Council of the European Union
General Secretariat

Brussels, 04 November 2025

WK 14186/2025 INIT

LIMITE

DATAPROTECT
JAI

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
N° prev. doc.:	WK 12926/2025
Subject:	Easing administrative burdens related to the General Data Protection Regulation (GDPR) - Comments from Member States

Delegations will find in the annex written comments from Member States on the Presidency discussion paper on easing administrative burdens related to the General Data Protection Regulation (WK 12926/2025).

ANNEX

I. CZECH REPUBLIC

CZ comments on easing administrative burden related to GDPR

- 22 October 2025
- document WK 12926/2025

General comments:

We are fully ready to explore any targeted proposals for simplification of GDPR, to seek the opportunities to make it easier for businesses, which are the backbone of our economy, to comply with their personal data protection obligations wherever this is compatible with the effective protection of fundamental rights. One systemic-friendly way of doing that is to deepen risk-based approach within GDPR. Another one is to better align the rules of related sectoral instruments.

Any simplifications should be specifically designed, should follow the systematic structure of the General Regulation, should use its parameters, and should not introduce non-systemic elements into it. **Specific proposals** that could be considered include:

- Controllers would not have to make disproportionate efforts to provide less important personal data (backup copies, contact email addresses for low-risk processing etc.) not requested for specific reasons, when responding to requests for access under **Article 15**.
- The obligation to ensure data protection by default in **Article 25(2)** should be subject to the same limiting factors (cost, context, risks etc.) as the obligation to implement data protection by design in Article 25(1).
- Keeping records of processing activities under **Article 30** could be entirely voluntary, as supervisory authorities cannot rely on their completeness and accuracy during audits anyway. Practical value of those records also makes this obligation less than necessary.
- Data breaches under **Article 33** could be reported only to the lead supervisory authority, which would make it easier for the controller dealing with the crisis situation.
- Documentation of data breaches under **Article 33(5)** could only be kept for three years and would not be necessary in low-risk cases that do not involve automated processing.
- A level of risk caused by the infringement should be explicitly taken into consideration when imposing sanctions, preferably directly influencing the maximum fines available under **Article 83**.

(end of file)

II. GERMANY

23 October 2025

German proposal for simplification of the GDPR

In its communication, '**A Simpler and Faster Europe**' of 11 February 2025, the European Commission announced its intent to reduce reporting requirements by at least 25% for all companies and 35% for SMEs, and to reduce all recurring administrative costs by 25%. As part of its objective of simplifying EU rules and reducing administrative burdens, the Commission has proposed the '**Omnibus IV**', which includes targeted modifications of the **General Data Protection Regulation** (GDPR) focused on reducing the burden of record-keeping obligations for SMEs and SMCs and organisations with fewer than 750 employees. The Commission has further announced that it will propose a **digital package** towards the end of the year. This is supposed to form part of a broader assessment of whether the expanded digital acquis adequately reflects the needs and constraints of businesses such as SMEs and small mid-caps, going beyond necessary guidance and standards that facilitate compliance.

Germany strongly welcomes the Commission's efforts to review, streamline, and simplify the digital regulation, including the area of data protection. Therefore, we would like to take the opportunity to contribute to this process with the following proposals:

1) Introductory remarks

With regard to emerging technologies, such as artificial intelligence (AI), which require and enable the processing of large amounts of data, the protection of citizens' and consumers' privacy rights remains extremely important. As an expression of the European fundamental rights to private and family life and data protection (Articles 7 and 8 of the European Charter of Fundamental Rights), the GDPR is a core part of the European community of values. In order to adjust the balance between the data subjects' fundamental rights and the fundamental rights of citizens and companies to process personal data (esp. freedom of information, freedom of the sciences, freedom to conduct a business), any adjustments to the GDPR, while ensuring an adequate level of data protection and preserving the core principles of the GDPR, should be considered carefully and carried out in a purposeful, precise and risk-based manner.

As we have already communicated, the Federal Government has agreed in its coalition agreement to start a discussion concerning a possible exclusion of non-commercial activities, small and medium-sized enterprises and low-risk data processing (e.g. customer lists of tradespeople) from the scope of the GDPR. Small businesses engaged in low-risk data processing activities should, if not completely be excluded from the scope of the GDPR, be exempt from certain GDPR requirements. To further clarify the needs of German companies and other organisations, the Federal Government held consultations with relevant stakeholders.

As a result of these consultations, Germany believes that the proposals in Omnibus IV for simplifying the GDPR do not go far enough. Germany proposes a two-stage process:

- Section 2 below: Germany sees a short-term need for some targeted adjustments to the GDPR, which should already be implemented as part of the Digital Omnibus. Below you will find specific proposals for amendments to the text of the GDPR with corresponding justifications, that should from our perspective be included in the Digital Omnibus.

- Section 3 below: In addition, Germany explicitly welcomes the Commission's intention to launch a Digital Fitness Check to stress-test the coherence and cumulative impact of the EU digital acquis governing the activity of businesses and to examine whether further action is needed to strengthen the competitiveness of the European economy and reduce bureaucracy without lowering the level of human rights protection under European and international law. To this end, Germany is submitting several requests aimed at a more in-depth discussion of a possible data protection reform.

2) Proposals with targeted modifications to include in the Digital Omnibus

Germany is aware that the Digital Omnibus is intended to achieve rapid relief for SMEs, small mid-caps and other organisations of similar size through a number of targeted adjustments. To this end, Germany has identified the following aspects that should be tackled in the Digital Omnibus by targeted measures, including specific proposals for amendments to the regulatory text of the GDPR:

a) Clarification in Recital 40 of the GDPR

We recognise that consent, which is explicitly mentioned in Art. 8 (2) of the European Charter of Fundamental Rights as a legal basis, is an important part of citizens' and consumers' fundamental right of the protection of personal data. However, insofar as the data subject has not exercised this right, Germany sees a need for clarification that consent does not take precedence over the other legitimate bases in Article 6 GDPR. There is a growing tendency in practice – including by some supervisory authorities and courts – to give priority to consent over the other legal bases set out in Article 6 GDPR. This leads to uncertainty in practice.

Germany therefore proposes the following amendment to Recital 40:

'*In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.* ***[The legitimate bases in Article 6 GDPR are equivalent]****.*'

Furthermore we would appreciate a clarification that distinguishes other voluntary elements (e.g. the 'request' in Art. 14 (3) lit a) SDG (Regulation (EU) 2018/1724)) from the 'consent' in Art. 6 (1) lit a) GDPR.

b) Amending Article 9 with regard to disaster relief workers

The range of operations required by disaster and civil protection services and the resulting short notice prior to operations make it practically impossible to collect the health data required to ensure adequate mission-related health protection for both emergency personnel and third parties who come into contact with them during an operation only at or before the start of an operation. Likewise, some vaccinations require multiple doses before they develop full protection, meaning that administering vaccinations at short notice before

operations is not a suitable means of ensuring the necessary health protection for both emergency personnel and third parties who come into contact with them during an operation in all conceivable operational situations. In addition to employees in employment relationships, volunteer civil and disaster protection personnel will also be covered by these regulations in the future, provided that the operation also includes similar activities, such as that of full-time employees of rescue services and fire brigades in the EU. An amendment to Article 9 GDPR is intended to ensure that volunteer emergency workers are treated the same as full-time emergency workers, as they are exposed to comparable health risks in civil protection and disaster relief.

Germany therefore asks for a targeted modification of Article 9 GDPR:

"h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services ***[or civil protection and disaster relief]*** *on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices ***[and for the purposes of protecting the health of civil protection and disaster control personnel]****, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;".*

c) Simplification of reporting obligations under Articles 13 and 14 GDPR

In its 2023 positions on the evaluation of the GDPR, Germany stated that, while the documentation requirement arising from Article 5 (2) GDPR and the information requirement derived from Articles 13 and 14 GDPR fulfil an important function in the overall design of the Regulation, these requirements

entail more work for those applying the GDPR. Meeting the documentation and information requirements may present a challenge with regard to data processing operations which involve only a low risk to data subjects. This is particularly true for controllers whose core activities do not include the processing of personal data. Germany is still of the opinion that this is not only about knowing how to meet these requirements, but primarily about the time and labour this entails.

From Germany's perspective, the comprehensive information requirements for data collection under Articles 13 and 14 GDPR are particularly disproportionate to the level of protection they provide to data subjects. Consumers are also often inundated with information that they cannot possibly comprehend and evaluate in their everyday lives.

With regard to the information requirements, it would furthermore be a significant relief for controllers if, in general, the requirements under Articles 13 and 14 GDPR could be fulfilled by providing the controller's contact details and a link or QR code to detailed information on the website. Currently, media discontinuities are only permitted in exceptional cases. Concentrating the information referred to in Articles 13 and 14 GDPR in one place would significantly reduce the burden on companies. This would mean that they would not always have to update a large number of privacy policies. It would simplify many processes considerably if such an approach were sufficient to fulfil the information requirements.

Germany therefore proposes the following amendments to Articles 13 and 14 GDPR:

Article 13 (4) GDPR should be amended as follows:

'Paragraphs 1, 2 and 3 shall not apply if and to the extent that the data subject already has the information ***[or if the provision of such information proves impossible or, provided the processing is to result in a low risk to data subjects, would involve a disproportionate effort; especially in every-day business; Article 14 (5) (b) shall apply accordingly].'***

/

A new paragraph should be inserted as Article 13 (5) and Article 14 (6) GDPR:

'The information obligations under paragraphs 1 and 2 shall be deemed to have been fulfilled if the controller

a) provides its name and contact details and

b) provides the further information required under this provision via an electronic link accessible to the data subject without disproportionate effort.'

A corresponding new recital should be added:

'In order to facilitate compliance with information obligations, the controller should be allowed to provide the information via appropriate electronic references (e.g. URL or QR code). This is subject to the condition that the data subject has direct access to this information without additional intermediate steps and without obstacles. This approach ensures transparency and protects the rights of data subjects without imposing a disproportionate administrative burden on controllers.'

d) Amendments to Articles 15 and 57 GDPR to counteract abusive requests for information

The GDPR guarantees a high level of protection for data subjects and grants individuals effective rights. This includes, in particular, the right of access under Article 15 GDPR. Only the right of access enables a data subject to effectively exercise the rights of defence provided for in Articles 16 to 22 GDPR.

However, in an increasing number of cases, the data subject rights of the GDPR are being misused for purposes unrelated to data protection. Such cases also have no relation to informational self-determination. These cases include data subjects who express their discontent with the state and its institutions by using access procedures to artificially create protracted and resource-intensive disputes and to bind the resources of authorities and courts for activities unrelated to their core activities. On the other hand, extensive information rights are increasingly coming into conflict with the legal procedures of the Member

States and jeopardising quality of arms in court proceedings. The claims are also misused to gather information about third parties (similar to pre-trial discovery) or to obtain concessions in other areas of law

In the current wording, the options granted to controllers in Article 12 (5) GDPR to deflect certain access requests by refusing to provide information or demanding a fee are not sufficiently practical. Data subjects acting with malign intent adapt to the Regulation and behave in such a way that controllers are regularly unable to prove that the request is excessive. This is due, among other things, to the very high burden of proof placed on controllers. Controllers are thus forced into court proceedings with a very uncertain outcome.

In order to restore the original purpose of the right of access, excessive requests should be defined in several non-exhaustive categories, and the requirement to provide evidence should be reduced to a requirement to present evidence. Instead of the burden of proof being solely on the data controller, a court-verified documentation obligation should be introduced. If the data controller has documented the reasons for assuming excessiveness in a comprehensible manner, the data subject must then explain why their request pursues legitimate purposes as referred to in the GDPR. If it turns out that the classification as excessive was incorrect based on this explanation, a claim for damages under Article 82 GDPR is regularly excluded if the responsible party could initially assume, based on the known facts, that it was dealing with an excessive request.

For the category of obviously unfounded requests, the burden of proof for the data controller should remain unchanged.

Under this new system, initial requests may be excessive, particularly if they are very broadly formulated and the responsible party is in charge of processing a variety of different data categories in various application areas (e.g., an authority with an interface function or a conglomerate company with cross-sectional tasks). In the case of repeated requests, the responsible party would be free to require the applicant to justify the need for a renewed information request. The request may be unfounded if the personal data stored with the controller have

not significantly changed since the last request, taking into account the request interval, the variability of the data set, and the type of stored data.

With regard to the legal consequences, this solution upholds the principle that the controller can decide whether to demand an appropriate fee or refuse to respond to the request. For the fee, the controller would have the option of making the (further) processing of a request which is perceived as excessive dependent on an advance. A final decision on the liability for costs would then be made in the context of clarifying whether the controller correctly assessed that the request was excessive.

If the excessive character of an access request becomes apparent in the course of an ongoing procedure, the proposed GDPR text clarifies that the assessment of a request as excessive by a controller can still be made at that stage, and the legal consequences referred to can thus be drawn from this point onwards.

Along with controllers, supervisory authorities too are increasingly becoming the target of applicants acting in bad faith and are overwhelmed with excessive requests from individuals. Often, the excessive conduct of applicants is not only directed at the controller, but at the competent supervisory authority as well. The explanations set out in points 1 to 6 apply accordingly. In order to address this issue as well, it is necessary to revise the provisions in Article 57 (4) GDPR in a similar way to Article 12 (5) GDPR.

Germany therefore proposes the following changes to Articles 15 and 57 GDPR:

'Article 15

(5) Where requests from a data subject are manifestly unfounded or excessive under paragraph 6, the controller may either

(a) charge a reasonable fee based on the administrative costs and taking into account the actual time spent for providing the information or communication or taking the action requested; in this regard, the controller is entitled to demand a reasonable advance on the expected administrative costs before further processing the request; or

(b) refuse to act on the request.

This also applies if the excessive nature of the request only becomes apparent in the course of the procedure.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. If the controller considers the request to be excessive, it may ask the data subject to substantiate the legitimate nature of their request.

(6) A request is considered excessive in particular if

(a) in the case of a first request, information cannot be provided without the involvement of the data subject or can only be provided with disproportionate effort, and the data subject does not comply with the controller's request to specify his or her request where possible;

(b) in the case of repeated requests, the data subject does not substantiate, contrary to the controller's request, the reasons why this procedure is necessary for the exercise of his or her rights under this Regulation;

(c) the overall circumstances of the individual case indicate that the data subject's request is intended to pursue abusive purposes;

(d) the request is impossible to fulfil.

Article 57

(4) In the case of manifestly unfounded requests or excessive requests under Article 15 (6), the supervisory authority may

(a) charge a reasonable fee based on the administrative costs and taking into account the actual time spent for processing the request; the supervisory authority is entitled to make the further processing dependent on the payment of a reasonable advance on its expected administrative costs; or

(b) refuse to act on the request.

This also applies if the excessive nature of the request only becomes apparent in the course of the procedure.

The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. If the supervisory authority considers the request to be excessive under Article 15 (5) and (6), it may ask the data subject to substantiate the legitimate nature of their request.

If the supervisory authority shares the controller's assessment regarding the manifestly unfounded or excessive nature of the request under Article 12 (5) and (6), it may reject the request without further justification.'

e) Simplifications with regard to the obligation to notify data breaches pursuant to Article 33 GDPR

The deadline for notifying data protection breaches often causes considerable stress, especially for controllers such as SMEs and SMCs and organisations of similar size. The 72-hour deadline is particularly problematic at weekends. With the introduction of further notification obligations concerning cybersecurity deriving from the Directive (EU) 2022/2555 (NIS 2 Directive), there can also be overlapping obligations for controllers. Germany sees a need to simplify notification obligations under Article 33 GDPR and to harmonise the obligation with the requirements of other EU legal acts.

As a first step, Germany therefore proposes clarifying the deadlines for notification of personal data breaches. The deadline of 72 hours should be changed to three working days. That would allow operators to meet the deadline regardless of weekends and national holidays. This should not apply to longer closing periods such as *ferragosto*.

Germany therefore proposes the following changes to Article 33 (1) GDPR:

'In the case *of a personal data breach, the controller shall without undue delay and, where feasible, not later than* ***[~~72 hours~~ three (3) working days]*** *after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data*

breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within ***[~~72 hours~~ three (3) working days]****, it shall be accompanied by reasons for the delay.'*

Recital 106 of Directive (EU) 2022/2555 (NIS 2 Directive) already stipulates that Member States may provide for the use of a single point of contact for reporting security incidents under the GDPR. In order to enable the legally compliant and uniform introduction of such a reporting channel, this idea should also be taken up in the GDPR. The following amendment is proposed for this purpose:

A new paragraph 6 should be included in Article 33 GDPR:

(6) 'Supervisory authorities shall provide technical procedures for fulfilling the reporting obligation under Article 33 which also enable the submission of further reports in accordance with other reporting obligations relating to data security incidents.

'The supervisory authorities shall provide a uniform European reporting form in accordance with the procedure laid down in Article 62.'

3) Further requests for review with regard to the Commission's work programme for this term

a) General remarks

Germany strongly supports the Commission in its intention to examine, in addition to targeted adjustments to the GDPR, whether further measures are necessary to strengthen the competitiveness of the European economy and to relieve other organisations of bureaucracy without lowering the general level of protection provided by the GDPR, and what these measures might be.

Germany suggests a broad dialogue with relevant stakeholders in this process, such as SMEs, SMCs, volunteer organisations, non-profit organisations, associations, the European digital sector (e.g. data holders, data processing services, providers of electronic communication networks/services), especially innovative SMEs and start-ups, civil society organisations in the field of digital rights, consumer protection

agencies researchers/ (public) research sector, cultural sector including cultural institutions, such as museums and theatres, the media sector, data intermediaries/data intermediation services, children and youth advocacy groups, information security experts, national labour administrations, the health sector including health professionals and relevant institutions in the healthcare systems, data protection authorities, the European Data Innovation Board, and the European Data Protection Supervisor.

It has been claimed that the GDPR impairs the competitiveness of European companies. Therefore, it should be examined whether and, if so, to what extent the GDPR affects the competitiveness of European companies. On the other hand, it should be investigated whether compliance with the GDPR can provide a competitive advantage, as others claim. Additionally, it should be examined whether and how economic competition itself has detrimental effects on the right to data protection (Art. 8 European Charter of fundamental rights) as it might incentivise practices that are detrimental to the interests of consumers.

Some claim that the GDPR prevents controllers from digitising out of fear of sanctions. Therefore, it should be investigated whether and to what extent the GDPR has 'chilling effects' which prevent personal data from being processed, even though such processing would be necessary, proportionate and beneficial to the common good or conducive to innovation, because controllers believe that they cannot comply with data protection law or are afraid of sanctions. In this context, the focus should also be on the question whether these are actual intimidation effects caused by regulatory effects or whether the GDPR is being used as an excuse not to push ahead with digital transformation.

It should be closely examined how possible changes to the GDPR would affect data subjects' rights to privacy and data protection, especially in light of risks to privacy and data protection due to digital transformation and artificial intelligence. It should be closely examined how possible changes to the GDPR would affect the fundamental rights at stake, namely the fundamental rights of data subjects (especially the right to private life and the right to data protection), the fundamental rights of controllers and third parties (especially freedom of information, freedom of sciences and freedom to conduct business) and the free movement of personal data.

b) Specific areas for action from Germany's perspective

Germany has already identified the following areas for action which it asks the Commission to examine in more detail with the goal of achieving a more thorough modification of the GDPR.

a. Further strengthening the risk-based approach

Germany is committed to further strengthening the risk-based approach in the GDPR and therefore asks the Commission to examine the following ideas in more detail:

Exclusion of non-commercial and/or low-risk activities from the scope of the GDPR: In particular, Germany requests that close consideration be given to how certain data processing operations (esp. data processing by SMEs, non-commercial data processing and/or low-risk data processing) can in accordance with primary European law, in particular Articles 7 and 8 of the European Charter of Fundamental Rights, and international law, be excluded from the GDPR. In this context, Germany asks the Commission in particular to examine the extent to which the household exemption in Article 2 GDPR could be used to exempt voluntary activities in associations from obligations under the GDPR.

Anchoring the principle of practical concordance: In this context, the principle of practical concordance, which is already enshrined in Recital 4 of the GDPR, could also be very important. Currently, only Recital 4 reflects the relativity of personal data protection and its interaction with other fundamental rights, especially of the controller, that need to be balanced. This could also be included in the text of the law.

Examination of proposals for a 3-layer model: There are currently several proposals for a fundamental reorientation of the GDPR in line with the risk-based approach (3-layer model, among others). Germany asks the Commission to thoroughly examine these proposals for their practicability and feasibility.

b. Security of processing

According to Article 32 GDPR the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The appropriate technical and organisational measures to be

maintained are based on objective legal obligations that are not at the discretion of the parties involved. A waiver of the technical and organizational measures is generally not permissible. For example, it is not possible to have documents containing personal data sent by (unencrypted) email from an authority, even if one specifically asks for them to be sent by email. This should be adjusted. It must be possible to decide for yourself, to a certain extent, on the level of protection on the basis of (voluntary and informed) consent.

c. Clarification regarding anonymisation and pseudonymisation

Germany proposes clarification in the regulatory part of the GDPR regarding (1) the status of anonymous information as opposed to personal data and (2) the process of anonymisation.

Recital 26 of the GDPR already states that the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable.

As Germany already stated in its 2023 contribution to the GDPR evaluation, in our view it is still unclear what anonymisation and pseudonymisation requirements need to be fulfilled to comply with the GDPR. This also applies to the risks that would come with de-anonymisation or re-identification. Germany sees an increasing need for greater clarity in this respect. The provisions of the GDPR need to be worded more precisely to give those applying them legal certainty and to help them calculate the time and money they need to spend on compliance.

This topic is increasingly significant with regard to new data-driven business models in the context of AI and data-intensive processing in the field of research and development, for example in the health sector.

In this regard, we also see it as crucial to **incorporate the ruling** of the European Court of 4 September 2025 (C-413/23 P, para. 86) regarding the concept of **relative anonymity** which – according to the Court – can also be reached by means of pseudonymisation (‘*pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data, in so far as pseudonymisation may,*

depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable').

Therefore, we propose either **clarifying** in Article 4 (1) GDPR that anonymous information is **not to be defined as personal data** (e.g. '*Anonymous information does not constitute 'personal data' in the sense of this regulation*') or **excluding anonymous information from the material scope** of the GDPR (in Article 2 GDPR).

We also propose **defining 'anonymisation'/'anonymous information'** in Article 4 GDPR. We suggest a more elaborate definition of 'anonymisation' than the one taken from Recital 26, e.g. with a reference to state-of-the-art technical measures and also by referring to pseudonymisation as a possible means to render personal data anonymous ('relative anonymisation', ECJ C-413/23 P).

In addition, it has not yet been clarified whether the **process of anonymisation as such** represents a data processing operation consequently requiring in itself the existence of a legal basis within the meaning of Articles 6 or 9 GDPR.

We believe that, for the effective use of data anonymisation to protect data subjects, it should be examined whether the process of anonymisation could be explicitly mentioned as constituting 'processing' in the sense of Art. 4 (1) GDPR (see above proposal). Additionally, it should be examined whether a legal basis for anonymization and exemptions from other obligations of the controller under the GDPR should be created or – alternatively where the need for a legal basis for anonymisation and other obligations of the controller under the GDPR could generally be waived.

Finally, at the level of implementation, the announced guidelines of the European Data Protection Board on anonymisation would still be very important for those applying the law.

cc) Introduction of manufacturer and supplier responsibility

Following the examples of the Cyber Resilience Act and the AI Act, the GDPR should also make manufacturers and providers of standard applications and software responsible for implementing the requirements in future. By using certified products, users should be able to demonstrate compliance with EU law in a straightforward and

legally compliant manner. Germany therefore asks the Commission to examine how manufacturers and suppliers of digital products and services can better be held accountable. Specifically, it should be examined whether and how manufacturers and suppliers could be held responsible for the data protection compliance of these products and services. Currently, responsibility for data protection when using software lies with the controllers and processors. This is insufficient; manufacturers should be held accountable and must ensure that, at a minimum, the processing activities carried out by default via their products can be performed in compliance with data protection regulations.

cc) Further areas for action

Germany has identified the following further areas for action where adjustments to the GDPR should be considered.

Artificial intelligence: The GDPR applies when personal data are processed in AI models and systems, as the Artificial Intelligence Act (AIA) does not affect the GDPR (Art. 2 (7) AIA). This means that the requirements of the GDPR and the AIA apply cumulatively to developers, providers and deployers of AI models and systems. Personal data can play a role in virtually all phases of AI use:

- Data collection and preparation (pre-training): Here, for example, the question arises as to whether personal data may be collected at all (e.g. through web crawling, in public registers, or through commercial acquisition).
- Training of AI models: Personal data may be included in training data sets. This raises questions such as whether further processing for training purposes is permissible at all, and whether and to what extent personal data may or even must be used for bias correction.
- Fine-tuning: AI models are retrained with domain-specific data that might be personal data.
- Use of AI models by deployers: This raises questions such as whether operators are permitted to use AI models that have been trained with personal data.
- Prompting/input: This raises questions such as whether and to what extent users are permitted to enter personal data into chatbots and analysis tools.

- Output generation: This raises questions such as what applies if the AI outputs personal data that was included in the training data set or if the AI "hallucinates" false personal data.

Despite, or perhaps because of, the GDPR's 'untouched' nature, there are numerous regulatory frictions that lead to legal uncertainty and thus burdens for users. Companies and authorities will often have to double-check and balance conflicts between regulatory standards. Mechanisms for solving these conflicts are missing.

In particular, two aspects should be examined: First it should be examined how AI models and systems can be set up in way that enables compliance with the GDPR Secondly – and where the former is not possible or feasible – it should be examined whether separate legal bases would be appropriate for the training and use of AI. It should be examined whether Member State law and opening clauses of the GDPR for AI use in the public interest are possible solutions. It should also be examined how specific rights for data subjects have an effect on the use of AI and how the respective legal framework governing data protection can be calibrated without lowering the standard of protection guaranteed by the GDPR. In this context, especially the risk of outputting false information or sensitive personal data must be taken into account and mitigated.

In general, it should be examined how regulatory frictions between GDPR and AIA could be reduced, how uncertainties about the legal basis for training AI and similar activities could be removed, how data subjects' rights in the context of general-purpose AI can be guaranteed, how unnecessary administrative burdens could be reduced.

Minors: We also want to underline the importance of protecting minors and consider age verification in particular an important issue. There could be an inconsistency with regard to Article 8 (2) GDPR (and Article 83 (4) (a) GDPR) and the lack of mandatory age verification. While the GDPR provides for sanctions for breaching the obligations under Article 8 (2) GDPR, there is no obligation to verify the age of the user in the first place. Germany asks the Commission to carefully evaluate whether this could undermine the whole concept of data protection for minors in general.

Consumer Protection: We call on to the EU-Commission to make use of the option provided for in Article 12 (7) and (8) GDPR to determine via delegated act standardised

icons in order to give citizens and data subjects/consumers in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing.

Research and archiving purposes: With regard to processing for research and archiving purposes (data linkage), we point out that there are still no guidelines with regard to what is permitted in research and how certain regulations are interpreted to ensure the same interpretation in all EU Member States. We want to emphasise the crucial importance of the archival privilege in the GDPR, which forms the basis for data processing for archival purposes in the public interest and makes it possible for archives to fulfil their tasks.

From a German perspective, the opening clauses for scientific research have proven their worth. The GDPR recognizes the special position of research interests in its recitals, for example by interpreting research purposes broadly. However, the special interests of research, which are of importance to society as a whole, should be given greater consideration in the text of the regulation. For example, the text of the regulation – and not just the recitals – should contain a specific reference to consent for areas of research in order to create greater legal certainty for research. This is because there are uncertainties regarding the requirements for effective consent in this area in particular. In research projects, it is often the case that certain purposes cannot be foreseen at the time the data is collected. If the purposes are formulated too broadly, the controller runs the risk of violating the specificity required by the GDPR for consent (Art. 4 No. 11 GDPR).

Certification mechanism: Discussions should also focus on the procedures for establishing certification mechanisms pursuant to Art. 42 et seq. GDPR. On the one hand, certification promises to create trust in the data protection compliance of products and services and, on the other hand, enables proof of compliance with obligations under the GDPR to be provided. Currently, the procedures for establishing certification processes are characterized by their length and complexity, thus preventing the creation of meaningful certificates. Possible areas for simplification could include the adjustment of the time limit in Article 42 (7) sentence 1 GDPR, the formal requirement for the mandatory crediting of existing similar evidence (e.g., information security standard ISO 27001 or data security standard BSI 5), the

introduction of modular certification procedures instead of comprehensive GDPR certification, and the introduction of deadlines for the processing time of administrative procedures.

Establishing coherence in EU data law

In addition, the instruments and administrative structures of various EU data acts must be consolidated in the interest of legal certainty, legal clarity, the competitiveness of the European economy, the fundamental rights of the individual, and the openness of the law to innovation which serve all citizens and businesses.

Regulatory sandboxes: Germany encourages the Commission to include in future adoption/adaptation of digital legislation additional use cases and further regulatory relief for regulatory sandboxes while recognizing protection standards. This would facilitate the use of experimentation clauses in Member States' national legislation.

III. ESTONIA

1. Do you consider that working on enhancing clarity, support and engagement from individual Supervisory Authorities and/or from the EDPB could ease administrative burdens related to the GDPR?

Yes, we do.

3. Do you identify other concrete measures which could be implemented by Member States or the Commission to ease administrative burdens related to the GDPR within the current legislative framework?

For cooperation purposes the DPA-s currently use the IMI system, and no other alternatives exist for cross-border cooperation. IMI is developed by the Commission, for this reason we think it is necessary to emphasize that IMI user interface should be updated in a way that supports an effective investigation process and in addition allows the DPA-s to retrieve necessary statistical data.

4. While ensuring a high level of data protection and preserving the core principles and provisions of the GDPR, do you identify concrete provisions of or obligations under the GDPR that might be subject to targeted amendments to ease administrative burdens related to the GDPR?

We are of the opinion that the GDPR does not require any further changes at the moment. We are of the opinion that companies processing personal data should have a better understanding of when they need to keep a data processing register and define more precisely the terms related to this obligation. Data controllers must also bear in mind that even if they are not obliged to keep a register, they must still comply with the GDPR, have information about what data was processed for what purpose, to whom it was transferred, etc. It must also be borne in mind that allowing a risk-based approach and margin of discretion also increases the possibility of abuse. Importantly, in addition to the condition that companies and organizations with 750/1000 employees do not have to keep a register of processing operations, an additional condition is also provided that these processing operations are not likely to result in a high risk to the rights and freedoms of data subjects. However, a high risk to data subjects is an unsubstantiated abstract legal concept that courts must give substance to the concept, which increases the administrative burden. Clearer guidance is needed in these areas.

IV. FRANCE

Objet : Commentaires des autorités françaises à la suite de la réunion du groupe Data protect du 10 octobre 2025 s'agissant de l'allègement de la charge administrative liée au RGPD pour les entreprises – Note des autorités françaises.

A la suite de la réunion du groupe de travail Data Protect du 10 octobre 2025, la présidence a sollicité les commentaires des États membre sur l'allègement de la charge administrative liée au RGPD pour les entreprises (WK 12926/25). Les autorités françaises souhaitent faire valoir les éléments suivants :

D'une manière générale, les autorités françaises ont déjà indiqué à plusieurs reprises que les besoins exprimés par les entreprises sur le RGPD doivent continuer d'être expertisés afin d'être le cas échéant traités, au besoin par le biais de modifications ciblées à l'occasion de l'omnibus numérique si cela est jugé opportun.

A ce stade, les retours des parties prenantes collectés par la Commission ont montré qu'elles ne souhaitaient pas d'une réouverture du RGPD. Les autorités françaises se sont également exprimées en ce sens et maintiennent cette position. Pour autant, pour atteindre un équilibre optimal entre les enjeux d'innovation et la protection des libertés fondamentales, les efforts de mise en œuvre du texte doivent se poursuivre.

Le rôle du Comité doit être renforcé avec l'adoption du règlement procédural. Le CEPD doit se saisir des sujets à son niveau pour assurer une approche uniforme au niveau européen sur les thèmes qui le méritent. L'harmonisation de l'interprétation et le renforcement de la cohérence dans l'application par les 27 autorités du règlement en Europe sont essentiels à la prévisibilité et à la sécurité de l'environnement juridique des entreprises. Il est nécessaire de réaffirmer le rôle stratégique du CEPD en qualité de garant de la mise en œuvre cohérente du règlement sur le marché intérieur.

Dans le fil des demandes relayées par les autorités françaises et les parties prenantes, ainsi que de la déclaration des autorités de protection des données à Helsinki, la doctrine et les outils développés pour permettre de mettre en œuvre les traitements de données suivant une approche fondée sur le risque doivent mieux répondre aux besoins concrets des acteurs, notamment pour apporter une meilleure visibilité sur les échelles de risques applicables. L'appréciation du degré de probabilité et de gravité des risques associés à un traitement de données est aujourd'hui peu reflétée explicitement dans les orientations des autorités de protection des données.

Le Comité européen de la protection des données pourrait ainsi adopter des lignes directrices communes sur les traitements de données pouvant être exonérés d'analyse d'impact sur la protection des données (AIPD), ainsi que ceux devant faire l'objet d'une AIPD afin que ces aspects soient unifiés pour toute l'Union européenne.

Les autorités françaises appellent le CEPD et les autorités de protection des données à mener rapidement des consultations des acteurs sur les sujets prioritaires que sont l'articulation du RGPD avec le règlement sur l'intelligence artificielle (RIA), la pseudonymisation et l'anonymisation, dans les semaines qui viennent. Il s'agit d'une attente très forte pour que les besoins concrets puissent être exprimés en amont de la finalisation du premier jet des lignes directrices sur ces sujets. Ces échanges doivent permettre de faire remonter les *use cases* sur lesquels les opérateurs ont très concrètement besoin d'éclairages des autorités de protection des données dans la doctrine.

A cet égard, la jurisprudence récente de la CJUE démontre qu'il est possible d'interpréter le RGPD de manière constructive, à droit constant. Elle montre qu'un équilibre pragmatique doit être recherché pour articuler le respect de leurs obligations par les responsables de traitement avec le respect des droits des personnes.

Des lignes directrices compréhensibles, le cas échéant sectorielles, devraient également être envisagées pour décliner les obligations générales de manière spécifique et concrète. De tels outils seraient utiles et nécessaires, par exemple dans des domaines comme celui de la santé, ou du travail.

Il est également nécessaire d'élaborer des référentiels clés en main permettant aux entreprises d'alléger leurs contraintes et leurs charges pour se conformer au règlement. En particulier, pour accompagner mieux encore les TPE/PME, *startups* et *small midcaps*, pour qui le déficit de ressources et d'expertises spécialisées en matière de conformité RGPD est souvent important, les outils de conformité prévus par le RGPD, tels que les codes de conduite, les lignes directrices et les certifications, constituent des moyens essentiels pour décliner l'application du RGPD à des secteurs spécifiques et ainsi renforcer leur sécurité juridique. Ceci permet d'éviter des coûts d'externalisation disproportionnés. Ces outils sont encore trop peu utilisés et les méthodes employées pour l'élaboration de certains d'entre eux suscitent parfois des difficultés pour les acteurs qui s'y engagent. L'implication proactive des autorités de protection des données et du CEPD dans l'identification des secteurs demandeurs de telles initiatives et la participation efficace de ces acteurs à l'élaboration de ces outils de régulation doivent être renforcées.

Enfin, des modes d'accompagnement innovants devraient être envisagés par les autorités de contrôle, par exemple, le développement d'accompagnements plus renforcés, voire de parcours plus expérimentaux, à l'instar des bacs à sables. Les mesures d'accompagnement, si elles nécessitent des ressources et de bien les articuler avec le rôle plus coercitif des autorités, sont essentielles pour assurer un respect optimal des règles de protection des données par les acteurs. L'expérience de la CNIL française à cet égard démontre que ces actions créent de la confiance et de l'adhésion et qu'elles permettent de rehausser le niveau général de conformité des opérateurs. Ces pratiques doivent se développer dans les autres Etats membres, le cas échéant en coopération.

In general, the French authorities have repeatedly indicated that the needs expressed by businesses regarding the GDPR must continue to be examined in depth and, where appropriate, addressed, possibly through targeted amendments on the occasion of the forthcoming Digital Omnibus, if deemed relevant.

At this stage, the feedback collected by the Commission from stakeholders has shown that they do not wish to see the GDPR reopened. The French authorities have also expressed this view and maintain this position. Nevertheless, in order to achieve an optimal balance between innovation challenges and the protection of fundamental rights, efforts to implement the Regulation must continue.

The role of the EDPB should be strengthened with the adoption of the regulation laying down additional procedural rules relating to the enforcement of the GDPR. The EDPB must take on issues at its level to ensure a uniform approach across Europe on topics that warrant it. Harmonising interpretation and reinforcing consistency in the application of the Regulation by the 27 national authorities are essential to ensuring predictability and legal certainty for businesses. It is therefore necessary to reaffirm the EDPB's strategic role with regards to the consistent implementation of the Regulation within the internal market.

In line with the requests relayed by the French authorities and stakeholders, as well as the declaration of data protection authorities in Helsinki, the doctrine and tools developed to implement data processing based on a risk-based approach should better address the practical needs of operators, notably by providing greater clarity on applicable risk scales. The assessment of the likelihood and severity of risks associated with data processing is currently not explicitly reflected in the guidance issued by data protection authorities.

The EDPB could thus adopt common guidelines on data processing operations that may be exempted from Data Protection Impact Assessment (DPIA), as well as a list of those which must be subject to such assessment of the risks, so that these aspects are harmonised throughout the European Union. The French authorities call on the EDPB and data protection authorities to swiftly conduct consultations with stakeholders on priority topics such as the interplay between the GDPR and the AI Act, pseudonymisation, and anonymisation, in the coming weeks. There is a strong expectation that concrete needs can be expressed ahead of the finalization of the first draft guidelines on these topics. These exchanges should allow use cases to be shared, highlighting where operators concretely need clarification from data protection authorities within their doctrine.

In this regard, recent case law from the CJEU demonstrates that it is possible to interpret the GDPR constructively, without amending the law. It shows that a pragmatic balance must be sought to reconcile controllers' compliance with their obligations and the respect for individuals' rights. Understandable, and where appropriate, sector-specific guidelines should also be considered to translate general obligations into specific and practical terms. Such tools would be useful and necessary, for example, in fields such as health or employment.

It is also necessary to develop ready-to-use reference frameworks that would help businesses reduce their compliance constraints and burdens. In particular, to better support micro-, small- and medium-sized enterprises, startups, and small mid-caps — for whom the lack of resources and specialised GDPR compliance expertise is often significant — the compliance tools provided for under the GDPR, such as codes of conduct, guidelines, and certification mechanisms, constitute essential means to tailor the application of the GDPR to specific sectors and thereby strengthen their legal certainty. This helps avoid disproportionate outsourcing costs. These tools remain underused, and the methods employed in developing some of them sometimes pose challenges for the actors involved. The proactive involvement of data protection authorities and of the EDPB in identifying sectors seeking such initiatives, as well as the effective participation of these actors in developing such regulatory tools, must therefore be reinforced.

Finally, innovative forms of support should be envisaged by supervisory authorities — for example, more extensive support mechanisms, or even more experimental pathways, such as regulatory sandboxes. Support measures, while resource-intensive and requiring careful coordination with the authorities' enforcement role, are essential to ensuring optimal compliance with data protection rules by operators. The experience of the French CNIL in this regard demonstrates that such actions foster trust and engagement and help raise the overall level of compliance among operators. These practices should be developed in other Member States, where appropriate in cooperation.

V. AUSTRIA

on discussion paper WK 12926/2025 on easing administrative burdens related to the General Data Protection Regulation (GDPR)

Guidance, enforcement and implementation

1. Do you consider that working on enhancing clarity, support and engagement from individual Supervisory Authorities and/or from the EDPB could ease administrative burdens related to the GDPR?

Yes. We consider that guidelines and other tools that provide clarifications on obligations under the GDPR, both by national supervisory authorities and by the EDPB, can significantly contribute to easing administrative burdens related to the GDPR. It is of utmost importance that controllers are aware of the extent of their obligations: Legal uncertainty can provoke overcautiousness and thus create unnecessary administrative burden.

In that context, we particularly support tools such as a common EU template for GDPR data breach notifications pursuant to Art. 33 GDPR or a single entry point going beyond the GDPR.

2. Do you identify concrete measures or best practices, which could be implemented by individual national Supervisory Authorities and/or by the EDPB to enhance clarity, support and engagement?

Coherence, strengthening legal certainty and practical relevance of the tools provided are key elements of any measure to enhance clarity, support and engagement, in particular with regard to SMEs. In Austria, the Data Protection Authority and the Chambers of Commerce have launched an EU-funded data protection service project to help SMEs master challenges related to data protection, reduce their risks related to data protection (also with regard to new technologies), enhance data security and strengthen customers' confidence in Austrian enterprises. That project, which was launched in February 2025 and is designed to run for two years, includes the development of a GDPR service portal providing

- *„online-self-assessment“ in the form of online guidance*
- *comprehensive service offered throughout the life cycle of SMEs (e.g. starting a business, hiring employees, establishing a web presence, foreign trade, outsourcing GDPR-relevant processes, business transfer)*
- *information on questions of doubt in various areas relevant to data protection where, currently, uncertainties exists (e.g. artificial intelligence)*

3. Do you identify other concrete measures, which could be implemented by Member States or the Commission to ease administrative burdens related to the GDPR within the current legislative framework?

We consider that the supervisory authorities should have a leading role in any measures implemented by Member States in order to ease administrative burdens related to the GDPR within the current legislative framework. The same applies to the EDPB at EU level.

Possible legislative measures

4. While ensuring a high level of data protection and preserving the core principles and provisions of the GDPR, do you identify concrete provisions of or obligations under the GDPR that might be subject to targeted amendments to ease administrative burdens related to the GDPR?

We currently do not identify concrete provisions of or obligations under the GDPR that should be subject to targeted amendments to ease administrative burdens related to the GDPR. The main focus should remain on easing administrative burdens related to the GDPR at implementation and enforcement level.

In general, we consider that upholding the fundamental rights achievements of the GDPR is the most important aspect of this discussion. Easing administrative burdens must not come at the expense of fundamental rights protection and legal certainty. The GDPR strikes a careful, well-considered balance between the protection of data subjects and the interests of controllers. Any amendments should be made only on a selective basis and where strictly necessary.

In our view, the risk-based approach already offers sufficient flexibility for controllers to provide, with regard to the context and circumstances of a processing operation, an appropriate data protection level. We have to keep in mind that the obligations set out in the GDPR are not ends in themselves, but serve the protection of data subjects. Easing administrative burdens should not lead to a decrease in the current level of protection. Moreover, the size of an enterprise should not be the sole criterion for targeted amendments: It is necessary to also consider the type of data processing conducted by a controller and in how far it affects (or could potentially affect) data subjects. In this context, it is essential to maintain the risk-based approach of the GDPR.

VI. POLAND

Q1: Do you consider that working on enhancing clarity, support and engagement from individual Supervisory Authorities and/or from the EDPB could ease administrative burdens related to the GDPR?

Poland is of the opinion that actions aimed at increasing clarity, support, and engagement from both – national supervisory authorities and the European Data Protection Board (EDPB) – are crucial for reducing administrative burdens resulting from the application of the GDPR. We believe this is a key direction for action that allows for the rationalization of obligations while maintaining a high level of personal data protection.

Poland considers that the European Data Protection Board and national supervisory authorities play a crucial role in ensuring consistent and practical application of the GDPR. Experience with GDPR implementation indicates that many administrative burdens, especially for small and medium-sized enterprises (SMEs), do not stem from the provisions themselves, but from a lack of legal certainty and divergent interpretations among Member States.

Active measures by supervisory authorities can significantly contribute to:

- increasing the clarity of regulatory interpretations,
- strengthening support for controllers and processors,
- facilitating the practical implementation of data protection principles.

Providing consistent, understandable, and practical guidance would allow controllers to better interpret their obligations without the need to engage excessive resources in legal analysis or risk incorrect interpretation.

Proposed directions for action:

To effectively mitigate administrative burdens through better support and engagement, Poland proposes focusing on the following main directions for action:

- **Strengthening the role of EDPB guidelines**

  The role of EDPB guidelines as an instrument supporting uniform and pragmatic interpretation of the provisions must be strengthened. It is crucial to publish clear examples, practical templates (e.g. for documentation), and best practices, as well as to ensure early and coordinated guidance on new technologies, such as AI. Preparation of short summaries or 'mini-guidelines' for specific sectors (e.g. education, public administration, e-commerce).

  Harmonisation of terminology – for example, clarifying the precise meaning of terms such as 'on a large scale' or 'significant risk to the rights and freedoms of individuals'.

- **Increasing predictability and consistency in GDPR application**

  It is necessary to strive for a more uniform approach by supervisory authorities across the EU. This particularly concerns areas such as risk assessment, the proportionality of measures taken, the interpretation of legal bases (e.g. legitimate interest), and the status of pseudonymized data.

- **Supporting non-legislative solutions**

  Further simplification and standardization of documentation (e.g., records of processing activities, data protection impact assessments) should be supported. It is also essential to promote practical support and self-assessment tools for controllers, and to promote voluntary certification mechanisms and codes of conduct, which are currently underutilised. It is also important to provide controllers with accessible, free tools and templates (forms, registers, checklists) so that even small companies and public institutions can meet GDPR requirements without engaging large resources, and to facilitate contact with supervisory authorities – for example, thematic hotlines, Q&A portals, and short procedure guides.

- **Emphasis on educational and advisory activities**

  Supervisory authorities should place greater emphasis on educational activities, dialogue, and cooperation with stakeholders. Developing educational initiatives, especially for local government administration and micro-enterprises (webinars, e-learning, guides). For example, online training for SMEs on information clauses or for schools regarding the protection of students' data. Particular attention should be given to entities that do not operate on a large scale or process high-risk data, especially SMEs. Efforts should be made to increase the participation of various groups in the interpretation and consultation process (e.g., entrepreneurs, non-governmental organisations, academic experts).

- **Facilitating access to uniform interpretations**

  Creating easily accessible knowledge bases, such as Q&A sections or databases of case law and decisions, would help avoid discrepancies in the application of the provisions between Member States. Creating information campaigns and materials understandable to citizens (plain language, graphics, short videos). Facilitating the understanding of concepts such as: 'controller', 'processor', 'consent', 'right to be forgotten'. Promoting a positive approach to data protection – not just a legal obligation, but an element of a culture of trust in relations with the customer or citizen.

- **Further developing and enhancing digital tools supporting cooperation**

We believe there is a need to ensure innovative digital solutions to support the cooperation of national authorities, as well compliance for stakeholders. Adequate funding should be ensured.

Poland wishes to emphasise that the GDPR provides a solid and timeless legal framework. We believe that the current provisions provide sufficient flexibility and broad interpretive possibilities. Existing administrative burdens can largely be rationalized precisely through a more active role of the EDPB and national authorities, and better implementation of the existing framework. We are open only to considering limited, technical, and proportionate changes (so-called 'targeted amendments'), provided their goal is to reduce burdens, especially for SMEs, while maintaining a high level of data protection.

In conclusion, Poland appreciates the initiatives already undertaken by the EDPB as part of the so-called *Helsinki Statement on enhanced clarity, support and engagement* and fully supports further, intensive action in this direction. This is the most appropriate way to reduce administrative burdens without weakening the right to personal data protection.

Q2: Do you identify concrete measures or best practices, which could be implemented by individual national Supervisory Authorities and/or by the EDPB to enhance clarity, support and engagement?

Poland identifies a range of concrete actions and best practices that could be implemented by both the European Data Protection Board (EDPB) and national supervisory authorities to increase legal clarity, strengthen support for controllers, and reduce administrative burdens.

We believe there are broad opportunities to reduce administrative burdens without the need for legislative changes, precisely through active measures by the authorities.

We propose focusing on the following concrete measures:

1. Strengthening the role of the EDPB in harmonisation and interpretation

It is crucial to ensure consistent and predictable application of the GDPR across the Union. EDPB guidelines should not be too general or theoretical, as this can lead to divergent interpretations among Member States. Small and medium-sized entities often do not know which recommendations are crucial and which are merely supplementary. To achieve this, the EDPB should:

- Strengthen guidelines as a pragmatic tool. EDPB guidelines should support uniform interpretation, but above all, they should include clear examples, templates (e.g., for documentation), and descriptions of best practices. Preparation of practical guidelines by the EDPB to facilitate the application of the GDPR in the context of new regulations and their links to the GDPR, such as the already adopted guidelines on the DMA and the guidelines on the interplay between the GDPR and the AI Act, developed in cooperation with the AI Office. Regular updating and standardisation of EDPB guidelines, so that they focus more on practical examples and sector-specific case studies.
- Sectoral guidelines on GDPR obligations, as proposed by France, are a good practice to support legal predictability for businesses.
- Ensure consistency in the approach of national authorities. Efforts should be made towards a more uniform approach by supervisory authorities across the EU, especially in assessing risk and the proportionality of measures applied by controllers. We have a platform for cooperation of national authorities and it should be used more strategically. Promoting the principle of proportionality by the EDPB in documentation and obligations, for example, by indicating which requirements are key and which can be simplified for small entities.

- Facilitate access to uniform interpretations through digital tools. Introducing 'short thematic guides' (so-called playbooks) — concise documents in a Question and Answer (Q&A) format, with examples of permitted and forbidden practices. Creating a unified repository of interpretations and decisions available online, with the possibility of searching by topic (e.g., employment, marketing, schools, health). This would allow controllers to quickly verify interpretations and avoid discrepancies between Member States.
- Coordinate the exchange of best practices. The EDPB and the European Commission should develop coordination initiatives to facilitate the exchange of experiences, especially regarding a proportionate approach to reporting and documentation obligations. A common taxonomy of infringements and criteria for imposing sanctions should be developed, so that similar cases are treated similarly across the Union, and that practices among authorities (e.g. in Ireland, or other Member States) do not lead to a lack of a uniform level of GDPR enforcement and hinder the cross-border activities of businesses.

2. Development of practical support for controllers (EDPB and national authorities)

Supervisory authorities should increase their engagement in supporting entities applying the GDPR, especially those with limited resources:

- Any changes must be backed by strong support for increased funding and institutional strengthening of national data protection authorities, enabling them to monitor compliance more effectively and provide appropriate guidance to stakeholders.
- Greater emphasis on education and advice. The GDPR is sometimes perceived as a difficult and formal regulation, and the dialogue between supervisory authorities and the market is limited. Greater openness and exchange of experiences are needed. Authorities should strengthen education, dialogue, and cooperation with stakeholders. These activities should be specifically directed at entities that do not operate on a large scale or process high-risk data, particularly SMEs. Support programs for SMEs, including through EU funds for GDPR compliance training, should be promoted. Proposed actions include: organising cyclical workshops and sectoral consultations (e.g. twice a year) with the participation of representatives from the EDPB, supervisory authorities, and industry organisations; establishing expert groups within the EDPB focused on the practical aspects of the GDPR, which would also include representatives from public administration and SMEs; running information campaigns on the rights of individuals and the obligations of controllers in an accessible format (e.g. video materials, graphics, plain-language guides); creating educational programs within national and EU initiatives (e.g. e-learning training for Data Protection Officers, civil servants, and entrepreneurs).

- Development of practical support and self-assessment tools. Many controllers, especially among SMEs and in the public sector, need practical tools that will help them meet GDPR requirements without excessive costs or external consultants. Therefore, we propose:
    - the creation of interactive compliance self-assessment tools ('GDPR-check') by the EDPB or national authorities – e.g. a simple questionnaire that, upon answering, would generate a set of obligations and suggestions for improvement;
    - the development of document templates and models (records of processing activities, impact assessments, breach notifications, information clauses) – in 'full' and 'simplified' versions for smaller entities;
    - the launch of digital communication portals with supervisory authorities (online forms, case status, expert chat).
- Support for the digitisation of compliance processes. The creation of EU or national electronic platforms should be supported, enabling the automation of maintaining records of activities, conducting risk assessments, or reporting breaches.
- Promotion of standard compliance tools. Certification mechanisms, codes of conduct, and accreditation mechanisms should be actively developed and promoted. Such standardized tools could significantly reduce the need for individual legal analysis and formal documentation obligations for controllers. We support working on enhancing measures to increase the availability of compliance tools (e.g. codes of conduct, certification), especially for SMEs and NGOs, while maintaining high standards of data protection. We also point out the need to increase the financial resources available to supervisory authorities to carry out these activities.

3. Ensuring the coherence of the regulatory ecosystem

In the context of new digital regulations, it is crucial for supervisory authorities and the EDPB to actively work towards legal coherence:

- Better integration of data protection policies with other regulatory frameworks. It is necessary to ensure the consistency of the GDPR with regulations such as the AI Act, DSA, or DMA. The goal is to avoid the duplication of obligations and make it easier for businesses to understand the requirements in the new digital landscape. The EDPB must closely cooperate with the AI Office and AI Board, actively acting towards ensuring coherence. The same should be done at the national level.

Q3: Do you identify other concrete measures, which could be implemented by Member States or the Commission to ease administrative burdens related to the GDPR within the current legislative framework?

Many controllers perceive the documentation obligations resulting from the GDPR (e.g. maintaining records of processing activities, impact assessments, legitimate interest analyses) as too complicated and disproportionate to the scale of their operations.

In our opinion, the priority should be to improve implementation, coordination, and the coherence of the regulatory ecosystem, rather than revising the regulation itself. We identify the following concrete measures:

1. European Commission actions

The Commission plays a key role in ensuring the coherence of the entire EU regulatory environment and in supporting Member States.

- **Ensuring horizontal coherence (combating duplication of provisions):**
    - The Commission should actively monitor and eliminate the overlapping of obligations arising from the GDPR and other digital legal acts (e.g., AI Act, DSA, DMA, Data Act). The simplification efforts should be speeded up.
    - Duplication of existing GDPR mechanisms (e.g., regarding impact assessment, transparency, data transfers) in new, sectoral regulations should be avoided.
    - Within legislative work, the Commission should strive for the harmonization of definitions of key concepts (e.g., "risk," "automated decision-making") across different legal acts, for example, by creating a central glossary.
- **Support for SMEs and digitisation:**
    - The Commission should promote and finance (e.g., from EU funds) support and training programs on GDPR compliance, specifically targeted at the SME sector.
    - The digitisation of compliance processes should be supported, for example, by creating uniform EU platforms or tools that facilitate the automation of records of activities, risk assessments, or breach notifications. There should be exchange of information and best practices to ensure there is no duplication and the products of different projects are widely used.

- Developing and continuously updating by the Commission and the EDPB:
  - model, simplified documentation formats – e.g. a 'record of processing activities' or a 'DPIA light' for entities processing data on a limited scale or with low risk;
  - a set of sectoral examples ('model cases') illustrating which processing operations require a DPIA and which do not.
- Supporting Member States in developing practical guides for public administration that will help avoid excessive formalism (e.g. simplified registers for schools, cultural institutions, or libraries).
- Promoting the principle of 'one assessment, multiple uses' – i.e. if an entity has conducted an impact assessment for one project, identical solutions in the same environment for a subsequent project do not need to be assessed anew.

These actions will help controllers reduce the time spent on preparing documentation, lower costs, and focus more on actual risk rather than formalities.

- **Activation of underutilised GDPR mechanisms:**
  - The Commission, in cooperation with the EDPB, should actively support the faster adoption of codes of conduct and certification mechanisms. These measures are currently underutilised but could significantly lower the cost of demonstrating compliance. Streamlining their approval process at the EU level could be considered.

2. Member States actions

Member States, with the support of the Commission, should focus on practically facilitating the application of the law at the national level.

- **Harmonization of reporting obligations:**
  - Member States (in cooperation with the Commission) should strive to harmonise and reduce the duplication of incident reporting obligations arising from the GDPR and other regulations (e.g., NIS2, DORA and other sectoral legislation). The complexity of reporting obligations poses particular challenges for entities operating in multiple Member States, and for SMEs with limited resources to navigate fragmented obligations. There should be the EU-level reporting standards, with a view to establishing harmonised reporting, allowing exchanging key information between stakeholders using single reporting platforms. The introduction of single entry point for incident notifications should be encouraged as it represents a valuable solution. Whether established at national level or through an EU-coordinated mechanism, such entry point would enable entities to interact with multiple regulatory regimes via a unified interface, ensuring that relevant authorities receive the necessary information. There is a need for close cooperation of EDBP with the NIS Cooperation Group and ENISA.

The notion of the once-only principle applied across different legislation should be promoted, ensuring that stakeholders are not required to submit the same information multiple times under different legal instruments. Instead, information provided under one regulation should be recognised and reused, where appropriate, across other frameworks. EDPB in cooperation with the NIS Cooperation Group and ENISA should play a key role in supporting the implementation of the once-only principle.

- **National support for SMEs:**
    - Member States should develop national educational programs and support tools (e.g., practical guides, helplines) aimed at SMEs and public entities with limited resources.
    - Communication portals with national authorities could allow for checking the status of a submission, the history of infringements, or the supervisor's current recommendations.
    - Electronic templates for DPIA, 'DPIA light', RoPA, and information clauses could be developed, which users could complete by filling in only the necessary fields.
    - The development of compliance self-assessment tools provided by national authorities could be supported – for example, simple online questionnaires for entrepreneurs.
- **Cooperation between authorities:**
    - The creation of national and EU cooperation forums between regulators (data protection authorities and sectoral authorities) should be supported to ensure interpretive coherence at the interface of the GDPR and other provisions.

3. Joint actions (Commission and Member States)

- **Exchange of best practices:**
    - It is crucial to develop coordination initiatives within the EDPB and the Commission that serve to exchange experiences and best practices among supervisory authorities. Particular emphasis should be placed on developing a proportionate approach to documentation obligations (e.g., the record of processing activities) in entities with low processing risk.
- **Maintaining dialogue with stakeholders:**
    - Broad consultations should be conducted with stakeholders to precisely identify whether the greatest burdens result from the GDPR provisions themselves or from interpretive problems or interaction with other regulations.

Q4: While ensuring a high level of data protection and preserving the core principles and provisions of the GDPR, do you identify concrete provisions of or obligations under the GDPR that might be subject to targeted amendments to ease administrative burdens related to the GDPR?

Poland approaches the issue of potential legislative changes to the GDPR with great caution. We share the widely expressed view that **there is no need for a systemic reopening of the GDPR**, as its principles and architecture remain appropriate and adequate.

At the same time, we are open to considering limited, technical, and proportionate changes (so-called '**targeted amendments**'), provided their sole purpose is to reduce administrative burdens, especially for SMEs, while maintaining a high level of data protection. Any changes must be pinpoint, supplementary, and technical in nature. We also emphasize that the fundamental principles, rights, and obligations contained in the key chapters of the GDPR (I, II, III, and V) should remain unchanged.

Within this limited scope, we identify the following concrete provisions and obligations that could be subject to targeted amendments:

1. Information obligations (Articles 13 and 14)

The current information requirements are perceived as a major source of burden, leading to the creation of extensive and complicated information clauses that are difficult for recipients to understand. Paradoxically, this makes it difficult for natural persons to understand how their data are actually being used.

- **Informing about rights (Article 13(2)(b) and Article 14(2)(c)):**
    - **Challenge:** These provisions require informing about all rights available to the data subject, even if some of them (e.g. the right to data portability) are not applicable in a given processing scenario (e.g. processing based on legitimate interest). This misleads the data subject.
    - **Proposed amendment:** Clarifying the provisions so that the controller informs only about '**applicable rights** that can be exercised by data subjects, taking into account the nature of the processing'.

- **Informing about data transfers (Article 13(1)(f) and Article 14(1)(f)):**
    - **Challenge:** The provision requires indicating 'the means by which to obtain a copy' of the appropriate safeguards (e.g., SCCs or BCRs). In practice, this is interpreted as an obligation to provide the full text of agreements, which is impractical and raises concerns about business secrecy.
    - **Proposed amendment:** Replacing the requirement to provide a 'copy' with the obligation to indicate a '**description**' of the safeguards applied and information on '**where such a description has been made available**'.
    - We propose considering the explicit introduction of the 'layered information obligation' principle, meaning a short summary (purpose, controller, legal bases) with additional details available upon expansion or clicking.
    - Allowing the use of common, approved templates for information clauses prepared and adopted by the Commission or the EDPB.

2. Maintaining a record of processing activities (Article 30)

- **Challenge:** The obligation to maintain a record of processing activities (RoPA) is a significant burden, especially for micro and small enterprises and is often perceived as overly formalised. The existing exemption in Article 30(5) is considered unclear, as the condition that the processing is 'not likely to result in a risk' is practically impossible to meet, as every processing generates some risk. It should also be noted that in practice, most entities still have to maintain full documentation anyway, because data processing is usually not only occasional.
- **Proposed amendment:** Simplifying and making this obligation more flexible for SMEs. This could be achieved by:
    - Changing the threshold for the exemption in Article 30(5) – replacing the current 'risk' criterion with the criterion of '**high risk**'. Clarifying the criteria for applying the exemption under Article 30(5), so that it genuinely covers low-risk entities.
    - Considering the European Commission's proposal (Omnibus IV Package), which suggests raising the employee threshold for this exception (e.g. to 750 employees), provided the processing is not high risk. Poland believes simplifications should not be based solely on the number of employees, but should also consider the scale, nature, and context of the processing (a risk-based approach).
    - Furthermore, we believe that the restriction of the obligation to keep a register of processing activities, as already proposed by the Commission, should apply to entities employing more than 500 people (not 750).
    - Introducing the possibility of using a 'simplified register' (RoPA-light), containing only basic information (e.g. purposes, categories of data, and recipients) for low-risk processing operations.

- Enabling the EDPB to develop register templates for different categories of controllers.

3. Notification of a personal data breach (Article 33)

Many controllers are uncertain whether every breach must be reported to the supervisory authority. The lack of a common risk matrix leads to over-reporting of incidents that do not pose an actual threat.

Therefore, an attempt should be made to clarify the concept of 'likely to result in a risk to the rights or freedoms of natural persons', enable the EDPB to develop a common EU risk assessment matrix, and consider allowing a simplified notification procedure for minor breaches or those with limited impact (e.g. an online form with automatic confirmation). As a result, more effective supervision and a reduced burden on authorities and controllers from minor notifications can be achieved.

4. Administrative fines and the principle of proportionality (Article 83)

Although the system of fines is intended to ensure effectiveness and a deterrent effect, in practice, it leads to fear of sanctions even for minor formal shortcomings, which discourages open dialogue with supervisory authorities.

We propose considering a clarification of Article 83(2) by introducing a 'remedy before sanction' principle – meaning that, exclusively for minor infringements, the controller should have the right to voluntarily rectify them before a fine is imposed, and by emphasising the importance of warnings and corrective recommendations as an alternative to financial penalties in the case of SMEs and public entities in such matters. As a result, a more partnership-based and educational nature of supervision for minor infringements can be achieved, reducing uncertainty and costs for controllers.

5. Definitional and scope issues

- **Automated decisions (Article 22):**
  - Amendments to Article 22 of the GDPR could be considered to ensure coherence of concepts and the interplay between the GDPR and the AI Act, while maintaining a high standard of protection of fundamental rights.
- **Joint controllership (Article 26):**
  - **Challenge:** Case law (e.g. *Fashion ID*) has led to a situation where unrelated entities with different purposes and varying authority (e.g. Facebook and a fan page administrator) are considered joint controllers, which creates practical problems.
  - **Proposed amendment:** Considering the introduction of the concept of '**parallel control**' into Article 26 to distinguish it from genuine joint controllership, where entities jointly decide on the purposes and means.
- **Processing agreements (Article 28(3)):**
  - **Challenge:** The concept of 'nature of processing' is interpreted differently in Member States, which hinders the standardization of agreements.
  - **Proposed amendment:** Clarifying this concept in the provision or recital.

- **Data processing by natural persons (non-professional use):**
    - **Challenge:** The rigours of the GDPR seem disproportionate in small-scale processing situations by natural persons outside of a purely personal purpose, e.g. in the case of dashcams or neighbourhood monitoring.
    - **Proposed amendment:** Considering the creation of a separate, simplified '**sub-regime**' for this type of processing, e.g., with lighter information obligations.
- **Unsolicited data:**
    - **Challenge:** The GDPR does not distinguish between active data acquisition and passive receipt (e.g. in the content of an unwanted email).
    - **Proposed amendment:** Adding explanatory language (e.g. in a recital or article) to clarify that the mere '**receipt of data and not taking conscious action**' (as opposed to, for example, anti-virus scanning) does not constitute automated processing within the meaning of the GDPR.

VII. SLOVENIA

Easing administrative burdens related to the General Data Protection Regulation (GDPR)

Slovenia supports efforts to make the EU legislative framework less burdensome for micro, small and medium-sized organisations. However, we firmly oppose any attempts to redefine fundamental rights, and the safeguards associated with them as mere administrative burdens. We also oppose the relaxation of obligations that are essential for the effective protection of these rights.

We are particularly concerned about proposals to introduce further amendments without prior impact assessments. Not only in terms of their implications for the protection of fundamental rights, but also regarding the potential shift of administrative burden onto supervisory authorities and judicial bodies. The impact on these institutions is of relevance, as it may affect the protection and effective exercise of the full spectrum of fundamental rights, potentially resulting in long-term adverse effects.

Slovenia does not support reopening the General Data Protection Regulation (GDPR), especially in the context of Omnibus proposals discussed in working groups that are not mandated to address substantive data protection matters. Discussions in working groups dealing with Omnibus packages often proceed at a very rapid pace, justified by the urgency to adopt simplification measures. However, this accelerated process frequently fails to reach the level of technical and legal scrutiny that matters of such complexity and sensitivity require.

Our focus should remain on non-legislative measures within the existing EU personal data protection framework. Ensuring uniform interpretation and providing additional implementation tools would be more effective than legislative amendments, as this approach would not require adaptation to a new legal regime but would instead strengthen the application of the established legal framework, whose primary objective remains the provision of a high level of protection of the fundamental right to the protection of personal data.

In this context, we see a way forward in the development of standardised templates, identified by the DPAs and the EDPB, as key instruments for improving the implementation and enforcement of the GDPR. It would be reasonable to first focus on those templates that enable a harmonised understanding of obligations introduced by various recent EU legislative acts in the digital sphere, and that facilitate or accelerate compliance with the broad range of obligations envisaged by these acts.

VIII. FINLAND

The Presidency has requested the Member States to submit their written contributions and suggestions on how to ease the administrative burden related to the General Data Protection Regulation (EU) 2016/679 (hereinafter the GDPR). As a follow up to the meeting of the Working Party on Data Protection on 10 October 2025, Finland provides the following written contributions.

1. Do you consider that working on enhancing clarity, support and engagement from individual Supervisory Authorities and/or from the EDPB could ease administrative burdens related to the GDPR?

Yes. Finland considers it important that the supervisory authorities (hereinafter the SAs) and **the European Data Protection Board (hereinafter the EDPB) give practical guidance**. Finland considers that guidance should primarily be given by the EDPB – **in order to ensure a harmonized interpretation of the GDPR and uniform level of data protection in the EU**.

Finland considers that **practical, tailormade guidance can increase legal certainty and reduce unnecessary administrative burden**. Finland emphasizes that both public and private sector needs legal certainty and encourages the EDPB to take both sectors into account in the future guidelines.

2. Do you identify concrete measures or best practices, which could be implemented by individual national Supervisory Authorities and/or by the EDPB to enhance clarity, support and engagement?

Finland considers that the Council position[1] **and the COM report**[2] from last year identifies several areas where practical guidance would be welcomed. For instance, practical guidance on **anonymization/pseudonymization**, on **scientific research** as well as **protection of minors'** personal data, are important matters. Overall, Finland considers that practical and tailor-made tools and guidance for SMEs is vital.

3. Do you identify other concrete measures, which could be implemented by Member States or the Commission to ease administrative burdens related to the GDPR within the current legislative framework?

Finland considers it important that the Commission gives joint guidance with the EDPB on the interplay between the GDPR and other digital sector legislation, such as the AI Act. A practical joint guidance would alleviate administrative burdens related to the GDPR. In addition, Finland welcomes the Commission to continue their work on developing practical tools to support the robust enforcement of the GDPR and support SMEs, in particular.

---

1 Council position and findings on the application of the General Data Protection Regulation (GDPR); ST 15507/23.

2 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Second Report on the application of the General Data Protection Regulation; COM/2024/357 final.

4. While ensuring a high level of data protection and preserving the core principles and provisions of the GDPR, do you identify concrete provisions of or obligations under the GDPR that might be subject to targeted amendments to ease administrative burdens related to the GDPR?

Finland considers that **the GDPR is still up-to-date, and the main emphasis should be on efficient and robust enforcement**. However, **Finland is willing to discuss on possible, targeted measures to alleviate administrative burden and legal uncertainty related to the GDPR**. Regarding this Finland emphasizes that the level of protection and the core of the GDPR should stay intact (e.g. the scope, principles, definitions, legal basis, elevated protection for special categories and data related to criminal convictions, as well as the core regarding international transfers).

In particular, **Finland considers it important to ensure that the GDPR does not lead to unnecessary administrative burden on the micro, small and medium-sized enterprises** (hereinafter the SMEs). With regard to easing the administrative burden related to SMEs, Finland considers that the Commission has already proposed measures to alleviate administrative burden in the **Omnibus IV -proposal** concerning the SMEs and small midcaps (hereinafter the SMCs). Finland has supported this proposal.

Finland considers that, in addition to Omnibus IV (small midcaps), it would be possible examine **Article 33 (Notification of a personal data breach to the supervisory authority) of the GDPR** and to assess whether the threshold for notification should be clarified or raised. This could increase legal certainty and reduce administrative burdens.

Concerning **Article 35(5) of the GDPR**, which was under discussion during the Working Party meeting, Finland sees value in establishing a harmonized list of the processing operations where there is no need for data protection impact assessments (hereinafter DPIAs). Therefore, **Finland is preliminarily willing to assess** whether establishing a list should be an obligation and especially **whether this list should be established by the EDPB**. Finland sees that this could improve legal certainty and reduce the administrative burden.

Other targeted amendments to ease administrative burden and improve legal certainty related to the processing of personal data

In addition to the GDPR, a large number of EU legislation (especially digital sector legislation) contains provisions which are somewhat overlapping, stricter and/or deviating compared to the GDPR. This causes legal uncertainty and unnecessary administrative burden.

Finland emphasizes that it is **vital to ensure the interoperability of other EU legislation with the GDPR**. Therefore, **Finland welcomes the Commission to examine horizontally other EU legislation with the GDPR**.

Finland considers that the Commission should examine in particular:

- **overlapping and stricter reporting and notification obligations** (e.g. Article 27(4) of the AI Act and Article 35 of the Platform Work Directive); as well as
- **unclear and deviating definitions** (e.g. *biometric data* in Article 4, paragraphs 34 to 36 of the AI Act and *special categories of data* in Article 7(1) of the Platform Work Directive).

In addition, **Finland encourages the Commission to continue its work on updating the ePrivacy legislation** in order to clarify and ensure the interplay with the GDPR.

IX. SWEDEN

Written comments on easing administrative burdens related to the General Data Protection Regulation (GDPR)

Dear Presidency,

Thank you for this opportunity to submit written comments on the ongoing discussion regarding easing administrative burdens related to the General Data Protection Regulation (GDPR).

Simplification for businesses is a vital part of strengthening Europe's competitiveness. Less administrative burdens and a predictable regulatory environment are integral parts of the work to improve the conditions for stronger growth within the EU. Sweden supports tangible simplifications while safeguarding core policies. It is also essential to recognize that a strong protection of privacy within the EU is of vital importance for the free flow of personal data and thus the proper functioning of the internal market.

For Sweden, it is essential to assess and address further needs for simplification and coherence within the current digital acquis. The upcoming Digital Omnibus should therefore assess and, where appropriate, streamline regulatory overlaps from a compliance perspective. Such measures could address reporting and documentations requirements as well as risk assessments. Another area of focus could be on the fragmentation in the application of the digital acquis and overcoming challenges in the application of the complex EU framework on data protection.

In terms of concrete provisions and/or obligations that might be subject to targeted amendments in the GDPR, Sweden would like the Commission to consider the following measures and areas:

- The possibility to ease the documentation obligation under Article 24(1), at least if the processing is not likely to result in high risk for individuals' rights and freedoms.

- The possibility to raise the threshold for personal data breaches that must be notified under Article 33, by e.g. broadening the current exception set out in Article 33(1) beyond "breaches unlikely to result in a risk to the rights and freedoms of natural persons".

- To clarify the requirement to carry out an impact assessment under Article 35 of the GDPR.

- The possibility to make the right to lodge a complaint under Article 77 subject to certain conditions, for instance making the right conditional upon prior notice or engagement with processor or controller concerned.

Further, Sweden would like to draw the Commission's attention to Chapter V of the GDPR regarding transfers of personal data to third countries or international organisations and asks the Commission to reflect
upon the possibilities to ease or simplify the responsibilities of the individual controller or processor.

Even though these measures and areas do not constitute an exhaustive list, they represent areas identified as important for the simplification agenda
while safeguarding core policies.