GDV Gesamtverband der Versicherer

POSITION PAPER

Position Paper

of the German Insurance Association
(GDV)
Transparency register no. 6437280268-55

on the Evaluation of the General Data Protection Regulation (GDPR)

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
P.O. Box 08 02 64, D-10002 Berlin
Phone: +49 30 2020-5000 · Fax: +49 30 2020-6000
Lobby Register No. R000774

Rue du Champ de Mars 23, B-1050 Brussels
Phone: +32 2 28247-30 · Fax: +49 30 2020-6140
ID Number 6437280268-55
www.gdv.de

Contact
Data Protection/Fundamental Issues

E-mail
data-protection@gdv.de

Contents

Executive Summary

The requirements on data processing have changed since the GDPR has come into effect. The ongoing **digitalisation** of business processes will require adaptations to the GDPR provisions and their interpretation by data protection authorities.

- The prohibition on **automated individual decision-making (Article 22 GDPR)** with its overly restrictive derogations does no longer meet the requirements of digitalisation in the mass market business of insurances and the clients' needs. In order to better meet these changing needs, we believe that a combination of other, but very effective protection instruments would be more suitable than a ban: Transparency about the automated decision and – at the customer's request – in-depth information on decision making and verifiability by a human being. At the very least, the restrictive interpretation of the derogations by the data protection authorities should be dismissed and additional derogations for settling the claims of third parties should be drawn up (see 2.1).
- The requirements on the **anonymisation** of personal data shall be defined and be clear and easy to fulfil (2.2).
- IT applications, products, systems and analysis models can often be developed with synthetic or anonymised data. In order to put them into operation safely and without discrimination, tests with real personal data are often necessary. This requires a clear legal basis for the use of personal data, including special categories, over and above Art. 10 (5) of the AI Regulation, insofar as this is absolutely necessary for the development and testing of IT applications, products, systems and analytics models. The protection of the rights and interests of the data subjects should be ensured through high technical and organisational measures. (2.3).
- The principle of **data minimisation** is obsolete with regard to self-learning systems (2.4).
- It should be possible to take technical and organisational measures based on the respective risk when it comes to the **transfer of data to third countries (Article 44 et seq. GDPR)**. In addition, the requirements on binding corporate rules (BCRs) and consents to the transfer of data to third countries should be limited to what is required by law (2.5)

The application of the GDPR has shown that further actions are required.

- A uniform **legal basis across Europe with regard to the processing of data concerning health in the insurance industry** would increase legal certainty and create a level playing field for direct insurers and reinsurers in Europe (3.1).
- A clear legal basis should be created with regard to the processing of data within groups of undertakings, in particular with regard to data within the meaning of Article 9 GDPR (3.2).

- The **rights of the data subjects** should correspond to the data protection risk. The obligation to provide information can be restricted with regard to business partners and their employees and can be limited based on the context of the processing (3.3.1). The right of access should be limited to its use for the purposes of data protection law (3.3.2).
- The development of industry-specific and processing-specific **codes of conduct** should be encouraged more effectively (3.4).

1. Introduction

German insurance undertakings manage more than 450 million insurance contracts. They settle claims and pay benefits in the amount of more than Euro 180 billion each year. Data processing has changed significantly in the undertakings since the General Data Protection Regulation (GDPR) has come into effect. The **processing of data** will be increasingly **digitalised**. The European Commission has recognised the importance of data for the competitiveness of the European economy and has initiated **numerous legislative projects to improve the exchange of data**. Most of this legislation does not affect the GDPR, which, however, leads to huge challenges in applying this legislation, as is the case for example with the Data Act, the European Health Data Space and the Financial Data Access Regulation.

However, data protection legislation must also be able to keep up with these developments. In many cases, the provisions of the GDPR can indeed be interpreted as “digitalisation-friendly”. As a result of **EDPB guidelines**, however, they are often subject to a much more narrow framing, which will eventually become a **barrier to digitalisation and thus to innovation** due to the interpretation by national data protection authorities.

In this paper, we will identify barriers to digitalisation caused by data protection legislation and present proposals on how to overcome these barriers. In addition, we will elaborate on the need for creating special **legal bases** with regard to data processing in the insurance industry, for restricting excessive **rights of data subjects** as well as for encouraging the implementation of **codes of conduct**.

2. Data protection as a barrier to digitalisation

2.1 Automated individual decision-making (Article 22 GDPR)

Customers of insurance undertakings expect ever faster processing of and decision-making on their insurance matters, in particular with regard to online conclusion of contracts and online claims reporting. This requirement can no longer be met without automated individual decision-making. Automated individual decision-making as stipulated under Article 22 GDPR will thus become increasingly relevant for day-to-day operations of insurance undertakings.

It has been shown that Article 22 GDPR, in its current version, puts overly narrow restrictions on digitalisation, which is due, amongst others, to its interpretation by data protection authorities and the European Court of Justice.

In its judgment on case “C-634/21 - SCHUFA Holding (Scoring)” of 7 December 2023, the European Court of Justice explicitly stated that Article 22 GDPR lays down a **prohibition**. That means that an automated individual decision that is subject to this provision will be illegal unless any of the derogations, referred to in Article 22(2) and (4) GDPR, apply.

Derogations from the prohibition, as stipulated under Article 22(2) and (4) GDPR, are **interpreted more narrowly than their wording suggests** by data protection authorities. In addition, there is a **lack of derogations** for issues that are relevant in practice. Solely automated decisions, which would be very useful in day-to-day operations of insurance undertakings, are heavily restricted as a result.

Overly narrow interpretation of the derogations referred to in Article 22(2) and (4) GDPR

The European Data Protection Board and national data protection authorities restrict the derogations provided under Article 22(2) and (4) GDPR in a way that goes beyond their wording.

According to the EDPB, a decision based solely on automated processing pursuant to **Article 22(2)(a) GDPR** shall only be “necessary” for entering into, or performance of, a contract within the meaning of the provision if the intended objective cannot be achieved with a less privacy-intrusive solution (Guidelines on automated individual decision-making and profiling, WP 251 rev.01 no. IV.C.1.). German data protection authorities therefore conclude that automated individual decision-making is usually not “necessary” for the performance of an insurance contract since this task can also be performed by a human being.

Data protection authorities are also of the opinion that consent pursuant to **Article 22(2)(c), Article 22(4), Article 7(4) GDPR** shall only be effective if the data subject, right from the outset, has the option to choose processing by a human being instead of solely automated decision-making. This opinion is based on the EDPB Guidelines 05/2020 on consent (para. 30). The freedom to provide digital products, which is part of the freedom to conduct a business, will be overly restricted as a result.

This narrow interpretation of the derogations results in the fact that customers' affairs may not be processed by undertakings in a fully automated way even in a first run (which may be verified later on). The digitalisation of processes will thus be prevented altogether or organisational measures which will outweigh the benefits of digitalisation will be imposed on undertakings.

Lack of derogations for third-party claims

The **derogations** referred to in Article 22(2) and (4) GDPR do not cover all data processing activities relevant in practice.

Example:

> Damages in third-party liability insurance, e.g. car accidents, can often be reviewed in a fully automated manner and thus be settled rapidly based on information provided online.

However, already due to its wording, Article 22(2)(a) GDPR is not applicable to automated individual decisions of an insurance undertaking concerning persons sustaining a damage under third-party liability insurance. This is due to the fact that the persons sustaining the damage are not contractual partners to the insurance undertaking. Obtaining consent is even more difficult than in a contractual relationship since the person sustaining the damage only asserts his or her claim for compensation and there is no contractual relationship between that person and the insurance undertaking of the person who has caused the damage.

Derogation from decisions as far as a request is being approved

It is still uncertain whether decisions which approve the request of the data subject are covered by Article 22 GDPR.

Example:

> An insurance undertaking accepts an application for the conclusion of an insurance contract or it pays the benefits requested by a policyholder to the claimant after having done a fully automated review of the claim.

These decisions produce “legal effects” and therefore – at first glance – seem to be covered by the wording of Article 22(1) GDPR. That they are nevertheless excluded from the scope of that provision can only be concluded from respective interpretation of the provision. For instance, in his opinion on case C-634/21, the advocate general concludes from the other alternative provided by law, namely “similarly significantly affects him or her”, that Article 22, in general, shall only cover “effects having a serious impact” (para. 34). Clarification under Article 22(1) GDPR or a clear derogation would create legal certainty.

Transparency and verifiability as better protection mechanisms

The ban on automated individual decisions with the overly narrow exceptions means that decisions that could be made quickly and easily by automated means have to be left to humans. The result is time delays and higher costs, which ultimately lead to premium increases for policyholders.

The fact that a ban is no longer in keeping with the times is also shown by Art. 6 et seq. AI Regulation, which do not prohibit even high-risk AI, but provide for transparency and verifiability.

The rights and interests of the data subjects could also be effectively safeguarded within the framework of Art. 22 GDPR. When the decision is communicated, transparency should be created about the fact that the decision was made fully automatically. Furthermore, data subjects should have the right, upon request, to be informed of the main reasons for the decision, to state their own position, to contest the decision and to have it reviewed by a natural person on the part of the controller.

Proposals of the German insurance industry:

⇒ For Article 22 GDPR to be able to meet the requirements of the ongoing digitalisation, the provision should **no longer be designed as a prohibition**. Automated individual decisions should be possible in principle. The **rights and interests of the data subjects** could be ensured throughout: Transparency on the fact that the decision was made in a fully automated manner and the right, upon request, to be informed about the major reasons for the decision, to contest the decision and to have the decision reviewed by a human being.

⇒ At least the following measures should be taken:

- It should be ensured by means of further specification that the derogations laid down in Article 22(2) and (4) GDPR do no longer become ineffective as a result of the restrictive interpretation by data protection authorities.

- Another derogation should also be drawn up for settling the claims of data subjects that do not have a contractual relationship with the controller (example: injured third party in third-party liability insurance). Their rights and interests would also be safeguarded here – as described in the first paragraph.
- It should be clarified in a legally certain way in the legal text that automated individual decisions are excluded from the scope of Article 22 GDPR as far as the request of the data subject is being approved.

2.2 Anonymisation of data

New legal acts by the EU on the exchange of data require an anonymisation of data, such as Article 18(5) Data Act with regard to the data transfer to public sector bodies. An anonymisation of personal data is also required with regard to many data analyses which play an increasingly important role within the scope of digitalisation. Anonymised data are also used for as long as possible to advance existing applications as well as to train and test new applications, products and systems. However, there is considerable legal uncertainty as to when data have been sufficiently anonymised, particularly since the EDPB has not yet provided the previously announced guidelines on this issue.

If data are only considered to be anonymous when they cannot be attributed to a specific person by anybody, anonymisation is practically impossible. For this reason, in its judgment of 26 April 2023 (T-557/20) the European Court of first instance rightly took a relative approach with regard to determining whether information can be related to a specific person. It is also seen critical that some data protection authorities demand a legal basis pursuant to Article 6 and Article 9 GDPR, if applicable, with regard to the anonymisation of data. Good anonymisation, however, is comparable to deletion, which is desirable for the purpose of data protection. This is also made clear in the fifth and sixth sentence of recital 26 of the GDPR. No legal basis should therefore be required for the anonymisation of personal data.

Proposals of the German insurance industry:

⇒ Undertakings require legally certain, reliable provisions which tell them when data are sufficiently anonymised and are no longer subject to the GDPR.
⇒ The reference of data to a person should be determined based on a relative approach. What matters is that the person processing the data is not able to attribute them to a particular data subject.
⇒ It should be clarified that the anonymisation of data does not require a legal basis pursuant to Article 6 and Article 9 GDPR, if applicable.

2.3 Developing and testing IT applications, products and systems

It is in the public interest that IT applications, products and systems that use real personal data work safely and provide accurate outcomes. This applies, in particular, where special categories of personal data are to be processed, such as health data in life and health insurance. In the initial development stage it is often possible to use synthetic or anonymised data. At least at the end, but sometimes already during the development stage, however, tests with real data are required to ensure data security and avoid undesirable outcomes. In addition, the problem with big data applications is that there is not sufficient synthetic test data so that it is necessary to use real data. Ultimately, there will always be some degree of uncertainty as to whether an anonymisation is sufficient (see 2.2).

Examples:

> After the development and integration testing of new IT applications, load and performance tests are being carried out with real datasets in a production-related environment prior to putting the IT applications into operation. The data will be pseudonymised for this purpose to the extent that it is possible and reasonable with regard to the specific use case.
>
> Intelligent applications are examined in secure test environments with a view to ascertaining whether they produce results that reflect reality. The output is compared to results that have been generated in real use cases by traditional means.

So far, a clear legal basis for data processing for the purpose of developing and testing IT applications, products, systems and analytical models with special categories of personal data within the meaning of Art. 9 para. 1 GDPR does not exist in the GDPR yet. In Germany, in particular, data protection authorities call (contrary to the unambiguous wording of the second sentence of recital 50) for another legal basis in addition to Article 6(4) GDPR. However, customer consent is not a practicable solution. It not only means bureaucratic effort. As customers have no immediate tangible benefit from the tests, hardly any feedback can be expected in response to corresponding enquiries.

Article 10(5) of the AI Regulation shows that the legislator has recognised the problem. However, it only provides a legal basis for tests with real data only for a narrowly limited case. It is limited to the development of high-risk AI systems and only applies to the extent that it is strictly necessary for the purpose of preventing discrimination. In all other cases, the use of real datasets in the development and testing stage should be possible as well in order to being able to fulfil the requirements of the GDPR on data security and to not risk any erroneous results and data

breaches when the applications and systems go live.

What is authorised in the AI Regulation for high-risk AI should be even more possible for less risky data processing with data in accordance with Art. 9 para. 1 GDPR.

It is essential that sufficient precautions are taken to protect the rights and interests of the data subjects. This includes limiting the use of genuine personal data to what is absolutely necessary as well as technical and organisational measures to ensure a high level of data security. These may include, for example, a strict limitation of access rights, a high level of protection of the confidentiality and integrity of the data and – where possible – pseudonymisation or encryption.

Proposal of the German insurance industry:

⇒ A clear legal basis regarding the processing of personal data, including special categories of personal data, should be incorporated into the GDPR as far as it is necessary for the purpose of developing and testing new IT applications, products and systems. To protect the rights and interests of the data subjects, technical and organisational measures, e.g. a strict limitation of access rights, a high level of protection of the confidentiality and integrity of the data and – where possible – pseudonymisation or encryption should be provided.

2.4 Data minimisation

The objective of legislation on digitalisation in Europe is to improve the exchange of data and thus the usability of data. More and better information shall be gained from the data for the benefit of the public. In particular where data is being evaluated by means of self-learning AI applications, the scope of the data used by AI cannot always be predicted a priori. It is thus inconsistent with the concept of limiting the processing of data to a minimum. As a result, there will inevitably arise conflicts with the **principle of data minimisation** as stipulated under Article 5(1)(c) GDPR.

The principle is also inconsistent with the aim of preventing discrimination, one of the key objectives of the legislators of the AI Regulation. Experience has shown that discrimination often occurred in cases where the database was outdated or comparably small. This problem can be solved by operating with a database that is as large and unfiltered as possible.

Proposal of the German insurance industry:

⇒ The EU Commission should consider relaxing the principle of data minimisation.

2.5 Facilitating the data transfer to third countries

In a connected world it is almost impossible for undertakings to restrict their data processing on the territory of the EU. Consequently, there must be legally certain tools for data transfers to third countries.

The EU-US Privacy Framework and the current confirmation of the already adopted adequacy decisions relating to further third countries are steps in the right direction. However, respective decisions for other third countries, such as India and Brazil, have not yet been adopted. It is desirable that the EU Commission actively supports the harmonisation of the jurisdictions in further countries in order to be able to adopt further adequacy decisions.

Notwithstanding the above, solutions are required now to enable the transfer of data in a way that complies with the law.

2.5.1 Risk-based approach in Article 44 et seq. GDPR and guidance for assessing the legal situation in third countries

According to the ruling of the European Court of Justice on Schrems II, using the revised standard data protection clauses is not sufficient to justify any data transfer to third countries. Following the Schrems II ruling, the EDPB laid down some very high requirements on the data transfer to third countries within the scope of the Recommendations 1/2020. Undertakings have to devote significant resources since they are required to verify, on a case-by-case basis, the level of data protection in the third country and take supplementary measures that fill any gaps in protection. National data protection authorities often consider the data transfer to be inadmissible even when it involves data that have a low need for protection and when the risk of access to the data is low (e.g. transfer of business e-mail addresses for the purpose of a video conference). It is not comprehensible why the risk-based approach provided by the GDPR (Article 24 and Article 32 GDPR) shall not be applied to the technical and organisational measures adopted for the purpose of transferring data to third countries.

Proposals of the German insurance industry:

⇒ The EU Commission should explicitly incorporate the application of the risk-based approach (Article 24 and Article 32 GDPR) to the measures adopted for the purpose of transferring data to third countries into Article 44 et seq. GDPR.
⇒ In addition, guidance by the EU Commission would be useful to assess the legal situation in third countries.

2.5.2 Binding corporate rules

Binding corporate rules within the meaning of Article 47 GDPR are, in principle, a reasonable tool for the transfer of data to third countries within groups of undertakings. After a short period of application, by issuing the Recommendations 1/2022, the EDPB significantly expanded the requirements which until then had been imposed on controller binding corporate rules (BCRs) (see WP 256 and WP 264 of the Article 29 Data Protection Working Party). According to the Recommendations, the binding corporate rules shall now virtually reflect all of the requirements of the GDPR. In addition, they shall provide a variety of additional measures which go beyond the requirements referred to in Article 47 GDPR. The amendments thus go significantly beyond what is required by the implementation of the ruling on Schrems II. Above all, in practice, the long duration of the approval process will make BCRs increasingly unattractive for groups as a tool for the transfer of data to third countries.

Proposal of the German insurance industry:

⇒ The EU Commission should work to ensure that the requirements on BCRs are being cut back to the level as stipulated under Article 47 GDPR and that the approval processes are being accelerated.

2.5.3 Less strict interpretation of the derogations pursuant to Article 49 GDPR

Under the conditions laid down in Article 49 GDPR, transfers of data to a third country shall be allowed even in the absence of safeguards pursuant to Article 46 GDPR. For instance, Article 49(1)(a) GDPR allows the transfer of data based on the condition that the data subject has explicitly **consented** to the proposed transfer after having been informed of the possible risks of such transfers. The requirements on transparency explicitly go beyond the general transparency requirements on consent pursuant to Article 6(1)(a) and Article 9(2)(a) respectively in connection

with Article 7 GDPR and take account of the special risk situation. The possibility of the data subject to consent to the transfer of data is not being further restricted neither in the wording nor in the recitals. Nonetheless, data protection authorities only allow consent as a legal basis for the transfer of data to third countries in exceptional circumstances. This does not comply with the right to informational self-determination that is being derived from Article 8 ECHR.

Proposal of the German insurance industry:

⇒ The EU Commission should ensure that the transfer of data to third countries is not being restricted beyond the wording of Article 49 GDPR.

3. Further need for amendments

3.1 Processing of data concerning health in the insurance industry

Private life, health and accident insurance in part replaces statutory social security (e.g. substitutive health insurance in Germany) and, in addition, provides important supplements to statutory social security. Contracts in life, health and accident insurance can only be entered into and performed if data concerning health are being processed. The same applies to third-party liability and legal expenses insurance when claims based on health-related harm are being filed. The legal situation with regard to the processing of these data concerning health in the private insurance industry, however, is uncertain. On the one hand, data protection authorities reject the application of Article 9(2)(f) GDPR as well as other derogations provided for social security under Article 9(2) GDPR. On the other hand, in practice, they impose requirements on the voluntariness of consent that are almost impossible to meet. Some European countries have created national legal bases for the processing of data, which vary in detail. The situation leads to practical differences in the cross-border transfer of data. For instance, for reinsurers which do not have any direct contact with customers it is difficult to obtain consent for their processing of data in countries where direct insurers do not require any consent. In general, consent is not a sufficiently reliable and efficient legal basis for the performance of an insurance contract since it can be withdrawn by the data subject at any time.

Proposal of the German insurance industry:

⇒ A clear legal basis with regard to the processing of data for the purpose of entering into and performing an insurance contract (including reinsurance) in Article 9(2) GDPR would create the urgently needed legal certainty for direct insurers and reinsurers in all European countries and a level playing field for all European insurers.

3.2 Processing of data in groups of undertakings

Within insurance groups as well as within groups operating in other industries, tasks are delegated and centralised in order to create synergies and to comply with the requirement of economic efficiency. This is permitted by insurance supervisory legislation pursuant to Article 38 and Article 49 of Directive 2009/138/EC and Article 274 of Regulation (EU) 2015/35.

Example:

> The parent company or a service provider carries out risk assessment and claims settlement for all members of the group of undertakings which include a health insurer, a life insurer and a multiple line insurer with an accident line.

If the data processing within a group does not constitute a form of processing pursuant to Article 28 GDPR, it is considered a transfer of data to a third party in legal terms. Article 6(1)(f) GDPR, however, does not justify the processing of special categories of personal data and therefore cannot serve as a legal basis here. Obtaining consent from all customers would be impractical and would hardly succeed during the term of an insurance contract. Experience has shown that the percentage of customer responses is usually in the single digits in such cases.

Proposal of the German insurance industry:

⇒ In order to allow for legally certain processing of data within in a group of undertakings, in particular of special categories of personal data pursuant to Article 9 GDPR, a clear legal basis should be created within the scope of the GDPR.

3.3 Risk-based approach to the rights of data subjects

The obligation to provide information and the right of access are very important tools to enforce data protection. High bureaucratic requirements, however, will result in the opposite.

3.3.1 Information to be provided (Article 13 and Article 14 GDPR)

Application of the GDPR has revealed early on that the comprehensive requirements to provide information as stipulated under Article 13 and Article 14 GDPR do not meet the needs of business transactions and impose unnecessary burdens

on the data subjects and the undertakings. This does not only apply to small and medium-sized undertakings.

Examples:

> In business communication and business correspondence, business partners and their employees do not expect any privacy information.
>
> During the initial contact with customers and claimants by phone, the “reading” of privacy information and even the respective reference are usually perceived as a tedious delay.

The layered approach introduced by the EDPB within the context of the Guidelines on Transparency pursuant to Regulation 2016/679 (WP 260 rev.01, para. 35 et seq.) makes things only a little easier since the information to be provided within the first layer are still very extensive.

Proposals of the German insurance industry:

⇒ The information to be provided **in the B2B sector** to business partners and their employees pursuant to Article 13 and Article 14 GDPR should **only** have to be kept available **electronically** to prevent unnecessary bureaucratic burden and an information overload of data subjects.
⇒ In other business transactions, the requirement, kind, scope and time of information to be provided proactively should be based on the **context of the data processing** and the risk involved. If, under the respective circumstances, no information is typically expected, the information should not have to be provided proactively, but rather also be kept available electronically and only be sent upon request.

3.3.2 Right of access (Article 15 GDPR)

Insurance undertakings save a wide range of personal data on their customers, insurance intermediaries and employees (e.g. claims, submitted bills, commission invoices, correspondence on behalf of the undertakings) within the scope of their normal course of business. In practice, it has become apparent that the right of access as stipulated under Article 15 GDPR is increasingly not used for the purpose of verifying the lawfulness of the data processing (see recital 63).

Example:

> In a dispute with an insurance undertaking, a former employee or customer

uses his right of access as leverage and demands to receive information on all e-mails that had been addressed to him and all documents in which he is being mentioned.

The European Court of Justice interprets Article 15 GDPR very broadly (case no. C-307/22) by affirming the right of access even when it serves a purpose which is not related to data protection. The interpretation by the EDPB in the Guidelines 1/2022 is also very broad.

According to this interpretation, the right of access goes far beyond the purpose of protection of data protection law. Pursuant to the first sentence of recital 63 GDPR, it is intended to enable the data subject to get an overview of the processing of his or her personal data by the controller and to verify the lawfulness of the processing. However, it is not being provided for in the GDPR that the right of access can be used for the purpose of collecting evidence, as a leverage or for the purpose of facilitating the data subject's document management. The right of access under data protection law should comply with the purpose of protection of the GDPR and should not provide the possibility to be misused for purposes other than the purpose of protection as stipulated in the GDPR.

Proposals of the German insurance industry:

⇒ The purpose of the right of access under data protection law, the verification of the lawfulness of the data processing, should be explicitly incorporated into Article 15 GDPR.
⇒ Purposes on which no information can be requested, e.g. assertion of the right to circumvent the allocation of the burden of proof in civil proceedings, use as leverage or harassment, should be incorporated as exemplary cases of a non-existing right of access into Article 15 or Article 12(5) GDPR.

3.4 Encouraging codes of conduct

Article 40 GDPR provides for codes of conduct for the purpose of specifying the GDPR. These codes of conduct can specify the general provisions of the GDPR for specific industries or areas of processing. They thus provide useful guidance to undertakings as well as to data protection authorities, which helps them assess the lawfulness of the data processing. Pursuant to Article 46(2)(e) in connection with Article 40(3) GDPR, codes of conduct can also provide appropriate safeguards for the transfer of data to third countries. In practice, however, this useful solution has rarely been used so far. This is due, in particular, to the fact that the requirements on codes of conduct and their monitoring stipulated in the Guidelines 1/2019 of the EDPB exceed the provisions stipulated under Article 40 and Article 41 GDPR and

are burdensome to implement. Furthermore, the Guidelines of the EDPB leave room for interpretation, which has led the national data protection authorities to increase the requirements even further or delay approval proceedings on the grounds of uncertainties.

Example:

> Some data protection authorities take the view that a code of conduct must not include any supplementary provisions which reflect the GDPR, beyond the provisions that specify the GDPR in terms of industries, even if it serves a better understanding of the data processing in the industry.

Proposal of the German insurance industry:

⇒ The Commission should actively carry out the mandate to encourage the drawing up of codes of conduct as stipulated under Article 40(1) GDRP and ensure that no requirements that go beyond those stipulated under Article 40 and Article 41 GDPR are being imposed.

Berlin, 27 March 2024