Privacy Next's Response to the EU Consultation on the Digital Fitness Check

Key Points:

- **Fragmentation and Resource Constraints**: Diverging national interpretations of GDPR have led to fragmentation across the Single Market, creating challenges for businesses, especially SMEs, and resource constraints for national supervisory authorities, which hinder enforcement and compliance.
- **Complexity of GDPR**: The excessively broad definition of personal data under GDPR has contributed to legal uncertainty and imposed high compliance burdens on companies, particularly SMEs, making the system overly complex and detrimental to innovation and economic activity.
- **Impact of Data Subject Access Requests (DSARs)**: The unfettered rights of individuals to submit DSARs, as provided for in GDPR, have created a significant burden for business, especially SMEs, by requiring extensive resources to respond to potentially frivolous or abusive requests, which may not necessarily enhance data protection.
- **Need for Streamlining GDPR Compliance**: The current implementation of GDPR unnecessarily hinders the EU's digital rulebook and competitiveness. There is a need for streamlining compliance processes to reduce regulatory burdens, address systemic challenges, and better calibrate the fundamental right to data protection with economic growth and innovation.

Summary

The EU's Digital Fitness Check is the second stage of the European Commission's digital simplification agenda, following the targeted regulatory adjustments proposed under the Digital Omnibus. The fitness check was designed as a broad, evidence-gathering exercise to assess whether the EU's digital rulebook remains effective, proportionate and fit for the future. The call for evidence and consultation sought the views of stakeholders to examine the cumulative impact of the EU's digital rules businesses, people, and public authorities, The process had a deliberately tactical focus, inviting stakeholders to share

practical experiences with overlaps, inconsistencies and synergies between the rules, and to provide evidence on regulatory burdens and real-world effects. It is hoped that the consultative process will provide an evidence-based assessment of the EU's digital rules to determine how well they support EU competitiveness while safeguarding values and fundamental rights.

The text below contains the primary arguments made in Privacy Next's response to the consultation.

Introduction

Privacy Next welcomes the opportunity to provide information on how the current EU digital rulebook is affecting businesses' competitiveness in the EU and the effective functioning of the Single Market. We wish to focus our response on matters related to the understanding and application of the General Data Protection Regulation (GDPR), which, in turn, has resulted in significant administrative burdens for companies, public bodies, and the supervisory authorities overseeing the Regulation. These burdens have reached a critical level, in which the integrity of the entire digital rulebook is weakened by misinterpretations of data protection in our society.

We recognise that GDPR and the EU's digital rulebook can be viewed as setting a high standard for regulation when compared to other jurisdictions. However, both the Draghi and Letta reports make clear that the EU needs to focus on how its regulatory systems and approaches impact the core activities of the Single Market. When examined from this perspective, the gold standard claimed by the Commission does not appear as valuable as the practical reality being faced by many organisations across the Single Market.

Impact and Consequences of GDPR

Our assessment of the negative impact of the GDPR on economic activity and regulatory institutions is based on a variety of reports produced by the EU.

The Second Report on the application of the General Data Protection Regulation (European Commission, COM(2024) 357 final) identified a number of matters concerning the application of GDPR having a negative impact across the system. These include –

- Diverging national interpretations of GDPR are leading to fragmentation across the Single Market.
- Economic actors, especially SMEs, are facing challenges in terms of resources and expertise to ensure compliance.
- National supervisory authorities facing resource constraints affecting the ability to enforce and support compliance.

A range of other negative impacts was also identified, including consequences for international cooperation, limiting the EU's ability to lead on practical multilateralism cooperation.

A 2024 study by the EU Fundamental Rights Agency emphasises that the demands of the GDPR have overwhelmed the ability of national supervisory authorities to fulfil their enforcement and compliance responsibilities. The study presents the burdens arising from the ongoing rise in complaints, data breach notifications, investigations, and cross-border cases since the adoption of GDPR, which has significantly increased the workload for supervisory authorities. This problem is most acute in relation to how the GDPR system has prioritised managing individual complaints at the expense of authorities' ability to engage in public awareness activities or provide advice to organisations. The overall impact of GDPR on supervisory authorities creates delays and gaps in ensuring compliance, which, over time, further weaken the data protection system.

A 2026 report commissioned by the European Parliamentary Research Service, at the request of the European Parliament's Committee on the Internal Market and Consumer Protection (IMCO), examines legislative overlap in the EU digital framework (Doc. PE 772.641). The report identifies problems arising from GDPR's definition of personal data, which is viewed as overly broad, contributing to legal uncertainty and imposing high burdens upon company activity.

The common theme in these studies and other reports on the impact of GDPR is that a "general" approach to data protection has created a system that is too complex. This complexity places a heavy burden on SMEs to focus their economic activity on core business practices in order to achieve economic success. Of course, compliance is a core business practice, but compliance with a system that creates untenable demands cannot become the primary objective of business activity.

The EU has identified innovation and competitiveness as essential for the ongoing growth of the Single Market and for supporting the EU's strength as a global trade bloc. Data protection is not an obstacle to achieving success in these areas, but the current system, as interpreted and understood under the GDPR, creates obstacles to innovation while not improving the data protection system.

Example – Excessive Rights Claims Damaging the System

A significant example of these challenges created by GDPR is the area of data subject access requests (DSAR). Article 8 of the Charter of Fundamental Rights and GDPR both provide for a right of individuals to access their data. Over time, individuals have increasingly leveraged this right, as any individual can contact any organisation to find out if their data has been processed. The evidence from the above reports does not show that the data protection system benefits from unfettered rights of this nature. The burden upon businesses, especially SMEs, is self-evident. But as the unfettered access rights also include an unquestioned right to complain to supervisory authorities, it is unclear that they system is able to effectively the data protection rights of all.

The current Brillen Rottler case before the CJEU (C-526/24) illustrates the challenges DSARs pose to the data protection system. In this case, an individual residing in one EU Member State submitted a DSAR to a company in another Member State after willingly sharing their personal data with that company. In this situation, there is, at best, a tenuous link between the individual and the company to which the personal data are willingly provided. Notably, the individual has a documented history of making similar requests and subsequently seeking compensation when the individual deems the responses unsatisfactory. The Advocate-General's opinion suggests that limitations on DSARs

should be minimal, placing a high burden on data controllers to prove that a request is abusive or excessive. While acknowledging that some DSARs may be vexatious, the Advocate-General indicates that merely submitting multiple requests is insufficient to demonstrate abuse without explaining why an individual should be able to disrupt the activities of economic actors without a substantial rights claim. This creates an unworkable framework for businesses, especially SMEs, as they must respond to potentially frivolous requests without more stringent process requirements regarding the reasons for a DSAR. With DSARs not requiring justification, unscrupulous individuals may exploit this right, knowing that data controllers' refusals pose risks of infringement and liability.

The question being raised by this example is not the right of individuals to access their data (as protected by Article 8(2) of the Charter of Fundamental Rights). Rather, the question is about how the right has come to be exercised following GDPR, which has expanded the content and institutional reach of the right to almost unreasonable parameters. The expansion is clear in article 15(1) GDPR, whereby any individual in the EU can contact any organisation to ask whether their data is being processed. From this, the GDPR empowers individuals to request extensive information about their data and how it has been processed. Furthermore, article 12 GDPR sets out a range of obligations on data controllers when responding to DSARs, requiring a one-month response, which again requires a company to allocate significant resources to a part of the business that may have very little to do with the core economic activities.

This example shows how the understanding of the GDPR hinders the EU's digital rulebook. The current implementation has imposed significant burdens that hinder the competitiveness of businesses, particularly SMEs, across the Single Market and does not necessarily enhance data protection across the system. The fragmentation resulting from diverging national interpretations, resource constraints on supervisory authorities, and the overwhelming demands of individual rights have created a complex regulatory environment that detracts from innovation and economic activity. To maintain the integrity of the digital framework and support the EU's position as a global trade leader, it

is essential to streamline GDPR compliance and address the systemic challenges that jeopardise both data protection and economic growth.

Submitted 11 March 2026