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.