



Warsaw, 9.07.2025

Chamber of Digital Economy's comment on the European Commission's draft proposal for GDPR deregulation

The current shape of data protection regulations in the European Union ("EU") was ultimately formed with the entry into force of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR") – it has now been 7 years since the EU set the tone for personal data protection, providing a global example of how to thoughtfully build a system that safeguards personal data. This has proven to be extremely important over the years of the GDPR's application – especially now, at a pivotal moment in history, as AI-based solutions are becoming widespread. These technologies require gigantic amounts of information (including personal data) for their development and proper functioning.

However, the current data protection environment is far from perfect – there are increasingly frequent discussions to reduce the scope of obligations, particularly for businesses operating on a limited scale (small and medium sized enterprises or SMEs). Their contribution to the EU economy is invaluable, and overburdening small entrepreneurs with an inappropriate number of obligations negatively affects their ability to continue operating in an increasingly complex regulatory landscape.

Such views have led to taking initial steps by the European Commission ("EC") aimed at deregulating the EU data protection framework. The EC has adopted the "Omnibus IV" legislative package, which aims to simplify EU regulations and reduce administrative burdens for SMEs. The package includes a proposal to limit the obligation to maintain records of processing activities under Article 30(1) of the GDPR.

As an entity actively engaged in legislative processes related to the digital economy and e-commerce, Chamber of Digital Economy hereby presents its position regarding the deregulation changes proposed by the EC in the area of personal data protection.

HIGH RISK – INTERPRETATION UNCERTAINTY

According to the proposal adopted by the European Commission, businesses and organizations with fewer than 750 employees would be exempt from the obligation to maintain a record of processing activities, provided it is unlikely that their personal data processing poses a "high risk" to the rights and freedoms of data subjects.

So far, the EC has not clarified how the term "high risk" used in the deregulatory package should be interpreted, nor how to determine whether such high risk actually exists.

Under the proposed solution, the ability to benefit from the exemption would require data controllers to conduct appropriate risk assessment in order to identify data processing

Chamber of Digital Economy

T + 48 506 577 824 E BIURO@EIZBA.PL | WWW.E-IZBA.PL

A ŁUCKA 18 LOK. 76, 00-845 WARSAW NIP 701-039—19-22 KRS 0000474028



activities that involve high risk. No guidelines or clarifications have been issued to support the interpretation of the proposal or to enable controllers to reliably determine the presence of high risk in the context of the obligation to maintain a record of processing activities.

In this context, it is worth mentioning that the provisions of the GDPR generally leave a wide scope of interpretive discretion to data controllers. This stems from the risk-based approach that controllers are expected to apply at every stage of personal data processing, as well as the so-called technological neutrality of GDPR provisions.

However, in this particular case, the deregulatory measure – intended primarily to benefit SMEs – may present challenges for small businesses due to the need for detailed verification of whether their data processing activities involve high risk. Any incorrect determination in this regard could potentially have far-reaching negative consequences.

The mere necessity of carrying out such verification may itself be problematic and could even require more effort than creating the record of processing activities, which actually helps organize a controller's data processing operations and serves as a key document forming the foundation of data controllers' documentation and personal data protection systems. In the absence of a clear position on how to interpret the concept of high risk or how to assess its existence, the new solution proposed by the European Commission may bring more uncertainty than benefits.

IS GDPR DEREGULATION MISGUIDED?

Furthermore, concerns arise regarding the subject of the deregulation proposal that the European Commission has focused on – namely, the record of processing activities.

Within the current regulatory landscape of the GDPR, maintaining a record of processing activities is considered as a fundamental obligation that applies to all entities involved in the personal data processing chain (in the case of processors, this obligation takes the form of maintaining a record of categories of processing activities). This stems from the nature of the document, which functions as a kind of inventory that outlines the status quo of personal data processing within a given organization. The record of processing activities is the document in which an organization, acting as a data controller, provides information on how it processes personal data – this makes it possible to determine, in particular, what personal data is processed and in what manner.

In the context of the proposed GDPR deregulation, the obligation to prepare and maintain such a record should not be regarded as burdensome. From the perspective of a small business, it is a relatively simple obligation to fulfill, and one that brings many benefits – especially in terms of mapping personal data processing activities (including determining the scope and methods of processing) as well as managing and organizing these processes.

Moreover, with relatively little effort, the record also enables the identification of non-compliance with GDPR requirements. Without knowing what data is being processed, for what



purpose, on whose behalf, and concerning which individuals, it is not possible to conduct a meaningful risk analysis – one of the core obligations under data protection law.

For the reasons outlined above, the European Commission should carefully reconsider the chosen scope of the proposed GDPR deregulation, which currently focuses on a single document that, in essence, appears to bring more benefits than burdens to data controllers.

INADEQUATE DEREGULATION CRITERIA

Furthermore, the size-based criterion adopted by the European Commission to determine the scope of exemption from GDPR obligations does not appear to be adequate.

The proposed threshold of employing up to 750 people, given current realities and the rapidly evolving digital economy of the European Union, carries the risk of exempting entities from data protection obligations that, in fact, should be subject to them. This would particularly apply to smaller entities (such as start-ups) that process personal data on a large scale (e.g. creating or using AI systems) or process personal data of a specific nature (e.g. special categories of data), which may pose a high risk to the rights or freedoms of individuals.

Perhaps the scope of obligations imposed on data controllers should instead depend on the scale of personal data processing and the nature of their activities – these factors seem to be more indicative of the potential impact and risks associated with personal data processing.

FRIENDLIER ENVIRONMENT FOR DATA CONTROLLERS

A solution that could provide genuine benefits to data controllers – while also reducing the burden of existing legal obligations – would be the creation of publicly accessible tools that enable the generation of documentation required under the GDPR.

Such tools could potentially allow for the automatic creation of templates for documents such as records of processing activities, risk assessments, data protection/transfer impact assessments or legitimate interest assessments. Of course, in order for these tools to offer real value, they should include relevant explanations and guidelines to help data controllers generate compliant and meaningful documentation that meets the requirements of current data protection laws.

A useful example of such a solution is the software made available by the European Data Protection Board, which can assess websites for compliance with applicable laws (e.g., with regard to cookie files usage). Providing such tools could gradually lead to the standardization of personal data processing practices (at least to a limited extent) for certain data controllers that the EC aims to relieve of some legal obligations. Establishing such a standard could also bring significant benefits within the specific data protection landscape of the EU, which is governed by harmonized regulation. A common challenge for many data controllers is the varying practices of supervisory authorities, which interpret GDPR provisions inconsistently. This inconsistency results in uncertainty and doubt among controllers about how to properly fulfill their legal obligations.

Chamber of Digital Economy

T + 48 506 577 824 E BIURO@EIZBA.PL | WWW.E-IZBA.PL
A ŁUCKA 18 LOK. 76, 00-845 WARSAW NIP 701-039—19-22 KRS 0000474028



The adoption of model solutions at the central level could help unify certain practices and lead to their broad acceptance by supervisory authorities across all European jurisdictions.

CONCLUSION

Undoubtedly, the European Commission's initiative for at least partial deregulation of the GDPR regulatory landscape deserves support. The experience of the last 7 years of GDPR applicability shows that there are areas where some controllers (especially those whose scale of operations is minor) are burdened with too many obligations. Such regulations do not bring the intended benefits while limiting competitiveness among entrepreneurs.

However, the solution proposed by the European Commission currently seems only as a starting point for further discussion and alteration. The proposal in its current form raises doubts in terms of interpretation, while the identified area of deregulation does not seem to be the right direction of change.

In principle, the European Commission's actions should rather focus on issues that can bring actual benefits to controllers, which, however, should not come at the expense of a lower standard of personal data protection. This is precisely the issue that should guide the European Commission's further legislative work, as deregulation should not be reduced to merely limiting the application of regulations and exempting some entities from the implementation of current obligations – this would only lead to a reduction in the high level of personal data protection in the European Union, without bringing the expected reform.

poświadczenie złożenia podpisów i pieczęci elektronicznych

Certyfikat dla dokumentu o Autenti ID: 56d1df8f-edcb-437f-9550-70af59a74e2e
utworzonego: 2025-07-09 14:10 (GMT+02:00)

Dokument przekazany do podpisu przez Izba Gospodarki Elektronicznej biuro@eizba.pl, został zabezpieczony pieczęcią elektroniczną Autenti przed wprowadzeniem nieautoryzowanych zmian.



2025-07-09 14:10 (GMT+02:00)

Patrycja Staniszevska

patrycja.staniszevska@eizba.pl

Izba Gospodarki Elektronicznej

NIP: 7010391922 | Prezes Zarząd



**Podpis elektroniczny
zabezpieczony pieczęcią Autenti**

Uwierzytelnienie: e-mail

Powód: Podpisanie dokumentu

Adres IP: 2a00:f41:183c:269cad52:898ab542:3723

2025-07-09 14:24 (GMT+02:00)

Autentyczność oraz integralność podpisanego dokumentu przed wprowadzeniem nieautoryzowanych zmian została zabezpieczona pieczęcią elektroniczną Autenti.



2025-07-09 14:24 (GMT+02:00)

Niniejszy dokument stanowi poświadczenie wykonania usługi zaufania, w tym złożenia podpisów elektronicznych, zgodnie z zasadami opisanymi w Polityce.

Osoby podpisujące dokument złożyły podpisy elektroniczne zgodnie z zasadami opisanymi w Polityce Usług Zaufania Autenti dla podpisów elektronicznych Autenti oraz obsługi podpisywania dokumentów (dostępnej na: <https://autenti.com/pl/regulaminy>) oraz oświadczyły, że znają i akceptują treść podpisywanego dokumentu a także potwierdziły poprawność i prawdziwość danych służących do złożenia podpisu elektronicznego.

W ramach składania podpisów elektronicznych przeprowadzono uwierzytelnienie podpisujących.

Usługa została wykonana zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Rozporządzenie eIDAS).

Karta podpisów stanowi poświadczenie Autenti w zakresie realizacji poszczególnych usług zaufania, zgodnie z zasadami ich świadczenia oraz definicjami zawartymi w Polityce.