Version as of 29 June 2018

Code of conduct
for the handling of personal data
by the German insurance industry

I. Introduction

The Berlin-based German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft e.V. - GDV) is the association of private insurers in Germany. It has more than 450 member companies. As risk takers, these offer coverage and assistance to private households, trade, industry and public institutions. The association deals with all technical issues concerning the insurance industry and works towards a regulatory framework that enables insurers to fulfil their tasks in optimal fashion.

The insurance industry has always heavily depended on using large amounts of personal data of insureds. These data are collected, processed and used to handle insurance applications, implement policies and process benefits, to provide advice and assistance to insureds and to assess the risk to be insured, to check the insurer's obligation to perform and to prevent insurance abuse in the interest of the community of insureds. Today, insurance undertakings are no longer capable to fulfil these tasks without the help of electronic data processing.

Ensuring informational self-determination and protection of privacy, as well as the security of data processing, are a main concern for the insurance industry in order to ensure the confidence of insureds. All provisions on the processing of data have to be in line with the provisions of the European General Data Protection Regulation (GDPR), the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) and with all sector-specific regulations on data protection; in addition to that, all insurance undertakings joining this code of conduct are obliged to undertake particular efforts in order to meet the principles of transparency, of necessity of the data processing operations and of data minimisation.

To this purpose, the German Insurance Association, in consultation with its member companies, has drawn up the following code of conduct for handling personal data of insureds. The code sets highly uniform standards for the insurance industry and promotes compliance with data protection regulations. The independent data protection authorities at both federal (*Bund)* and federal state (*Länder)* level take the view that undertakings complying with the sector-specific code of conduct thereby contribute to specifying the rules of the General Data Protection Regulation for the insurance industry. GDV member companies joining this code of conduct according to Article 30 undertake to comply with it.

The rules of the code of conduct aim to provide a guarantee to the insureds of undertakings having joined it that data protection and data security concerns are taken into account when designing and adapting products and services. GDV assures these undertakings of its support in this regard. Undertakings having joined this code of conduct shall instruct their executives and staff members to comply with it. Applicants and insureds shall be informed about the code of conduct.

Moreover, the code of conduct is intended to make any additional consent unnecessary, where possible. In principle, such additional consent will henceforth only be required for the

processing of particularly sensitive types of personal data – such as health data – and for the processing of personal data for purposes of advertising or market and opinion research. As regards the processing of particularly sensitive types of personal data – such as health data – GDV, in cooperation with the competent supervisory authorities, has prepared model declarations including explanations on their use. Undertakings having joined this code of conduct are called upon by the data protection authorities to use declarations of consent that correspond to the model clause.

The present code of conduct specifies and complements the data protection regulations applicable by insurance undertakings. As special rules for GDV member companies having joined this code of conduct, it covers the most important methods of processing personal data used by the undertakings in connection with the conclusion, performance, termination or acquisition of insurance contracts or to meet legal obligations.

The code of conduct needs to regulate the data processing of all undertakings having joined it. To this end, it has been formulated as generally as possible. As a consequence, it may be necessary for individual undertakings to specify the code of conduct by drawing up undertaking-specific provisions, which may not fall short of the data protection and data security level achieved by the code of conduct. Moreover, undertakings are free to stipulate specific rules that have added value in terms of data protection, e.g. for particularly sensitive data like health data or for the processing of data on the internet. Where the undertakings having joined this code of conduct have already stipulated such particularly data-protection-friendly rules or where special agreements or arrangements on particularly suitable procedures in terms of data protection have been made with the competent supervisory authorities, these shall of course remain in force after the undertaking concerned has joined this code of conduct.

Notwithstanding the rules stipulated in this code of conduct, the regulations of the GDPR and the German Federal Data Protection Act shall apply. The regulations on the rights and obligations of employees in the insurance industry shall remain unaffected.

II. Definitions

The definitions of the General Data Protection Regulation and the Federal Data Protection Act shall apply to the code of conduct.

In addition:

Undertakings:
shall mean GDV member companies, provided they carry out insurance business as primary insurers, as well as primary insurers affiliated to the latter within a group of insurance and financial services undertakings, including pension funds, which have joined this code of conduct,

Insurance relationship:

shall mean the insurance contract including the related pre-contractural measures and legal obligations,

Data subjects:

shall mean insureds, applicants or other persons whose personal data are processed in connection with the insurance business,

Insureds:

shall mean

- policyholders of the undertaking,
- insured persons including participants in group insurance,

Applicants:

shall mean persons having solicited an offer or filing an application for the conclusion of an insurance contract, irrespective of whether or not the insurance contract is actually concluded,

Other persons:

shall mean data subjects outside the insurance relationship, such as injured parties, witnesses or other persons whose data are processed by the undertaking in connection with the establishment, performance or termination of an insurance relationship,

Injured parties:

shall mean persons who have or might have suffered a damage, e.g. claimants in liability insurance,

Data processing:

shall mean the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination or restriction of the processing, erasure or destruction of personal data,

Data collection:

shall mean the procurement of data on data subjects,

Automated processing:

shall mean the collection, processing or use of personal data using data processing equipment,

Automated decision:

shall mean a decision taken on an individual person that is based exclusively on automated processing, without a natural person taking a decision based on a substantive assessment,

Master data:

shall mean general data of data subjects: name, address, date of birth, place of birth, customer number, occupation, civil status, legal representatives, information on the type of exist-

ing contracts (such as contract status, commencement and expiration dates, insurance number(s), type of payment, roles of the data subject (e.g. policyholder, insured person, contributor, claimant), as well as bank details, telecommunications data, authentification data for electronic or telephone communication, exclusions from advertising and other exclusions, consent to advertising and blocking for the purposes of market and opinion research, powers of attorney and custodianship arrangements, competent intermediaries and data similar to the aforementioned examples,

Service providers:

shall mean other undertakings or persons performing tasks on behalf of the undertaking on their own responsibility,

Processors:

shall mean natural or legal persons, agencies or other bodies processing personal data on behalf of the responsible undertaking,

Intermediaries:

shall mean individuals acting independently (sales representatives) and companies selling or concluding insurance contracts as insurance agents or brokers within the meaning of Sect. 59 of the German Insurance Contract Act (*Versicherungsvertragsgesetz - VVG*),

Legitimate interests:

shall mean the fundamental rights and freedoms of the data subject requiring the protection of personal data, especially if the data subject is a child.

III. GENERAL PROVISIONS

Art. 1 Scope

(1) [1]The code of conduct shall apply to the processing of personal data in connection with the insurance business carried out by the undertakings. [2]This shall include – in addition to the insurance relationship – in particular the fulfilment of legal claims, even where no insurance contract is concluded or where no insurance contract exists or no longer exists. [3]Insurance business also includes the design and calculation of rates and products.

(2) Notwithstanding the rules stipulated in this code of conduct, the legal provisions on data protection shall apply, especially the EU General Data Protection Regulation and the Federal Data Protection Act.

Art. 2 Purposes of the processing

(1) [1]As a matter of principle, the processing of personal data for the purpose of insurance business shall only take place where it is necessary for the establishment, performance or termination of an insurance relationship, in particular for handling an application, for assessing the risk to be insured, for fulfilling the advisory duties of the German Insurance Contract Act (VVG), for checking the insurer's obligation to perform or for internal controls of the timely settlement of receivables. [2]It shall also take place to assess and settle claims of injured parties in liability insurance, to assess and settle recourse

claims, to conclude and implement reinsurance policies, to develop rates, products and services, to draw up statistics, for insurance-related research, e.g. accident research, to combat abuse or to fulfil legal and supervisory obligations or for purposes of advertising or of market and opinion research.

(2) [1]As a matter of principle, personal data shall be processed within the scope of the purpose known to the data subjects. [2]Any alteration or extension of the purpose shall only take place if it is legally sound and if the data subjects have been informed about it in line with Article 7 or 8 of this code of conduct or if the data subjects have given their consent.

Art. 3 Principles regarding the quality of data processing

(1) The undertakings shall process all personal data in a lawful and transparent manner and in line with the legitimate interests of the data subject.

(2) [1]The processing of data shall be performed with an eye to data avoidance and data minimisation. [2]Subject to the research and statistical purposes under Art. 5 (1) (e) GDPR, personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. [3] In particular, the possibilities of anonymisation and pseudonymisation shall be used where possible and where the effort involved is not disproportionate with regard to the purpose of protection pursued. In this respect, anonymisation is to be preferred to pseudonymisation.

(3) [1]The undertaking shall ensure that existing personal data are stored accurately and kept up to date, where required. [2]All appropriate measures shall be taken to ensure that inaccurate or incomplete data are rectified, deleted or that their processing is restricted immediately.

(4) [1]The measures taken according to the preceding paragraphs shall be documented. [2]The undertakings shall include the underlying principles in their data protection concepts (Article 4 (2)).

Art. 4 Principles of data security

(1) [1]To ensure data security, the required technical and organisational measures, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing as well as the varying likelihood and severity of the risks caused by the processing for the rights and freedoms of natural persons, to ensure a level of security appropriate to the risk are taken by the undertakings. [2]In particular, the measures taken shall ensure that:

1. only authorised persons may gain knowledge of personal data (confidentiality). In particular, this shall be achieved through authorisation concepts, pseudonymisation or encryption of personal data.

2. personal data remain intact, complete and up to date during processing (integrity),

3. personal data are available in a timely manner and can be processed properly (availability, resilience),

4. personal data can be attributed to their source at any time (authenticity),

5. it can be ascertained who has entered, transferred and altered what personal data at what time and in which manner (capability of revision),

6. the procedures used in processing personal data have been documented completly and updated in such a way that they can be reconstructed within a reasonable amount of time (transparency).

(2) [1]The measures adopted by the undertakings shall be incorporated into a comprehensive data protection and data security concept, which regulates responsibilities and is developed in cooperation with the data protection officers of the undertakings. The concept shall include, in particular, a process for regularly testing and assessing the effectiveness of the adopted measures.

Art. 5 Consent

(1) [1]Where the processing of personal data is based on a declaration of consent and – where required – on a declaration on release from confidentiality by the data subjects, the undertaking shall ensure that these declarations have been freely given in an informed and unambiguous manner, that they are effective and have not been revoked. [2]Where special categories of personal data – e.g. health data – are processed, express consent of the data subject is required.

(2) [1]Where the processing of personal data of minors is based on consent and – where required – on a declaration on release from confidentiality, these declarations shall be obtained from the legal representative. [2]At the earliest, these declarations shall be obtained from the minor him- or herself after reaching the age of 16 years, provided he or she has the required capacity of discernment.

(3) [1]The undertaking or intermediary obtaining the consent shall ensure and document that the data subjects have been informed in advance about the controller(s), the extent, the form and the purpose of the data processing as well as about the possibility of refusing and revoking consent and the consequences thereof. [2]Art. 7 (3) of this code of conduct shall remain unaffected.

(4) [1]The consent and the release from confidentiality can be revoked at any time with future effect without giving reasons. [2]The data subjects shall be informed about the options and effects of revoking a declaration of consent. [3]Among other consequences, an effective revocation may particularly make it impossible to perform a particular service.

(5) Where the written or electronic consent is given together with other declarations, it shall be highlighted so that it catches the eye.

(6) [1]Consent can be declared in written or electronic form or orally. [2]The undertaking shall document the declaration of consent in a way that makes it possible to verify the individual declaration's content. [3]Upon request, the content of the declaration shall be provided to the data subjects.

(7) Where the consent is obtained orally, this shall be immediately confirmed to the data subjects in written form or in text form.

Art. 6 Processing of special categories of personal data

(1) [1]Special categories of personal data within the meaning of the EU General Data Protection Regulation (especially health data) shall be collected and processed based on legal provisions (in particular Art. 6 in conjunction with Art. 9 GDPR) or in line with Art. 5 based on the consent of the data subjects and – where required – based on a release from confidentiality. [2]The consent shall explicitly refer to these data.

(2) [1]The processing of special categories of personal data based on legal provisions shall be permitted, in particular where required for the establishment, exercise or defence of legal claims. [2]This applies e.g. to the assessment and settlement of the claims of insureds and of injured parties in liability insurance.

(3) In addition to that, the health data of data subjects can be processed without their consent in order to establish, exercise or defend legal recourse claims of the undertaking or of a third party that has provided a service to the data subjects, e.g. for the assessment and settlement of recourse claims of a social insurance agency, employer or private health insurer.

(4) The processing of special categories of personal data can also be permissible, within the limits of legal provisions, where it is necessary for the purposes of preventive medicine or health care.

(5) Moreover, health data can be processed without consent where it is necessary to protect the vital interests of the data subject or of another person if the data subject is physically or legally incapable of giving consent, especially where the person concerned has a right to assistance services (e.g. emergency call services, ambulance transport from abroad or coordination of medical treatment) and is incapable of giving consent in case of an insured event, e.g. because an accident has occurred and an unconscious person is in need of an ambulance transport.

(6) [1]Special categories of personal data are also processed, based on legal provisions, for statistical purposes and for research purposes according to Article 10 of this code of conduct.

IV. COLLECTION OF DATA

Art. 7 Principles on the collection of data and information to be provided where personal data are collected from the data subject

(1) [1]Personal data shall be collected in a transparent manner. [2]The obligations to cooperate applicable to insureds and applicants according to Sections 19, 31 German Insurance Contract Act (VVG) shall be taken into account.

(2) [1]Personal data of other persons within the meaning of this code of conduct shall be collected and processed where this is necessary to establish, exercise or defend legal

claims or to comply with a legal obligation. [2]In particular, this applies to situations where the data of witnesses or injured parties are collected to assess and provide liability insurance services, to situations where data are processed to settle direct claims in motor vehicle liability insurance or to comply with legal notification obligations. [3]Data mentioned in the first sentence may also be collected and processed where this is necessary for the establishment, performance or termination of an insurance relationship, provided there are no overriding legitimate interests of the persons concerned, e.g. where data in the possession of a lawyer or a repair workshop are needed to enable the necessary correspondence in case of an insured event.

(3) [1]To ensure transparency and protect the rights of the data subjects, the undertakings shall make sure that the data subjects are informed about the following:

a) the identity of the controller (name, location, contact details, authorised representatives),
b) the contact details of the data protection officer,
c) the purposes and legal basis (including the legitimate interests, if any) of the processing,
d) the recipients or categories of recipients of the personal data, where applicable,
e) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation under the terms referred to in Art. 13 (1) (f) GDPR,
f) the period for which the personal data will be stored (or the criteria used to determine that period),
g) the rights of data subjects stipulated under section VIII of this code of conduct, including the right to lodge a complaint with the competent supervisory authority and the right to object, if applicable,
h) where the processing is based on consent: about the right to withdraw consent and its consequences,
i) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and about the possible consequences of failure to provide such data,
j) in case of automated decision-making: meaningful information about the logic, significance and consequences of such processing.

[2]This information shall not be provided where and insofar as the data subject already has the information.

Art. 8 Data collection without participation of the data subjects

(1) [1]Data shall be collected without participation of the data subjects where this is necessary for the establishment, performance or termination of insurance relationships and particularly for the assessment and processing of benefit claims. [2]This is the case e.g. where the policyholder legitimately provides the data of the insureds in group insurance or the data of the beneficiaries in life and accident insurance or where he or she provides information on the injured party or witness in liabilitly insurance. [3]It is also possible to collect personal data without participation of the data subjects for the purposes of Art. 10 (1).

(2) [1]The collection of health or genetic data from third parties, if any, shall require an effective declaration on release from confidentiality by the data subjects and be in line with Section 213 German Insurance Contract Act (VVG) and Section 18 German Genetic Diagnosis Act (GenDG), provided these provisions apply. [2]The collection of special categories of personal data from third parties may also be necessary in the scenarios mentioned under Article 6 (2-5) of this code of conduct.

(3) [1]An undertaking that collects personal data without participation of the data subjects shall ensure that the data subjects are informed about the following withing a reasonable period after obtaining the personal data, but at the latest within one month:

a) the identity of the controller (name, location, contact details, authorised representatives),
b) the contact details of the data protection officer,
c) the purposes and legal basis (including the legitimate interests, if any) of the processing,
d) the categories of personal data concerned,
e) the recipients or categories of recipients of the personal data, where applicable;
f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation under the terms referred to in Art. 14 (1) (f) GDPR,
g) the period for which the personal data will be stored (or the criteria used to determine that period),
h) the rights of data subjects stipulated under section VIII of this code of conduct, including the right to lodge a complaint with the competent supervisory authority,
i) where the processing is based on consent: about the right to withdraw consent and its consequences,
j) from which source the personal data originate and whether they came from publicly available sources, and
k) in case of automated decision-making: meaningful information about the logic, significance and consequences of such processing.

[2]If the personal data are to be used for communication with the data subjects, the information shall be provided at the latest at the time of the first communication to that data subject, e.g. where beneficiaries of life insurance policies are designated they shall be informed upon occurrence of the insured event, and where beneficiaries are designated for cases of emergency, they shall be informed upon occurrence of said emergency. [3]If a disclosure to another recipient is envisaged, the information shall be provided at the latest when the personal data are first disclosed.

(4) [1]This information shall not be provided where and insofar as the data subject already has the information, the provision of such information proves impossible or would involve a disproportionate effort, in particular where data are processed for research or statistical purposes, or where data came from publicly accessible sources and providing the information would involve disproportionate efforts due to the high number of cases involved. [2]The information shall also not be provided where the data must be kept secret due to a legal provision or due to their nature, in particular due to the legitimate overriding interests of a third party. [3]This applies e.g. to life insurance, if a policyholder does not wish a beneficiary to be informed.

(5) [1]The information shall also not be provided according to Section 33 (1) (2) German Federal Data Protection Act in conjunction with Art. 23 (1) (j) GDPR, where:

- it would impair the establishment, exercise or defence of civil law claims or includes the processing of personal data from civil law contracts and helps preventing damages from criminal offences, provided the data subject has no overriding legitimate interest in receiving the information, or
- the disclosure of the information would interfere with the work of the prosecutorial authorities.

[2]As a general rule, no information shall therefore be provided on data collections aiming at the clarification of contradictions as set out under Art. 15 of this code of conduct.

(6) [1]In the cases set out under paragraph 5, the undertaking shall take appropriate measures to protect the legitimate interests of the data subjects (e.g. assessment and, where required, adoption of further access restrictions). [2]Where the undertaking refrains from providing information, it shall document its reasons.

V. PROCESSING OF PERSONAL DATA

Art. 9 Processing of master data within a group of undertakings

(1) Where the undertaking belongs to a group of insurance and financial services undertakings, the master data of applicants, insureds and other persons as well as details on the connection to other existing contracts may be processed for the centralised handling of certain procedural steps in the business process (e.g. telephone calls, mail, cash collection) using a joint data processing procedure accessible to members of the group, provided that the technical and organisational measures set out under Art. 4 of this code of conduct (e.g. authorisation concepts) meet the requirements under data protection law and that the controllers responsible for the procedure ensure that this code of conduct is complied with.

(2) Master data from jointly used data processing procedures shall only be further processed where this is necessary for the respective purpose. This shall be ensured at the technical and organisational level.

(3) [1]Where a joint processing of data takes place in accordance with paragraph 1, the insureds shall be informed of this in text form upon conclusion of the contract or upon the establishment of such a procedure. [2]To this end, the undertaking shall hold an up-to-

date list of all undertakings in the group participating in centralised processing and provide information on this list in an appropriate manner.

(4) Where an undertaking performs further data processing on behalf of another member of the group or where several members of the group process data together, Articles 21 to 22 (a) of this code of conduct shall apply.

Art. 10 Statistics, calculation of rates and premiums

(1) [1]The insurance industry develops its rates by calculating the probability of occurrence of insured events, including the related amount of loss, based on statistics and empirical values and by means of actuarial methods. [2]For this purpose, the undertakings evaluate data from insurance relationships, insured events and claims events as well as data provided by third parties, e.g. the "German Federal Motor Transport Authority" (Kraftfahrtbundesamt).

(2) [1]The undertakings shall take technical and organisational measures to ensure that the rights and freedoms of data subjects are protected according to the General Data Protection Regulation and that, in particular, the processing of personal data is limited to what is necessary for the relevant statistics. [2]These measures include anonymising and pseudonymising the data at an early stage, provided the statistical purpose can be achieved in this manner.

(3) [1]Any transfer of data to the German Insurance Association, the Association of Private Health Insurers (*Verband der privaten Krankenversicherung e. V.*) or other entities for the purpose of calculating intercompany statistics or risk classifications shall only take place in anonymised or – where required for the statistical purpose – pseudonymised form. [2]The aforementioned associations shall not be able to identify the data subjects concerned. [3]Paragraph 2 shall apply accordingly. [4]For the purpose of drawing up statistics in motor vehicle and property insurance, it shall also be possible to transfer data sets with information that can be used to identify individual persons, such as license plates and vehicle identification numbers or location data of risk objects, e.g. buildings.

(4) [1]Undertakings that process data for statistical purposes can also process special categories of personal data, especially health data, provided that this is required for the individual statistical purpose and that the undertaking's interest in processing the data significantly overrides the data subject's interest in preventing the processing. [2]This shall apply e.g. to statistics on the developement and review of rates or for purposes of statutory risk management. [3]In these cases, the undertakings shall take appropriate, specific measures to protect the interests of the data subjects and particularly the principles under Articles 3 and 4. [4]Due to the high need for protection of the data concerned, the specific measures include i. a.:

- sensitising the employees and services providers involved in the processings,
- pseudonomysing personal data according to paragraph 2 sentence 2,
- limiting the access to personal data for undertakings and service providers,
- using encryption when transferring personal data.

[5]All statistical data shall be anonymised as soon as possible considering the statistical purpose, provided that no legitimate interests of the data subjects prevent the anonymisation. [6]Until then, the identification features allowing to allocate individual details to

individual data subjects shall be stored separately. [7]The identification features shall only be merged with the individual details where it is required for statistical purposes.

(5) [1]The data subjects may object to the processing of their personal data for statistical purposes if their personal situation speaks against processing their data for this purpose. [2]The right to object shall not apply where the processing is required to fulfil a task which lies in the public interest, e.g. to reply to requests made by the German Federal Financial Supervisory Authority (BaFin).

(6) [1]To determine the risk-appropriate premium, rates as set out under paragraph 1 shall be applied to the individual situation of the applicant. [2]In addition, an assessment of the individual risk of the applicant, performed by specialised risk assessors such as physicians, may be included in the calculation of the premium. [3]For this purpose, personal data, including any special categories of personal data (such as health data), which have been processed according to this code of conduct, may also be used.

(7) The insurance industry shall also process personal data in accordance with the preceding paragraphs for the purpose of scientific research, e.g. accident research.

Art. 11 Scoring

Scoring shall be governed by the applicable legal provisions.

Art. 12 Data on creditworthiness

The collection, processing and use of data on creditworthiness shall be governed by the applicable legal regulations.

Art. 13 Automated individual decision-making

(1) [1]Automated decisions which produce legal effects on the data subjects or similarly significantly affect them shall only be taken under the conditions stated under paragraphs 2, 3 and 4.

(2) [1]Decisions which are necessary to enter into or perform an insurance contract with the data subject or which are necessary to provide benefits may be automised. [2]In particular, this shall apply in the following cases:

1. decisions regarding applicants on the conclusion and conditions of insurance contracts,

2. decisions regarding policyholders on claims events in insurance relationships,

3. decisions regarding the fulfilment of certain criteria in case of behaviour-linked rates, e.g. discounts for a safe driving style in motor vehicle insurance.

(3) [1]Automated decisions on benefit claims under an insurance contract, e.g. decisions with regard to co-insured persons or injured parties in liability insurance are also admissible where the data subject's request is met. [2]Decisions on the provision of insurance benefits may also be automated if they are based on binding fee terms for cura-

tive treatments and if the undertaking prepares for the event that the request is not fully met by implementing suitable measures to safeguard the data subject's legitimate interests, including at least the right to obtain human intervention on the part of the undertaking, to express his or her point of view and to contest the decision.

(4) In addition to that, automated decisions may be taken with the data subject's explicit consent.

(5) [1]Special categories of personal data shall be processed based on automated decision-making where the data subjects have given their consent. [2]In the scenarios described under paragraph 3, automated decisions on special categories of personal data shall not require consent.

(6) [1]Where automated decisions are taken to the detriment of the data subjects, at least the following measures shall be taken: The undertaking shall inform the data subjects about the fact that an automated decision has been taken. [2]In this process, they shall receive meaningful information on the underlying logic of the automated decision and on its scope and intended effects, provided they have not already received this information. [3]Upon request, the main reasons for the decision shall also be communicated and explained to the data subjects, to enable them to express their point of view, to obtain human intervention on the part of the undertaking and to contest the decision. [4]This shall also include the types of data used as well as their relevance for the automated decision. [5]The data subjects shall be entitled to contest the decision. [6] On this basis, the decision shall then be reviewed in a procedure that is not fully automated. [7] Article 28 (1) of this code of conduct shall apply accordingly.

(7) The use of automated decision-making shall be documented.

(8) [1]The undertakings shall ensure that technical and organisational measures are taken so that elements leading to incorrect personal data can be rectified and the risk of errors is minimised. [2]As regards health data, the legal provisions under Sections 37 (2) and 22 (2) German Federal Data Protection Act shall be taken into account.

Art. 14 Detection and Information System (*Hinweis- und Informationssystem - HIS*)

(1) [1]The undertakings of the German insurance industry – with the exception of private health insurers – use an information system (*Hinweis- und Informationssystem – HIS*) to support risk assessment in the case of an application, for establishing the facts in claims assessment and for combating insurance fraud. [2]The operation and use of HIS is based on the balancing of interests and fixed notification criteria.

(2) [1]HIS is operated separately for each insurance division. [2]In each division, the stored data are processed separately in two data pools: one pool for data retrieval for the purpose of risk assessment in the case of an application (*Antragsfall* = A pool), another pool for data retrieval for the purpose of claims assessment (*Leistungsprüfung* = L pool). [3]Accordingly, the undertakings shall organise access authorisations for their employees separated according to divisions and tasks.

(3) [1]The undertakings shall report data on persons, vehicles or real estate to the operator of HIS if there is an increased risk or if a conspicous fact has been discovered, provided this is necessary to reveal or prevent current or future insurance fraud and there are

no overriding legitimate rights and freedoms of the data subject preventing the reporting. [2]The consent of the data subjects is not required. [3]Prior to any reporting of data on persons, the interests of the undertaking shall be weighed against the interests of the data subject. [4]If the defined reporting criteria are met, it shall generally be assumed that the undertaking has a prevailing legitimate interest in the reporting. [5]The weighing of interests shall be documented in a sufficiently meaningful manner. [6]Special categories of personal data, such as health data, shall not be reported to the HIS. [7]Where an increased risk level is reported as an "obstacle" in personal insurance, no information shall be submitted on the underlying reasons, e.g. health data or a dangerous occupation or hobby. [8]Personal data on criminal convictions and offences shall also not be reported to the HIS, except where the processing is monitored by the authorities or where it is permitted under Union or national legislation, which provide for suitable safeguards for the rights and freedoms of the data subjects.

(4) [1]Upon conclusion of the contract, the undertakings shall provide their policyholders with general information about the HIS, indicating the controller and its contact details. [2]At the latest, they shall notify the data subjects about the relevant information under Art. 8 (3) at the time of reporting. [3]In the scenarios described under Art. 8 (5) of this code of conduct, notification is not required.

(5) [1]Data may be retrieved from the HIS upon filing of the application and in the event of a claim, but not when an endowment insurance policy is paid out in the event of survival. [2]The data retrieval shall not be the sole basis for a decision on an individual case. [3]The information shall only be considered as an indication of the fact that the case requires closer inspection. [4]Any data retrieval shall take place according to the automated retrieval procedure and shall be recorded both for the purpose of revision and for the purpose of being able to verify its justification by means of random checks.

(6) [1]Where required for the further establishment of facts in the event of a claim, data may also be exchanged between the reporting and the retrieving undertaking, provided there is no reason to assume that the data subject has a legitimate interest in preventing the transfer. [2]For instance, data and expert assessments on vehicle and building damages can be requested from the undertaking which had entered a claim into the HIS. [3]The exchange of data shall be documented. [4]Unless the data exchange takes place according to Article 15 of this code of conduct, the data subjects shall be informed about the data exchange. [5]No information shall be required if this would jeopardise the clarification of facts or if the data subjects have gained knowledge of the data exchange in a different manner.

(7) [1]Data recorded in the HIS shall be erased no later than at the end of the 4th year after the conditions for the reporting have been met. [2]The recording period shall be extended to a maximum of 10 years with regards to life insurance benefits or in the case of renewed reporting within the regular recording period according to Sentence 1. [3]Data on applications which have not led to the conclusion of a contract shall be erased from the HIS no later than at the end of the 3rd year following the year in which the application has been filed.

(8) The German Insurance Association will provide the undertakings with a detailed manual on the use of the HIS, with due regard to the requirements of data protection legislation.

Art. 15 Clarification of contradictions

(1) [1]Provided there are clear indications, the undertakings can assess at any time whether incorrect or incomplete information has been provided upon filing of the application or upon updating application data during the term of the insurance relationship and whether this has influenced the risk assessment or whether incorrect or incomplete information has been provided in the process of assessing a claim. [2]To this end, the undertakings shall collect and process data, provided this is necessary to clarify the existing contradictions. [3]The undertakings shall be given a certain margin of judgment for deciding which data they need to be able to take their decision based on an adequate factual basis.

(2) [1]In the event of a claim, the assessment according to paragraph 1 shall also be possible without the existence of indications. [2]This shall include the collection of preliminary information (e.g. periods of time in which treatments or examinations have taken place), enabling the undertaking to verify which information is actually relevant for the assessment, if any.

(3) [1]The statements used for risk assessment in the application process shall only be processed for verification purposes for a period of five years after conclusion of the contract, three years in case of health insurance. [2]The statements may be verified after this period has expired if an insured event has occurred before expiry of the period. [3]As regards the verification whether the policyholder has intentionally or maliciously provided inaccurate or incomplete details upon filing the application, this period shall be extended to 10 years.

(4) If the collection and processing of special categories of personal data, particularly of health data, is necessary according to paragraph 1, the data subjects shall be informed – in accordance with their statement in the insurance application – prior to any data collection according to Sect. 213 (2) German Insurance Contract Act and advised of their right to object or a separate declaration of consent and release from confidentiality shall be obtained from the data subjects in advance.

(5) [1]The right to refuse making a declaration of consent and release from confidentiality shall remain unaffected and the undertaking shall inform the data subject about this right. [2]If the data subject refuses to make a declaration of consent and release from confidentiality, he or she shall be required to procure all information necessary for settling the claim and pass it on to the undertaking. [3]The undertaking shall then declare which information it deems necessary in case of refusal to make the declaration of consent and release from confidentiality.

Art. 16 Exchange of data with other insurers

(1) [1]Data shall be exchanged between a previous insurer and its subsequent insurer for the purpose of collecting rate-relevant or benefit-relevant details, taking into account the provisions under Article 8 (1). [2]This is particularly the case where the information is necessary:

1. within the scope of risk assessment to review no-claims bonuses, particularly no-claims categories in motor third party liability and full comprehensive insurance,

2. for the transfer of pension rights in the case of change of provider or employer,

3. for the transfer of old-age provisions in health insurance to the new insurer,

4. for complementing or verifying details provided by applicants or insureds.

[3]In the cases described under points 1 and 4, the data exchange shall only be admissible for the purpose of risk assessment if the data subjects are informed about the possible data exchange and its purpose and subject matter in the application process upon collection of the data. [4]Following a data exchange for the purpose of benefits assessments, the data-collecting undertaking shall inform the data subjects about the data exchange to the same extent. [5]Article 15 of this code of conduct shall remain unaffected.

(2) An exchange of data with other insurers not covered by the rules stipulated for the Detection and Information System of the Insurance Industry (HIS) shall also take place where it is necessary for the assessment of applications and the assessment and provision of benefits, including the settlement of claims in case of joint, multiple or combined coverage of risks, of the legal subrogation of a claim against another person or for the settlement of claims between several insurers through existing knock-for-knock or waiver of recourse agreements and if there is no reason to assume that overriding legitimate interests of the data subject prevent this exchange of data.

(3) The exchange of data shall be documented.

(4) [1]Motor vehicle insurers use a damage class file (Schadenklassendatei), provided by the GDV Dienstleistungs-GmbH as a shared institution to prevent insurance fraud. [2]Reporting of information shall take place to enable a correct classification in the system of no-claims bonuses. [3]This is necessary e.g. where a motor vehicle liability insurance contract has been terminated, no information on this prior insurance is presented upon conclusion of the contract and it would therefore violate the applicable system of rates to carry out a reclassification in the no-claims categories as if no prior insurance had existed. [4]The motor vehicle insurer shall report the name and address of the policyholder, the policy number, the registration number of the previously insured vehicle, the termination date of the insurance contract including the relevant no-claims category as well as the number of claims not yet registered in the year of reporting. [5]The data shall only be retrieved in case of an application where the policyholder does not request the no-claims bonus from his or her previous insurance contract to be applied to the new contract. [6]Upon conclusion of the contract, the motor vehicle insurers shall inform the policyholders in the insurance information about the damage class file and the contact details of the shared institution. [7]Where data are reported upon termination of the insurance contract, the motor vehicle insurers shall inform the policyholders about the type of reported data, the purpose of the reporting, the recipient of the data (name and location of the shared institution) and the possible retrieval of the data. [8]Data retrievals from the damage class file shall follow an automated procedure. [9]They shall be recorded for the purpose of revisions and randomised authorisation checks. [10]At the latest, the data recorded in the damage class file shall be deleted at the end of the third year after the conditions for the reporting have been met.

Art. 17 Data transfer to reinsurers

(1) [1]To be able to meet their obligations from insurance relationships at any time, undertakings cede a part of their risks from insurance contracts to reinsurers. [2]For the purpose of further risk spreading, some of these reinsurers resort to further reinsurers. [3]For the purpose of the proper establishment, performance or termination of the reinsurance contract, data from the insurance application or relationship, in particular the insurance policy number, the premium, the type and level of insurance cover and of the risk as well as any risk premiums, shall be disclosed in anonymised or – where this is insufficient for the aforementioned purposes – pseudonymised form.

(2) [1]Reinsurers shall only receive personal data where this is necessary:

a) for the conclusion or performance of the insurance contract, or
b) to ensure that the undertaking is capable of meeting its obligations arising from the insurance relationships and where there is no reason to assume that a legitimate interest of the data subject overrides the interests of the undertaking.

[2]This may be the case where the transfer of personal data to reinsurers within the scope of the concrete reinsurance relationship takes place for the following reasons:

a) Risk and claims assessment are carried out by reinsurers in individual cases, e.g. in the case of high sums insured or where a risk is difficult to classify.
b) Reinsurers assist undertakings in risk and claims assessment and in evaluating procedures.
c) Reinsurers are provided with lists of the portfolio of contracts covered by reinsurance to determine the scope of reinsurance contracts, which includes verifying if and to what extent they are affected by the same risk (accumulation control), and for clearing purposes.
d) Risk and claims assessments carried out by the primary insurer are verified by reinsurers by means of random checks or individual checks, in order to assess their payment obligations to the primary insurer.

(3) [1]The undertakings shall agree with the reinsurers that the latter may only use personal data for the purposes stated in paragraph 2 or for other purposes compatible with these purposes (e.g. statistics and scientific research). [2]In addition to that, they shall agree whether the reinsurer will provide the data subject with legally required information itself or whether the undertaking will forward the information provided by the reinsurer to the data subject. [3]Should they agree for the information to be forwarded, they shall also agree how this will be done. [4]Where undertakings are subject to an obligation of secrecy according to Sect. 203 of the German Criminal Code (*Strafgesetzbuch – StGB*), they shall require reinsurers to maintain silence with respect to data received according to paragraph 2 and to require other reinsurers and parties acting on their behalf to also maintain silence with respect to such data.

(4) Special categories of personal data, especially health data, shall only be transferred to reinsurers if the conditions under Article 6 of this code of conduct have been met.

VI. PROCESSING OF PERSONAL DATA FOR PURPOSES OF DISTRIBUTION AND OF MARKET AND OPINION RESEARCH

Art. 18 Use of data for advertising purposes

(1) For advertising purposes, personal data shall only be processed based on Art. 6 (1) (a) or (f) General Data Protection Regulation and subject to Section 7 of the German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb - UWG*)

(2) [1]Data subjects may object to the use of their personal data for purposes of direct advertising. [2]In this case, their personal data shall no longer be used for these purposes. [3]The undertaking shall take suitable technical and organisational measures to implement this provision.

Art. 19 Market surveys

(1) Undertakings conducting market surveys shall proceed with special regard to the legitimate interests of the data subjects concerned.

(2) [1]Where the undertakings entrust other parties with market and opinion surveys, they shall be able to prove that the selection process for said parties has been performed in compliance with the applicable provisions on data protection. [2]Prior to the transfer of data, the details of the research project shall be stipulated by contract, in accordance with the requirements under Article 21, 22 or 22 (a) of this code of conduct. [3]It shall be laid down, in particular:

a) that the data transferred and collected additionally shall be pseudonomyised at the earliest possible date and anonymised as early as possible considering the purpose of the survey,
b) that the evaluation of the data and the transfer of the results of market and opinion surveys to the undertakings shall take place as anonymised and pseudonymised as possible, where required for the underlying purposes (e.g. follow-up surveys).

(3) [1]Where the undertakings process or use personal data for the purpose of market and opinion surveys themselves, such data shall be pseudonymised at the earliest possible date and anonymised as early as possible considering the purpose of the survey. [2]The results shall only be recorded and used in a form that is as anonymised and pseudonymised as possible, where required for the underlying purposes (e.g. follow-up surveys).

(4) Where commercial activities to be considered as advertising take place within the scope of market and opinion surveys, e.g. where statements are made in the process of data collection that aim at the promotion of sales, the processing of the respective personal data shall be subject to the rules stipulated in Article 18 of this code of conduct.

Art. 20 Transfer of data to self-employed intermediaries

(1) [1]Any transfer of personal data to the intermediary serving the customer shall take place only where it is necessary for the adequate preparation or handling of a concrete appli-

cation or contract or for the purpose of proper handling of the insurance matters of the data subject. [2]Intermediaries shall be advised of their specific obligations of secrecy.

(2) [1]Prior to the first transfer of personal data to an insurance agent or in the case of a switch from the insurance agent serving the customer to another insurance agent and subject to the rule stipulated in paragraph 3, the undertaking shall inform the insureds or applicants as soon as possible, but at the latest two weeks before the transfer of their personal data about the forthcoming transfer of data, the identity (name, location) of the new insurance agent and their right to object. [2]There is no notification required where the changing of insurance agents has been requested by the data subject. [3]Information provided by the previous insurance agent shall be considered equivalent to information provided by the undertaking. [4]In principle, there shall be no transfer of data in case of an objection. [5]In this case, the customer shall be offered to be served by another insurance agent or the undertaking itself.

(3) There shall be an exception to paragraph 2 where the proper service to insureds in individual cases or – due to an unexpected discontinuation of the service – the continuation of contractual relationships is at risk.

(4) [1]Personal data of insureds or applicants may be transferred to an insurance broker or a service association of insurance brokers if the insureds or applicants have conferred power of attorney or a similar authorisation covering the transfer of data to the broker. [2]In case of a change of brokers, paragraph 2 shall apply accordingly.

(5) [1]As a matter of principle, there shall be no transfer of health data by the undertaking to the intermediary serving the customer, unless the data subjects have given their consent. [2]This shall be without prejudice to any legal authority for the transfer of data.

VII. DATA PROCESSING BY PROCESSORS, SERVICE PROVIDERS AND JOINT CONTROLLERS

Art. 21 Obligations with respect to processing on behalf

(1) [1]Where an undertaking has personal data processed on its behalf in accordance with Article 28 General Data Protection Regulation (e.g. electronic data processing, scanning and assigning of incoming mail, address administration, handling of applications and contracts, claims and benefits handling, ensuring the correct booking of incoming payments, outgoing payments, disposal of documents), the processor shall at least have to comply with Article 28 (3) General Data Protection Regulation. [2]Only processors shall be selected who provide sufficient guarantees that they will implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the General Data Protection Regulation and ensure the protection of the rights of the data subject. [3]The undertaking shall require any necessary information demonstrating that the contractor has taken adequate technical and organisational measures and complies with them, e.g. suitable certificates. The results shall be documented.

(2) [1]Any data processing by the processor shall only take place for the purposes and within the scope of the instructions issued by the undertaking. [2]Contractual terms should be submitted to the data protection officers, who shall provide advice, where required.

(3) [1]The undertaking shall keep an up-to-date list of processors available. [2]Where the automated processing of personal data is not the main subject of the processing on behalf or where many different processors (e.g. services proviers offering document destruction services at several sites of the undertaking) are entrusted with similar tasks, the processors may – notwithstanding internal documentation requirements – be grouped into categories, specifying their task. [3]This shall also apply to processors providing their services only occasionally. [4]The list shall be published in an appropriate form. [5]Where personal data are collected from the data subjects, these shall, as a matter of principle, be informed about the list upon collection.

(4) Contracts or other legal instruments within the meaning of Art. 28 (3) and (4) General Data Protection Regulation for the purpose of processing on behalf shall be put down in writing. This may include electronic formats.

Art. 22 Data processing by a service provider without processing on behalf

(1) [1]Where required for the purpose of the insurance relationship with the data subjects, personal data can be transferred to service providers without processing on behalf and be processed by them at their responsibility. [2]That is the case, in particular, where experts are entrusted with the assessment of an insurance claim or where service providers are entrusted with the provision of contractually agreed insurance services comprising a benefit in kind, e.g. ambulance services, domestic help services, key services and other service providers.

(2) [1]Personal data may also be transferred to service providers for the accomplishment of data processing and other tasks on the service provider's own responsibility if it is necessary to protect the legitimate interests of the undertaking, provided there are no overriding legitimate interests of the data subject. [2]This may, for instance, be the case where service providers undertake tasks supporting the business processing of the undertaking, such as risk assessment, claims and benefits handling and cash collection, provided this is no data processing on behalf and the prerequisites under paragraphs 4 to 8 are met.

(3) [1]The transfer of personal data to service providers in accordance with paragraph 2 shall be refrained from where the data subject objects to it on grounds relating to his or her particular situation and where it results from a check that the undertaking has no compelling legitimate reasons to have the data processed by a service provider that override the interests of the data subject. [2]The transfer to the service provider shall take place despite the objection where it serves the establishment, exercise or defence of legal claims. [3]The data subjects shall be advised of their right to object in an appropriate manner.

(4) The undertaking shall enter into a contractual agreement with service providers taking action in accordance with paragraph 2, which shall include at least the following points:

- clear description of the tasks of the service provider,

- ensuring that the data transferred are processed or used only within the scope of the agreed purpose,
- ensuring data protection and data security standards complying with this code of conduct,
- committing the service provider to provide the undertaking with any information it needs to comply with its remaining information requirements, or to inform the data subject directly.

(5) The outsourcing of tasks according to paragraph 2 shall be documented.

(6) [1]In the cases described under paragraph 2, the undertaking and the service provider shall also agree that data subjects having suffered damage due to the transfer of their data to the service provider or due to the processing of their data by that service provider shall be entitled to claim damages from both parties. [2]The undertaking shall be held liable in the first instance for the damage suffered by the data subjects. [3]The parties agree that they shall be jointly and severally liable and that they can be released from liability only if they prove that neither party is responsible for the damage suffered.

(7) [1]The undertaking shall keep available an up-to-date list of service providers within the meaning of paragraph 2, to which tasks are mainly delegated. [2]Where the automated processing of personal data is not the main subject of the contract, service providers may be grouped into categories, specifying their task. [3]This shall also apply to entities providing their service only once. [4]The list shall be published in an appropriate form. [5]Where personal data are collected from the data subjects, these shall, as a matter of principle, be informed about the list upon collection.

(8) The undertaking shall ensure that the rights of the data subjects according to Articles 23 to 24 (c) are not curtailed due to the involvement of the service provider according to paragraph 2.

(9) The transfer of personal data to lawyers, tax advisors and auditors, within the scope of the fulfilment of their tasks, shall remain unaffected by the aforementioned provisions.

(10) [1]Special categories of personal data may only be processed in this context if the data subjects have given their consent or if there is a legal basis to do so. [2]Where the undertakings are subject to an obligation of secrecy according to Sect. 203 German Criminal Code (StGB), they shall require service providers to maintain secrecy with respect to data received according to paragraphs 1 and 2 and to require other service providers as well as entities acting on their behalf to maintain secrecy as well.

Art. 22a Joint controllers

(1) Groups of insurance undertakings and financial service providers may establish joint data processing procedures in accordance with Article 26 General Data Protection Regulation for their common business purposes.

(2) [1]In case of joint data processing procedures involving two or more controllers, the undertakings shall determine their respective responsibilities under the General Data Protection Regulation in a transparent contractual arrangement, in particular regarding their respective duties to comply with the rights of the data subjects. [2]They shall also agree on the respective duties to inform the data subjects.

(3) The undertaking shall maintain an up-to-date list of the joint data processing procedures including the responsible undertakings and inform the data subjects about this list in an appropriate manner.

(4) Data subjects may exercise their rights under data protection legislation against each of the controllers.

VIII. RIGHTS OF DATA SUBJECTS

Art. 23 Right of access

(1) Data subjects shall have the right to obtain confirmation as to whether or not personal data concerning them are being processed, and where that is the case, they shall have a right of access to the data stored by the undertaking.

(2) Where the undertaking processes a large quantity of information concerning the data subject or in case of unspecific information requests regarding personal data, the undertaking shall at first provide information on the master data it has stored regarding the data subject as well as summarising information on the processing and ask the data subject to specify the information or processing steps he or she wishes to receive information on.

(3) [1]The data subject shall be informed according to his or her request. [2]The information shall be provided in a manner that allows the data subject to understand the type and scope of processing and assess its lawfulness. [3]It shall be ensured that the data subject is provided with all legally required information. [4]In case of a (planned) disclosure of the data, the data subject shall also be informed about the recipients or categories of recipients to whom the personal data have been or will be disclosed.

(4) [1]It shall be ensured that only the authorised person receives the information. [2]For this reason, the information shall only be submitted to the data subject or his or her legal representative, even if it is requested by an authorised representative.

(5) [1]The information shall be provided in written or other form, in particular in electronic form, e.g. via a customer portal. In case of an electronic request, the information shall be provided in a commonly used electronic format. [2]This shall not be done where something else has been requested or where the authenticity of the recipient or the safe transmission of the information cannot be guaranteed. [3]Upon request of the data subjects, the information may also be provided orally, provided that the identity of the data subjects has been proven.

(6) The information may not adversely affect the rights and freedoms of other persons. Trade secrets of the undertaking may be taken into account.

(7) [1]This information may be omitted where the data must be kept secret according to a legal provision or by virtue of their nature, particularly because of the overriding legal interest of a third party, or where the disclosure of the information would jeopardise criminal prosecution. [2]In addition to that, no information shall be provided on data that have only been recorded because they may not be erased due to legal or statutory retention periods or on data serving the sole purpose of safeguarding data or monitoring data protection, if the provision of information would require disproportionate efforts and the processing for other purposes based on appropriate technical and organisa-

tional measures is impossible. [3]Examples include restrictions on data processing due to retention requirements and access-protected backups.

(8) [1]In the scenarios described under paragraph 7, the reasons for denying the right of access shall be documented. [2]The data subject shall be informed about the reasons to deny the right of access. [3]There shall be no such explanation insofar as communicating the real or legal reasons for denying the right of access would jeopardise the underlying reasons of the denial, in particular where communicating the reasons would adversely affect the overriding legitimate interests of third parties or criminal prosecution.

(9) In the case of reinsurance (Article 17), data processing by service providers without processing on behalf (Article 22) or processing by joint controllers (Article 22 (a)), the undertaking shall receive the requests for information and shall also provide any information the reinsurer, service provider or any controller are required to provide or it shall ensure that they provide the information.

Art. 23a Right to data portability

(1) The data subject shall receive the personal data which he or she has provided from the undertaking where the processing of the data is based on the data subject's consent or on a contract concluded with him or her and if the processing is carried out by automated means.

(2) [1]This right shall include the data communicated or provided by the data subject to the undertaking. [2]In particular, this shall include the data indicated by the data subject in applications, such as name and address and the requested data regarding the insured risk as well as any further personal data indicated during the insurance relationship, such as data provided in claims reports.

(3) The data subject shall receive the data in a structured, commonly used and machine-readable format.

(4) The data subject shall also have the right to have the personal data transferred directly from the undertaking to another controller, where technically feasible and provided that the security requirements regarding the transfer can be met.

(5) The data shall not be transmitted directly to another controller where this would adversely affect the rights and freedoms of others.

Art. 24 Right to rectification

Where the stored personal data prove to be inaccurate or incomplete, they shall be rectified.

Art. 24a Right to restriction of processing

(1) Upon request from the data subjects, the undertaking shall restrict the processing of their data:

a) as long as the accuracy of contested data is being assessed,
b) where the processing is unlawful and the data subjects require the further retention of the data,

c) where the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subjects for the establishment, exercise or defence of legal claims, or
d) where the data subjects have objected to processing pending the verification whether the legitimate grounds of the undertaking override those of the data subjects.

(2) Where the data subjects have made use of their right to restriction of processing, their data shall only be processed:

a) with the data subjects‘ consent,
b) for the establishment, exercise or defence of legal claims,
c) for the protection of the rights of another natural or legal person, or
d) for reasons of important public interest of the European Union or of a Member State.

(3) Data subjects who have obtained restriction of processing shall be informed by the undertaking before the restriction of processing is lifted.

Art. 24b Erasure

(1) [1]Personal data shall be erased without undue delay if the collection or processing has been inadmissible from the start, if the processing proves to be inadmissible due to circumstances having occurred subsequently or if knowledge of the data is no longer necessary for the undertaking to fulfil the purpose of the processing. [2]The data shall also be erased where necessary for compliance with a legal obligation or where they have been collected in relation to the offer of information society services to a child referred to in Article 8 (1) General Data Protection Regulation.

(2) [1]The checking of the stored data with regard to the necessity of erasure according to paragraph 1 shall take place at regular intervals, at least once a year. [2]Upon request of the data subject, it shall be verified without undue delay whether the data concerned by the request are to be erased.

(3) [1]There shall be no erasure pursuant to paragraph 2 where the data are necessary:

a) for compliance with a legal obligation of the undertaking, in particular for compliance with legal storage obligations,
b) for the statistical purposes in accordance with Article 10,
c) for archiving purposes in the public interest, scientific or historical research purposes (e.g. to come to terms with the Holocaust), or
d) for the establishment, exercise or defence of legal claims.

[2]The data shall also not be erased where their processing is not carried out by automated means, where erasure is not possible or is only possible with disproportionate effort due to the specific type of storage and where the interest of the data subjects in having them erased can be considered as negligible. [3]In this case or where personal data only have to be stored to comply with statutory storage obligations, their processing shall be restricted according to the principle of data minimisation.

Art. 24c Notifications regarding rectification, restriction of processing and erasure

(1) [1]The controller shall communicate any rectification, restriction of processing or erasure of data required due to a request of the data subject to each recipient, in particular to reinsurers and insurance agents, unless this proves impossible or involves disproportionate effort. [2]This shall also apply e.g. where the recipient must already have erased the data due to contractual arrangements. [3]Upon request, the undertaking shall inform the data subjects about these recipients.

(2) Where the rectification, erasure or restriction of data has taken place upon request by the data subjects, these shall be informed of it following execution.

(3) Other notification requirements regarding rectifications or erasures of personal data as well as restrictions of processing without request of the data subject shall remain unaffected.

Art. 24d Period

[1]The undertaking shall comply with the rights under Articles 23 to 24 (b) of this code of conduct without undue delay and in any event within one month of receipt of the data subject's request to exercise the corresponding right. [2]That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. [3]In this case, the undertaking shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

IX. COMPLIANCE AND CONTROL

Art. 25 Responsibility

(1) The undertakings, as controllers, shall ensure that the requirements of data protection and data security are complied with.

(2) [1]Employees entrusted with the processing of personal data shall be required to maintain confidentiality with regards to personal data, to comply with data protection requirements and the corresponding instructions given by the undertaking and to respect legal obligations of secrecy. [2]They shall be informed that any infringement of data protection regulations may also be punished as a regulatory offence or be prosecuted and may entail claims for damages. [3]Any violations of data protection regulations by employees may entail sanctions under labour law in accordance with applicable legislation.

(3) The obligations of employees under paragraph 2 sentence 1 shall continue to apply after the employment relationship has ended.

Art. 26 Transparency

(1) [1]Texts addressed at data subjects shall be informative, transparent, easy to understand and concise and formulated in clear and plain language.[2]They shall be provided to the data subjects in an easily accessible form.

(2) [1]The undertakings shall maintain a record of processing activities (processing record). [2]Upon request, they shall provide data protection authorities with this record. [3]In addi-

tion to that, the undertakings shall use their processing records internally as a basis to fulfil their information and disclosure obligations towards data subjects.

Art. 26a Data protection impact assessment

(1) The undertakings shall assess the necessity of performing a data protection impact assessment, in particular before using the following types of processings for the first time or on a much larger scale:

a) procedures using automated individual decisions, which are based on systematic and extensive evaluation of several personal aspects of data subjects, provided they have legal effects on the data subjects or similarly significantly affect them, e.g. procedures for automated risk and claims or benefits assessments,
b) processing of special categories of personal data on a large scale, e.g. procedures for claims or benefits assessments in health insurance, for risk assessments in life insurance or for benefits assessments in disability insurance, or
c) procedures for the calculation of premiums using behaviour-based data of data subjects (e.g. for so-called telematics rates in motor vehicle insurance or using data from wearables).

(2) [1]The decision on whether or not a data protection impact assessment should be carried out and the underlying reasons for this decision shall be documented. [2]The undertakings shall take appropriate organisational measures to ensure that the data protection impact assessment is carried out under consultation with the data protection officer.

Art. 27 Data protection officers

(1) [1]The undertakings or a group of insurance and financial services undertakings shall designate data protection officers according to the applicable legal requirements. [2]The data protection officers shall be independent and monitor compliance with the applicable national and international data protection provisions and with this code of conduct. [3]The undertaking shall contractually ensure the data protection officer's independence.

(2) The data protection officers shall monitor compliance with the General Data Protection Regulation and other data protection provisions, including the undertaking's strategies for the protection of personal data. For this purpose, they shall be informed in due time before the establishment of or significant changes to procedures for the automated processing of personal data and shall participate in an advisory capacity.

(3) [1]To this effect, they may prompt all divisions of the undertaking to take the necessary data protection measures, in coordination with the management of the undertaking concerned. [2]In this respect, they shall have an unrestricted right of control within the undertaking.

(4) The data protection officers shall inform and advise the undertakings and employees engaged in the processing of personal data regarding the respective special requirements in terms of data protection.

(5) [1]In addition, all data subjects may approach the data protection officers at any time with suggestions, enquiries, requests for information or complaints related to issues of data protection or data security. [2]Enquiries, requests and complaints shall be treated as confidential. [3]The data required for contacting shall be made known in an appropriate form.

(6) The executive boards of the undertakings responsible for data protection shall support the data protection officers in exercising their tasks and trustfully cooperate with them to ensure compliance with applicable national and international data protection regulations and this code of conduct.

(7) The undertakings shall provide the data protection officers with the resources necessary to carry out their tasks and to maintain their expert knowledge.

(8) [1]The data protection officers shall cooperate with the data protection supervisory authority responsible for the undertaking. [2]To this end, they may trustfully consult with the respective responsible data protection authority at any time and shall serve as a point of contact to the supervisory authority in all matters of data protection.

Art. 28 Complaints and reaction to infringements

(1) [1]The undertakings shall process complaints made by insureds or other data subjects because of infringements of data protection regulations and this code of conduct in a timely manner and reply to them within one month or send an interim notice. [2]The report on the measures taken may also be completed until up to three months after the filing of the application, provided that the extension of deadline is required due to the complexity and number of applications. [3]The necessary details to contact the undertaking shall be communicated in an appropriate form. [4]If the responsible division is unable to take remedial action in a timely manner, it shall approach the data protection officer without delay.

(2) In case of justified complaints, the executive boards of the undertakings shall take remedial action as soon as possible.

(3) [1]Should this not be the case, the data protection officers may approach the responsible data protection authority. [2]They shall notify the data subjects of this under specification of the competent supervisory authority.

Art. 29 Notification of a personal data breach

(1) [1]In the case of a personal data breach, e.g. where personal data have been unlawfully transferred or unlawfully revealed to third parties, the undertakings shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subjects. [2]The rights and freedoms of data subjects are particularly at risk where the breach may give rise to identity theft, financial loss or damage to the reputation.

(2) [1]The undertaking shall document personal data breaches, comprising any facts relating to the personal data breach, its effects and the remedial action taken. [2]The documentation shall enable the supervisory authority to verify compliance with this Article.

(3) [1]The data subjects shall be notified if the personal data breach is likely to result in a high risk to their personal rights and freedoms. [2]The notification shall take place without undue delay. [3]Taking into account the current risk situation, it shall be decided whether measures to safeguard the data or measures to prevent future breaches are

taken first. [4]Where a notification would require disproportionate efforts, e.g. due to the multitude of cases concerned or where it is not possible to identify the data subjects within a reasonable period of time or with reasonable technical effort, it shall be substituted by public information.

(4) [1]The data subjects shall not be notified if the controller has taken technical and organisational measures which ensure that the high risk to the rights and freedoms of the data subjects is not or no longer likely to materialise. [2]The data subjects shall also not be notified if the notification would require the disclosure of information which has to be kept secret according to a legal provision or by virtue of its nature, in particular because of the overriding legitimate interests of a third party, unless such secrecy interests are overridden by the data subjects' interests in the notification, in particular with regards to pending losses.

(5) The notification to the data subject shall describe in clear and plain language the nature of the personal data breach and include at least:

a) the name and contact details of the data protection officer or other contact point where more information can be obtained,
b) a notification of the likely consequences of the personal data breach,
c) a description of the measures taken or proposed to be taken by the undertaking to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(6) The undertakings shall oblige their processors to inform them about incidents according to paragraph 1 without undue delay.

(7) [1]The undertakings shall create a concept for handling personal data breaches. [2]They shall ensure that the data protection officers of the undertaking are informed of any breaches. [3]The data protection officers shall directly report to the undertaking's highest management level.

X. FORMALITIES

Art. 30 Accession

(1) [1]The undertakings having joined this code of conduct commit themselves to comply with it as from the date of accession. [2]The accession of the undertakings will be documented by GDV and made known in an appropriate form.

(2) Policyholders whose contracts have been concluded prior to the accession of the undertaking to this code of conduct shall be informed about the undertaking's accession to this code of conduct through the undertaking's website and no later than with the next contractual information in text form.

(3) [1]Undertakings having joined this code of conduct shall comply with its currently valid version. [2]The undertakings can withdraw their accession at any time by declaration to GDV. [3]Where an undertaking declares its withdrawal from accession, GDV will document this decision by deleting the respective undertaking from its list of accessions and make it known in appropriate manner by publishing an updated list of accessions. [4]In

addition, the undertaking shall inform the responsible data protection authority and the insureds about its decision to withdraw from the code of conduct.

Art. 31 Evaluation

Any legislative changes to this code of conduct shall require an evaluation of this code of conduct regarding these changes. In addition to that, the code of conduct shall be evaluated as a whole no later than three years after the entry into force of the General Data Protection Regulation.

Art. 32 Entry into force

This version of the code of conduct shall enter into force as of 1 August 2018 and shall replace its previous version of 7 September 2012.