privacy violations, stating that Facebook's EU-US data flows had relied on standard contractual clauses (SCCs) that "did not address the risks to the fundamental rights and freedoms" of users.⁶⁹ The inquiry was initially commenced in August 2020, and was subsequently stayed by Order of the High Court of Ireland, pending the resolution of a series of legal proceedings, until 20 May 2021.

While other national DPAs agreed with the DPC's draft decision to make an order to suspend the data transfers, four disagreed with the proposal not to subject Meta to an administrative fine for the infringement that was found to have occurred, which the DPC did not consider would be "appropriate, proportionate and necessary". The objections were referred to the EDPB, which adopted its decision in April 2023. The DPC adopted its decision "on the basis of" this, imposing:

- An order requiring Meta to suspend any future transfer of personal data to the US within the period of five months;
- An administrative fine of €1.2bn; and
- An order requiring Meta to bring its processing operations into compliance with the GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EU/EEA users transferred in violation of the GDPR, within six months.

As an administrative penalty, no consumer compensation was mandated, although Meta launched an appeal against the decision, which remains ongoing, implying further work of the DPC and EU authorities to reach a final conclusion in this case.

Uber €825m (2026)

In August 2026, the Autoriteit Persoonsgegevens (AP), the Dutch DPA, confirmed it had fined Uber just under €825m for its use, between 2018-2022, of automated systems to deactivate driver accounts.⁷⁰ Although the AP has not yet (at the time of writing) formally published its decision, it appears that it has penalised Uber for non-compliance with Article 22 of the GDPR. According to

⁶⁹ [Data Protection Commission announces conclusion of inquiry into Meta Ireland](#), DPC, 2023

⁷⁰ [Uber fined nearly 825 million euros for automated driver blocking](#), AP, 2026

the AP, Uber violated the GDPR by subjecting its drivers to automated decision-making that had “major consequences” for them and did so without human intervention and the drivers’ knowledge. Uber has stated the fine is “disproportionate” and that the AP had examined “historic policies that were discontinued years ago”, adding that it will appeal the decision.

This fine represents the fourth imposed on Uber by the AP and follows a €290m penalty issued in August 2024 after the firm was found to have violated the GDPR’s rules against illegal personal data transfers outside of the European Economic Area (EEA).⁷¹

 **€746m**
(2021)

On 30 July 2021, Amazon reported that it received a €746m fine from the La Commission nationale pour la protection des données (CNPd), the Luxembourg DPA, earlier that month. It was initially disclosed in a US regulatory filing (rather than by the CNPD itself, who later confirmed the penalty⁷²), with Amazon stating that it believed the decision to be without merit and that it would defend it vigorously.⁷³ It is understood the decision follows a complaint filed in 2018 from the French civil rights group La Quadrature Du Net. The complaint led the CNPD to investigate Amazon’s targeted advertising practices, which were allegedly carried out without consent.⁷⁴ The then-record fine under the GDPR amounted to around 4% of Amazon’s annual net income for 2020 (\$21.3bn, or €18.3bn). Discussions between European DPAs and concerns raised with the EDPB reportedly contributed to the size of the fine, since the CNPD’s draft decision outlined a penalty of only half this amount.

Amazon appealed the decision, with a hearing taking place in January 2024; however, the legal challenge was dismissed by Luxembourg’s administrative court in a ruling of 18 March 2025. This meant that the fine imposed for GDPR infringements would stand, and that Amazon would need to comply with the corrective measures ordered by the CNPD.⁷⁵ In March 2026, the Luxembourg Court of Appeal overturned the decision, stating that while it agreed that Amazon had breached the GDPR (by relying on legitimate interests as a legal basis for collecting and processing personal data used for behavioural advertising), the CNPD should undertake a new analysis of whether the breaches were the consequence of intentional or negligent conduct – and therefore whether a fine should be imposed. In light of the legal challenge, no compensation has been paid to consumers affected by the violation of the GDPR, while the CNPD notes that its action has led to Amazon’s practices

⁷¹ [Dutch DPA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US](#), AP, 2024

⁷² [Decision regarding Amazon Europe Core S.à r.l.](#), CNPD, 2021

⁷³ [10-Q Quarterly Report \(30 July 2021\)](#), Amazon

⁷⁴ [Amazon fined €746m in largest GDPR fine to date](#), Assembly Research, 2021

⁷⁵ [CNPd decision regarding Amazon Europe Core S.À R.L.](#), CNPD, 2025

being brought into full compliance with the relevant provisions of the case regarding online behavioural advertising.⁷⁶



€530m
(2025)

In May 2025, Ireland's DPC concluded an inquiry into the lawfulness of TikTok's transfers of the personal data of EEA users to China.⁷⁷ The investigation determined that TikTok infringed the GDPR regarding its transfers of this data (despite the ongoing changes brought about by the company under "Project Clover") and its transparency requirements. Specifically, TikTok failed to verify, guarantee and demonstrate that the personal data of EEA users, remotely accessed by staff in China, was afforded a level of protection essentially equivalent to that guaranteed within the EU, thereby materially diverging from the bloc's data protection standards.

The DPC imposed administrative fines on TikTok totalling €530m (consisting of a fine of €45m for its infringement of transparency obligations and a fine of €485m for its breach of data protection requirements), as well as corrective measures that must be complied with within a six-month period. In addition, TikTok updated its privacy policy during the course of the inquiry, identifying the third countries to which EEA user data was transferred and informing EEA users that personal data was stored on servers in the US and Singapore, and was the subject of remote access by entities in TikTok's corporate group located in Brazil, China, Malaysia, Philippines, Singapore and the US. No user compensation was mandated as part of the decision (and no class action lawsuits have since been filed), although it included an order suspending TikTok's transfers to China if processing was not brought into compliance within the relevant timeframe.

In June 2026, the Irish High Court delivered its judgment on TikTok's appeal against the fine, considering that the corrective measures may have been affected by errors made by the DPC.⁷⁸ While the court upheld the infringement findings, it ordered the regulator to reconsider the sanctions that should be imposed. The DPC has stated that it would determine its next steps "in the coming period".⁷⁹

⁷⁶ [The CNPD has secured effective data-processing compliance by Amazon, has seen its key findings confirmed and pursues its work](#), CNPD, 2026

⁷⁷ [Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China](#), DPC, 2025

⁷⁸ [Verify, guarantee, demonstrate: The TikTok decision and what it means for international data transfers](#), Arthur Cox, 2026

⁷⁹ [Irish regulator reconsidering TikTok data-transfer ban after court ruling](#), Reuters, 2026

∞ Meta

€479m
(2025)

In November 2025, the Commercial Court No. 15 of Madrid issued a ruling partially upholding a claim brought by 87 Spanish digital media companies and news agencies (via the Association of Information Media, AMI) against Meta for an alleged breach of the Unfair Competition Act and the GDPR.⁸⁰ The court found that between May 2018 and July 2023, Meta had unlawfully processed the personal data of Facebook and Instagram users in Spain for behavioural advertising purposes, relying on invalid legal bases for processing personal data under the GDPR.

As a result, Meta had been able to gain a significant and disproportionate competitive advantage by advertising on its social media platforms over those online media outlets in the digital advertising market. As Meta did not submit its Spanish business accounts to the proceedings, the judge applied the rules of burden of proof and corroborated the data presented by the AMI, concluding that, during the five years of the alleged infringement, Meta earned close to €5.3bn in Spain from online advertising. With this figure considered to have been obtained in violation, the judge saw fit to order Meta to pay €479m in compensation to the affected firms.

∞ Meta

€405m
(2022)

In September 2022, following a two-year investigation, Ireland's Data Protection Commission (DPC) announced the conclusion of an inquiry into Meta concerning the processing of personal data relating to child users of the Instagram social networking service. The inquiry examined, in particular, the public disclosure of email addresses and/or phone numbers of children using the Instagram business account feature and a public-by-default setting for personal Instagram accounts of children.⁸¹

After six national regulators raised objections to the DPC's draft decision of December 2021, the case was referred to the EDPB, in line with the Article 65 dispute resolution process of the GDPR. On 28 July 2022, the EDPB adopted its binding decision, which rejected many of the objections but upheld those requiring the DPC to amend its draft decision to include a finding of

⁸⁰ [Meta, ordered to pay 479 million euros to the Spanish digital press for unfair competition by violating the European General Data Protection Regulation \(GDPR\)](#), ECIJA, 2025

⁸¹ [Data Protection Commission announces decision in Instagram Inquiry](#), DPC, 2022

infringement of Article 6(1) of the GDPR and to reassess its proposed administrative fines on the basis of this additional infringement.

Having taken account of the EDPB's binding decision, the DPC imposed a fine on Meta totalling €405m, including a fine of €20m for the specific infringement of Article 6(1). In addition to the administrative fine, the DPC also imposed a reprimand and an order requiring Meta to bring its processing into compliance by taking a range of specified remedial actions. No automatic compensation was mandated, although Meta mounted a legal challenge, therefore likely incurring costs for the DPC to defend its decision. Meta firstly lodged an appeal over a number of aspects of the decision, including how the fine was calculated, and then to seek a judicial review of the decision. The litigation remains ongoing, yet to reach a conclusion from the Irish court system.

The GDPR's largest fines have set important enforcement precedents

The collective redress imposed on the four firms across the six fines is substantial, reflecting the gravity of the infringements identified and the potential impact tech companies in particular can have in terms of the protection of consumer data, while setting precedents regarding the types of behaviours expected by the GDPR. They are also indicative of the diligence of DPAs, such as the DPC in particular, in upholding the regulation's principles and provisions, underlining that active enforcement (including costly financial sanctions) should not be considered a theoretical risk but a genuine prospect in instances of non-compliance. Although these penalties only account for a fraction of the total volume of fines issued under the GDPR to date, they compound the harm to consumers and the wider economy when organisations fail to comply with the regulation.

The potential economic benefits of higher standards of data protection

Estimating the benefits of strengthening privacy protections

Strong privacy and data protection rules already deliver significant benefits to consumers and the wider EU economy. By increasing trust in digital services, reducing the risk of misuse of personal data and providing individuals with greater visibility and control over how information about them is used, the GDPR helps support participation in the digital economy and creates incentives for more responsible data-driven innovation.

However, as emphasised by European consumer bodies,⁸² the experience of the GDPR's first years of application, together with developments in technology and in the business models of certain tech firms, indicates that there remain areas where the framework could be strengthened or clarified. Targeted improvements could further enhance consumer protection, increase legal certainty for organisations, encourage privacy-preserving innovation and unlock additional economic benefits.

The EC's Digital Omnibus package presented an opportunity to address some of these challenges. While aspects of the proposal seek to clarify the application of the GDPR and reduce unnecessary complexity, some of the proposed changes risk weakening existing protections rather than strengthening them.⁸³ Against this backdrop, the following section considers a number of areas where stronger data protection measures could deliver additional benefits for consumers, businesses and the economy.

Implementing a more consumer-centric consent framework could benefit consumers and businesses

A central objective of the Digital Omnibus proposal is to strengthen meaningful consumer choice and control in the digital environment. The introduction of automated, machine-readable privacy signals (under proposed Article 88b) intends to address challenges such as “consent fatigue” and intrusive cookie banners. By enabling users to express their preferences once, in a standardised and reusable format, these mechanisms aim to reduce friction in the user experience while ensuring that preferences are more consistently respected. This is aligned with improved privacy outcomes – where user choices are easier to exercise and less burdensome, they are more likely to

⁸² [Five years of GDPR: Endless "checkboxes" but poor privacy protection](#), Sveriges Konsumenter, 2023

⁸³ [Open Letter: Reopening the GDPR is a threat to rights, accountability, and the future of EU digital policy](#), EDRI, 2025

reflect genuine intentions rather than fatigue-driven acceptance.

However, this approach sits alongside an ongoing shift in data collection. The current reliance on third-party cookies and browser-mediated tracking is shifting towards models based on first-party data, server-to-server exchanges and application programming interfaces (APIs). These approaches usually operate outside the visibility or control of the browser. As a result, the point at which user data is processed – and decisions about its use are made – is increasingly removed from the interface through which the user expresses their preferences.

The Omnibus proposal is narrowly focused on the consumer interaction layer, and assumes that the service receiving their signal is the primary decision-maker for their data. However, data processing often involves multiple actors and stages, including onward sharing and further processing. The absence of an explicit requirement to enforce machine-readable privacy signals across these downstream processing chains risks limiting their effectiveness. Without these stricter requirements, there is a possibility that user preferences are honoured at the point of collection but not consistently applied to later uses of the data.

Addressing this gap could benefit consumers and businesses. For consumers, ensuring that machine-readable signals are respected throughout the full lifecycle of data processing would enhance trust and deliver more reliable and meaningful control, reducing the risk of discrepancies between expressed preferences and actual data use. Consumers would benefit from greater control, convenience and confidence when interacting online, with less need to overshare personal data just to access and use everyday online services. This increased control and ease-of-use would enhance consumer trust in the digital services they use.

For businesses, clearer end-to-end rules could support regulatory certainty and reduce fragmentation, especially in complex data ecosystems involving multiple businesses. Standardised approaches to the transmission and enforcement of privacy signals could streamline compliance processes, lower transaction costs and encourage the development of interoperable solutions across the market. Extending the Omnibus proposal to address downstream data processing more explicitly has the potential to strengthen consumer protection and to support more efficient and sustainable business models.

Stronger certainty around pseudonymisation and re-identification risk are required to combat one of the most common GDPR breaches

A lack of regulatory certainty around pseudonymisation and re-identification risk can lead to a range of protection levels for consumers, rather than ensuring strong protections for all. The EC's Digital Omnibus proposal to 'specify means

and criteria' for companies to assess this re-identification risk should be seen as an opportunity to strengthen protections for consumers with new guidance and regulatory certainty.⁸⁴ It is important to note that this should not be interpreted as a need to redraft the GDPR's current definition of personal data, which the Omnibus also proposes. A new definition would create legal uncertainty and unclarity as the GDPR's scope would be brought into question. This scope would need to be reassessed, discarding many years of CJEU work on interpreting the current definition. Instead, the EDPB should look to continually set clear guidance on pseudonymisation and re-identification risks, developing these guidelines over time as anonymisation techniques evolve, as it has done with its July 2026 publication of new guidelines on anonymisation.⁸⁵ With clearer regulatory guidelines on these issues, consumers would gain stronger protection against covert re-identification and the misuse of their data.

With this added clarity, there would be a lower risk of unlawful data processing and therefore a lower risk of GDPR fines, particularly in relation to organisations falling foul of Articles 25 and 32 of the GDPR for having insufficient technical measures to ensure information security, which have been at least partially responsible for over 500 GDPR fines, averaging a cost of approximately **€1.7m** since its application.⁸⁶ Both of these GDPR Articles cite the use of pseudonymisation as a potential measure for ensuring this information security. Pseudonymisation should not be treated as excluding a controller's processing from the scope of the GDPR, but should be considered as a design and risk-reduction measure under Article 25. While clearer guidance on pseudonymisation and re-identification risk would not eradicate all future GDPR fines under these Articles, it could reduce them by ensuring greater certainty for businesses, making them more aware of how they can use these measures to limit the re-identification risk and better protect consumers. This added certainty could benefit the economy more widely too. For example, it may encourage further investment into data analytics and sharing systems that are more privacy-preserving, supporting innovation across a variety of sectors without undermining consumer trust in their digital services.

Greater transparency is necessary for algorithmic feeds to limit the harmful effects of the attention economy

Social media feeds have become bloated with algorithmically recommended and AI-generated content, and addictive "infinite scroll" features together producing harmful consequences (e.g. harmful content, societal division and hatred, mental health issues, undermined democratic processes etc). While not exclusively a data protection issue, such activity depends on the use of consumer profiles derived from the collection of personal data. The EC should require greater transparency regarding algorithmic feeds and set boundaries for

⁸⁴ [Digital Omnibus Regulation Proposal](#), EC, 2026

⁸⁵ [Guidelines 02/2026 on Anonymisation](#), EDPB, 2026

⁸⁶ [GDPR Enforcement Tracker Report 2026](#), CMS Law, 2026

what can be considered fair processing in this area, taking into account the harmful effects of the attention economy.

Stronger transparency requirements, increased oversight and limits on profiling would limit how targeted much of the content and advertising on algorithmic feeds is, and would provide consumers and regulators with a better understanding of how these feeds work. Limiting the algorithmic use of personal data, particularly where it drives content recommendation, engagement optimisation or behavioural influence would also be beneficial. Reduced targeting would better protect consumers from some of the most addictive and harmful effects of algorithmic feeds, especially those using an “infinite scroll” mechanism. It could reduce consumers’ exposure to dangerous content (e.g. self-harm or eating disorder content), and polarising or manipulative content. European citizens would benefit from healthier digital environments and reduced social harm while businesses benefit from clearer boundaries for acceptable design choices.

Increased algorithm transparency could benefit the economy by strengthening competition. Some of the most dominant online platforms rely heavily on their algorithmic feeds to retain consumer attention through targeted content and advertising, but the details of these algorithms are often opaque and have been criticised for self-preferencing, especially in search and news ranking feeds. These algorithmic decisions can have significant financial consequences on other businesses that rely on these feeds for their content or services to be promoted.⁸⁷ Some businesses have also reported that they think some algorithm changes may be commercially motivated to favour the platforms or affiliated parties at the expense of other businesses. Stricter transparency requirements would ensure impacted businesses are given a better understanding of these algorithms, and may unearth potentially anti-competitive behaviour, which could then be acted upon by regulators.

This added transparency would ensure a stronger and clearer safeguard for consumers to access information that more meaningfully explains such automated and algorithmic decision-making. Article 22 of the GDPR requires that consumers must not “be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her” without their consent.⁸⁸ Consumers do not currently have access to meaningful and actionable explanations in practice of how they may be subject to such automated decision-making. So, stronger transparency measures would ensure consumers can better understand these algorithms, enabling them to make more informed choices about their consent.

⁸⁷ [Algorithms: How they can reduce competition and harm consumers](#), CMA, 2021

⁸⁸ [Regulation \(EU\) 2016/679 of the European Parliament and of the Council](#)

The EC should look to strengthen the GDPR's accountability mechanisms

The GDPR is based on principles and accountability mechanisms that place the burden of identifying and mitigating risk on businesses who must not only comply with data protection rules, but also be able to demonstrate how they comply. The scope of data protection principles, including the principle of accountability, are broad, applying to personal data across the economy without being linked to specific technologies or business models. One possible means to strengthen data protection throughout the economy could be to increase regulatory oversight of the GDPR's accountability mechanisms, for example in how businesses conduct data protection impact assessments or legitimate interests assessments. This would provide assurance to the consumer that effective safeguards are being implemented and the accountability principle is being adhered to by businesses not only complying but being able to demonstrate that compliance. This added oversight and expectation of stronger enforcement of the accountability mechanisms should come in the form of regulators actively checking the quality and effectiveness of those accountability measures. These clearer benchmarks for compliance with the rules could support businesses in identifying and mitigating current practices or external threats that may put consumers' personal data at risk. These measures would improve businesses' risk management procedures, reducing the likelihood of major failures that lead to costly data breaches, large enforcement fines and reputational damage. Over time, this could lower the systemic cost of non-compliance and create a more level playing field for responsible businesses.

Important notice

By accepting this research, the recipient agrees to be bound by the following terms of use. This research has been prepared by Assembly Research Limited and published solely for guidance and general informational purposes. It may contain the personal opinions of analysts based on research undertaken. Assembly Research Limited gives no undertaking to provide the recipient with access to any additional information or to update or keep current any information or opinions contained herein. The information and any opinions contained herein are based on sources believed to be reliable but the information relied on has not been independently verified. Assembly Research Limited, its officers, employees and agents make no warranties or representations, express or implied, as to the accuracy or completeness of information and opinions contained herein and exclude all liability to the fullest extent permitted by law for any direct or indirect loss or damage or any other costs or expenses of any kind which may arise directly or indirectly out of the use of this research, including but not limited to anything caused by any viruses or any failures in computer transmission. The recipient hereby indemnifies Assembly Research Limited, its officers, employees and agents and any entity which directly or indirectly controls, is controlled by, or is under direct or indirect common control with Assembly Research Limited from time to time, against any direct or indirect loss or damage or any other costs or expenses of any kind which they may incur directly or indirectly as a result of the recipient's use of this research.

© 2026 Assembly Research Limited. All rights reserved. No part of this research may be reproduced or distributed in any manner including, but not limited to, via the internet, without the prior permission of Assembly Research Limited. If you have not received this research directly from Assembly Research Limited, your receipt is unauthorised.

Assembly

36 Spital Square
London
E1 6DY
United Kingdom

+44 20 3026 2700
info@assemblyresearch.co.uk