

PRIVACY THAT POWERS THE EUROPEAN DATA ECONOMY

The results from Assembly Research's study into the economic costs of weakening privacy and data protection highlight the often-overlooked economic benefits of privacy: strongly enforcing the GDPR and protecting consumers' rights is an economic asset for companies, not a burden.

Consumers are giving away value they cannot see

Most consumers are unaware that Big Tech resells their personal data in the secondary data market. Signing up for "free" services and the lack of transparency around the secondary data market mean consumers are left in the dark about how much their data is really worth.

Data brokers monetise consumers' personal data as part of a market worth €40.5bn per year. Consumers see none of this value.

Companies derive enormous value from the resale of data, but consumers have no control over what happens to it, nor to whom or where it goes.



€107.57

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



€40.5bn

The estimated value of the secondary data market

European businesses cost €1.9bn per year to consumers by overlooking privacy and data protection measures

€1.9bn

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



European businesses cost €1.9bn per year to consumers by overlooking privacy and data protection measures that should ensure protection against data breaches or empower consumers' with basic rights of access, erasure and data portability.

This cost is the value attributed to our privacy rights and comes as a cost to companies violating data subject rights under the GDPR.

€406m

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



European businesses lose about €406m per year to data breaches and phishing attacks due to the lack of involvement or appointment of a Data Protection Officer to make compliance easier and ensure their data remains protected.

Insufficient training for employees and a lack of compliance monitoring means companies risk unnecessary exposure of their data to rogue actors, risking data breaches and falling victim to scams.

Consumer confidence is essential for a competitive economy

Organisations lose around €25bn per year when services are taken offline. This includes the immediate loss of revenue due to downtime, but also considers the loss of productivity or losing consumers who may switch to a competitor.

It can take an average of two months to rectify a data breach, which means time and money lost for companies.

Whilst compliance may be challenging, the impact of data breaches is swift and devastating. It has been estimated that **60% of small businesses close their doors within six months of a data breach.**

Data shows that 87 % of consumers consider it important to be able to trust a company with handling their personal data before using their services.



€25bn

Organisations lose around €25bn per year when services are taken offline



60%

of small businesses close their doors within six months of a data breach

HOW TO PROTECT OUR DATA PROTECTION RIGHTS AND DELIVER A COMPETITIVE ECONOMY?

For a truly competitive European economy that properly leverages privacy and data protection as a competitive advantage, BEUC recommends the following.

TOPICS

BEUC RECOMMENDATIONS

KEEP PERSONAL DATA PROCESSING BASED ON USERS' CONSENT - NOT LEGITIMATE INTEREST

- To stop 'cookie fatigue', companies should not be allowed to simply process more and more data without users' consent. Rather, we need to simplify how consumers can meaningfully exercise their choices on how and which data is shared. Ending complicated cookie banners and instead implementing mandatory **browser-based consent gives a simple way for consumers to choose and for companies to respect that choice.**
- EU policymakers should also not allow legitimate interest as a basis to **use personal data for AI training.**
- When consumers feel that companies are collecting their personal data for free and reusing them in ways they did not anticipate or consent to, confidence in digital services diminishes, leading to greater reluctance to engage, share information, or adopt new technologies.

STRENGTHEN CONSUMERS' RIGHTS TO ACCESS, CORRECT, TRANSFER, AND ERASE THEIR PERSONAL DATA

EU policymakers should reject the Digital Omnibus' proposal to limit the ability for consumers to exercise their right of access. Limiting consumers' rights would only further reduce their trust in how companies handle their personal data and in turn lead to fewer consumers feeling safe to use their services and participate in the digital economy.

IMPROVE ENFORCEMENT OF COMPANIES' OBLIGATIONS TO PROPERLY SECURE AND MONITOR PERSONAL DATA

The EU should empower **regulators** to investigate and remedy data breaches more effectively by giving them more resources, creating an effective **single-entry point to report data breaches** and enable consumers to **better understand their rights.** If consumers better understand their rights, and they feel their rights are properly respected and enforced, consumers can make more informed choices about their consent and actively and safely participate in the digital economy.