ERGO

Version / Last revised: 29/06/2018

Code of Conduct

for handling personal data

within the German insurance industry

I. Introduction

The Association of German Insurers (GDV), headquartered in Berlin, is the umbrella organization for private insurers in Germany. It has more than 450 member companies. As risk carriers, they offer risk protection and support for private households as well as for industry, trade and public institutions. The Association is involved in all technical issues relating to the insurance industry and the regulatory framework that enable insurers to fulfil their tasks in the best possible way.

The insurance industry has always been dependent on the use of personal data of policyholders on a large scale. Data is collected, processed and used to process applications, contracts and benefits, to advise and support insured persons, to assess the risk to be insured, to check the obligation to pay benefits and to prevent insurance abuse in the interest of the insured community. Today, insurance companies can only fulfil their tasks with the help of electronic data processing.

Safeguarding information self-determination and the protection of privacy as well as the security of data processing are core concerns for the insurance industry in order to guarantee the confidence of the insured. All rule for processing personal data must not only comply with the provisions of the European General Data Regulation (GDPR), the Federal Data Protection Act and all relevant sector-specific regulations on data protection, but the companies that have joined the insurance industry also undertake to comply with the principles of transparency, the necessity of the data processed and data minimisation in particular.

In consultation with its member companies, the GDV has drawn up the following Code of Conduct for handling the personal data of insured persons. They create largely uniform standards for the insurance industry and promote compliance with data protection regulations. In the opinion of the independent data protection authorities of the Federal Government and the *Länder*, companies that apply the industry-specific Code of Conduct thus ensure that the provisions of the General Data Protection Regulation are specified in a sector-specific manner for the insurance industry. The member companies of the GDV, which have adopted this Code of Conduct in accordance with Article 30, thus undertake to comply with its provisions.

The Code of Conduct are intended to guarantee policyholders from adopting companies that data protection and data security concerns will be taken into account in the design and processing of products and services. The GDV assures its support in this matter. The adopting companies will instruct their managers and employees to comply with the Code of Conduct. Applicants and insured persons will be informed about the Code of Conduct.

In addition, the Code of Conduct is intended to make additional consents as dispensable as possible. In principle, it is only 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. For the processing of particularly sensitive types of personal data - such as health data - the GDV has drawn up sample declarations together with the responsible supervisory authorities with information on their use. The adopting companies are requested by the data protection authorities to use consent texts that comply with the model clause adapted to their respective business processes.

This Code of Conduct specifies and supplements the data protection regulations for the insurance industry. As special rules for member companies that have joined the GDV, it summarizes the most significant processing of personal data that the companies carry out in connection with the establishment, performance, termination or acquisition of insurance contracts as well as for the fulfilment of legal obligations.

The Code of Conduct is formulated as universally as possible given that it must be suitable for regulating the data processing of all member companies. Therefore, it may be necessary for individual companies to adapt the rules specifically in their own internal rules. However, any such rules may not fall below the level of data protection and data security provided for in the Code of Conduct. Furthermore, companies are free to make individual rules with added value in terms of data protection, e.g. for particularly sensitive data such as health data or for the processing of data on the Internet. If the adopting companies have already adopted such particularly data protection-friendly guidelines or if there are special agreements or arrangements with the responsible supervisory authorities on particularly data protection-compliant procedures, these naturally remain valid even after adopting this Code of Conduct.

The regulations set out in the GDPR and the Federal Data Protection Act apply irrespective of the rules set out here. These rules are without prejudice to the provisions on the rights and obligations of employees in the insurance industry.

II. Definitions

The definitional provisions of the General Data Protection Regulation and the Federal Data Protection Act apply to this Code of Conduct.

In addition:

Companies:

The member companies of the GDV, insofar as they conduct insurance business as primary insurers and primary insurance companies affiliated with them in a group of insurance and financial services companies, including pension funds, which have adopted this Code of Conduct;

Insurance relationship:

Insurance contract including the related pre-contractual activities and legal obligations;

Data subjects:

Insured persons, applicants or other persons whose personal data is processed in connection with the insurance business;

Insured persons:

- Policyholders at a company;
- Insured persons including participants in group insurance policies;

Applicants:

Persons who have requested an offer or make an application for the conclusion of an insurance contract, irrespective of whether the insurance contract is concluded,

Additional persons:

Data subjects outside of the insurance relationship, such as injured parties, witnesses and other persons whose data the company processes in connection with the establishment, performance or termination of an insurance relationship;

Injured parties:

Persons who have suffered or may have suffered a loss, e.g. claimants in the context of liability insurance;

Data processing:

Collecting, recording, organizing, arranging, storing, adapting or modifying, reading, querying, using, disclosing by transmitting, disseminating or making available in any other form, match or link or restrict processing as well as the erasure or destruction of personal data;

Data collection:

The collection of data regarding data subjects;

Automated data processing:

Collecting, processing or using personal data using data processing systems;

Automated decision-making:

A decision concerning an individual based on exclusively automated processing without a substantive evaluation and decision based on it having been made by a natural person;

Master data:

General data concerning a data subject: name, address, date of birth, place of birth, customer number, profession, marital status, legal representative, information on the type of existing contracts (such as contract status, start and expiry dates, insurance number(s), method of payment, roles of the person concerned (e.g. policyholder, insured person, payer of premiums, claimant), as well as account details, telecommunications data, authentication data for electronic or telephone communication, advertising bans and other objections, advertising consent and bans for market and opinion research, powers of attorney and support regulations, responsible intermediaries and data comparable to the examples given;

Service providers:

Other companies or persons who perform tasks for the company on their own responsibility;

Processor:

A natural or legal person, entity or other body processing personal data on behalf of the company responsible;

Agents:

Self-employed natural persons (commercial agents) and companies who act as insurance agents or brokers within the meaning of section 59 of the German Insurance Contract Act (Versicherungsvertragsgesetz - WG) and who broker or conclude insurance contracts.

Legitimate interests:

The interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

III. GENERAL PROVISIONS

Art. 1 Scope of application

(1) [1]The Code of Conduct applies to the processing of personal data in connection with the insurance business carried on by the Companies. [2]In addition to the insurance relationship, this includes in particular the fulfilment of legal claims, even if an insurance contract is not concluded, does not exist or no longer exists. [3]The insurance business also includes the design and calculation of tariffs and products.

(2) Irrespective of the rules set out here, applicable statutory provisions on data protection, in particular the EU General Data Protection Regulation and the Federal Data Protection Act shall continue to apply.

Art. 2 Purposes of processing

(1) [1]The processing of personal data for the purposes of insurance business shall only take place if this is necessary for the establishment, performance and termination of insurance relationships, in particular for processing an application, for assessing the risk to be insured, for fulfilling the consulting obligations under the Insurance Contract Act (Versicherungsvertragsgesetz, WG), for checking a duty to pay benefits and for internal verification of the timely settlement of claims. [2]It is also used to review and settle claims of injured parties in liability insurance, to review and settle claims for recourse, to conclude and execute reinsurance treaties, to develop tariffs, products and services, for the compilation of statistics, for research purposes relevant to insurance, e.g. accident research, for combating abuse or for the fulfilment of legal and regulatory obligations or for purposes of advertising as well as market and opinion research.

(2) [1]Personal data will be processed within the scope of the purpose known to the data subjects. [2]A change or extension of the purpose shall only take place if it is legally permissible and the data subjects have been informed of it in accordance with Articles 7 or 8 of this Code of Conduct or if the data subjects have given their consent.

Art. 3 Principles of data processing quality

(1) The companies undertake to process all personal data in a lawful and comprehensible manner in accordance with the legitimate interests of the data subject.

(2) [1]Data processing is geared to the goal of minimizing data and limiting storage periods. [2]Personal data shall be stored, subject to the purposes of research and statistics in accordance with Article 5(1)(e) GDPR, in a form that allows identification of the data

subjects only for as long as is necessary for the purposes of the processing. [3]In particular processes that permit anonymization and pseudonymization are to be used, as far as this is possible and the effort is not disproportionate to the desired protective purpose. In this context, anonymization is preferred to pseudonymization.

(3) [1]The company shall ensure that the available personal data is stored correctly and, if necessary, up to date. [2]All reasonable measures shall be taken to ensure that inaccurate or incomplete data is rectified, erased or restricted in processing without delay.

(4) [1]The measures referred to in the preceding paragraphs shall be documented. [2]Principles for this are to be included in the companies' data protection concept (Art. 4 (2)).

Art. 4 Principles of data security

(1) [1]In order to ensure data security, the necessary technical and organisational measures shall be taken, taking into account the state of the art, implementation costs and the nature, scope, circumstances and purposes of the processing and the different likelihood and severity of the risks to the rights and freedoms of natural persons associated with the processing, in order to ensure a level of protection appropriate to the risk. [2]Appropriate measures shall be taken to ensure in particular that

1. Only authorized persons have access to personal data (confidentiality). Without limitation, measures to ensure this include authorization concepts, pseudonymization or encryption of personal data.
2. Personal data remains intact, complete and up-to-date during processing (integrity).
3. Personal data is available on time and can be processed properly (availability, resilience).
4. The origin of personal data may be established at any time (authenticity).
5. It can be determined who entered, transmitted and changed which personal data and when and in what way (auditability).
6. The procedures for processing personal data are complete, up-to-date and documented in such a way that they can be traced in a reasonable time (transparency).

(2) [1]The measures initiated at the companies are to be integrated into a comprehensive data protection and security concept that regulates responsibilities and which is to be drawn up with the involvement of the company's data protection officer. [2]Without limitation, it includes procedures for the regular review and evaluation of the effectiveness of the measures taken.

Art. 5 Consent

(1) [1]Where the processing of personal data is based on consent and, where necessary, on a declaration of confidentiality of the data subjects, the company shall ensure that such consent is voluntary, informed and unambiguous, effective and not revoked. [2]In cases where special categories of personal data - in particular data relating to health - are processed, the relevant consent must be expressly given.

(2) [1]In cases where the processing of personal data of minors is based on consent and - if necessary - on a confidentiality release, these declarations shall be obtained from the legal representative. [2]No earlier than the age of 16, these declarations shall be obtained from the minor themselves provided they have sufficient capacity to understand.

(3) [1]The company or intermediary obtaining the consent shall ensure and document that the data subjects are previously informed about the data controller, the scope, form and purpose of data processing and the possibility of refusal and revocability of the consent and its consequences. [2]This is without prejudice to Art. 7 (3) of this Code of Conduct.

(4) The consent and the release of confidentiality can be revoked at any time with effect for the future without a need to provide grounds. [2]The data subjects will be informed about the possibilities and consequences of revoking a declaration of consent. [3]Without limitation, potential consequences of an effective revocation may include the circumstance that a service cannot be provided.

(5) If consent is obtained in writing or electronically together with other declarations, it shall be highlighted in such a way that it catches the eye.(6) [1]Consent may be given in writing, electronically or verbally. [2]The company will document the declaration in such a way that the content of the declaration of consent issued can be verified. [3]The content of the declaration shall be made available to the data subjects upon request.

(7) If consent is obtained orally, this must be confirmed immediately in writing or in text form with the data subjects.

Art. 6 Special categories of personal data

(1) [1]Special categories of personal data within the meaning of the EU General Data Protection Regulation (in particular information on health) are collected and processed on a statutory basis (in particular Art. 6 in conjunction with Art. 9 General Data Protection Regulation) or with the consent of the data subjects pursuant to Article 5 and - if necessary - on the basis of a release from confidentiality obligations. [2]The consent must refer explicitly to this data.

(2) [1]The processing of special categories of personal data on a legal basis is permitted, in particular if it is necessary for the establishment, exercise or defence of legal claims. [2]This applies, for example, to the examination and settlement of the claims of insured persons and injured parties in the context of liability insurance.

(3) Furthermore, the health data of data subjects may be processed without their consent for the assertion, examination and settlement of legally regulated recourse claims on the one hand of the company or on the other hand of a third party who has provided a service to the data subjects, for example for the examination and settlement of recourse claims of a social insurance carrier, employer or private health insurer.

(4) The processing of special categories of personal data may also be permitted within the framework of statutory provisions, insofar as this is necessary for preventive health care or health care.

(5) Health data may also be processed without consent in order to protect the vital interests of the data subjects or other persons if they are unable to give their consent for physical or legal reasons, in particular if assistance services (e.g. emergency call services, transport of patients from abroad or coordination of medical treatment) have been agreed for these persons and they are not in a position to give their consent in the event of an accident, e.g. because a transport of an unconscious person is required after an accident.

(6) [1]Special categories of personal data may also be processed on a statutory basis for statistical purposes and for research purposes in accordance with Art. 10 of this Code of Conduct.

IV. DATA COLLECTION

Art. 7 Principles of data collection and information when collecting data from the data subject

(1) [1]Personal data shall be collected in a transparent manner. [2]In the case of insured persons and applicants, the duties to cooperate in accordance with sections 19, 31 WG shall be given consideration.

(2) [1]Personal data of other persons within the meaning of this Code of Conduct is collected and processed if it is necessary to establish, exercise, or defend legal claims or to fulfil a legal obligation. [2]This applies in particular to the collection of data from witnesses or injured parties in connection with a performance review and performance in liability insurance and to data processing for the fulfilment of direct claims in motor liability insurance or for the fulfilment of statutory reporting obligations. [3]Data referred to in sentence 1 may also be collected and processed if this is necessary in connection with the establishment, performance or termination of an insurance relationship and the legitimate interests of such persons are not predominant, for example if data from a lawyer or a repair workshop is required for correspondence in the event of the payment of benefits.

(3) [1]Companies shall ensure that, in order to ensure transparency and to safeguard their rights, data subjects are informed of the following:

a) The identity of the data controller (name, registered office, contact details, authorised representative);

b) Contact details for the data protection officer;

c) The purposes and legal bases (including, where applicable, legitimate interests) for data processing;

d) If applicable, the recipient or categories of recipients of the personal data;

e) If applicable, any intended transfer of personal data to a third country or an international organisation in accordance with Art. 13(1)(f) GDPR;

f) The duration (or criteria) of the storage of personal data;

g) The rights of data subjects as provided for in Section VIII of this Code of Conduct, including the right to lodge a complaint with a supervisory authority;

h) Where processing is based on consent: the right to withdraw the consent and its consequences;

i) If applicable, any legal, contractual obligation to provide data, or obligation to provide data in connection with the conclusion of a contract, and the consequences of a failure to provide information; and

j) Where automated decision-making is used, meaningful information on the logic used, the scope and effects of such processing.

[2]The information need not be provided if and to the extent that the data subjects have already obtained such information by other means.

Art. 8 Data collection without the involvement of the data subjects

(1) [1]Data shall be collected without the involvement of the persons concerned if this is necessary in connection with the establishment, performance or termination of insurance relationships and in particular also for the examination and processing of claims for benefits. [2]This applies, for example, if the policyholder legitimately provides the data of the insured persons for group insurance policies or the data of the beneficiaries for life and accident insurance policies, or if they provide information about the injured party or witnesses in the context of liability insurance. [3]Personal data may also be collected for the purposes set out in Article 10 (1) without the involvement of the data subject.

(2) [1]The collection of health data or genetic data from third parties shall - if necessary - take place with an effective declaration of confidentiality from the data subjects and in accordance with section 213 WG and section 18 German Genetic Diagnosis Act (GenDG), insofar as such provisions are applicable. [2]The collection of specific categories of personal data from third parties may also be necessary in the cases referred to in Article 6 (2) to (5) of this Code of Conduct.

(3) [1]The company collecting personal data without the involvement of the data subjects shall ensure that the data subjects are informed within a reasonable period of time in each individual case, but no later than one month after the data were first collected concerning:

a) The identity of the data controller (name, registered office, contact details, authorised representative);

b) Contact details for the data protection officer;

c) The purposes and legal bases (including, where applicable, legitimate interests) for data processing;

d) The categories of personal data being processed;

e) If applicable, the recipient or categories of recipients of the personal data;

f) If applicable, any intended transfer of personal data to a third country or an international organisation in accordance with Art. 14(1)(f) GDPR;

g) The duration (or criteria) of the storage of personal data;

h) The rights of data subjects as provided for in Section VIII of this Code of Conduct, including the right to lodge a complaint with a supervisory authority;

i) Where processing is based on consent: the right to withdraw the consent and its consequences;

j) The source of the personal data or whether it comes from a publicly accessible source; and

k) Where automated decision-making is used, meaningful information on the logic used, the scope and effects of such processing.

[2]If the data is to be used for communication with the data subjects, the information shall be provided no later than the first notification to them, for example in cases of the designation of beneficiaries in life insurance upon the occurrence of the insured event or in cases of the designation of beneficiaries for emergencies if this occurs. [3]If disclosure to another recipient is intended, the information shall be provided at the time of the first disclosure at the latest.

(4) [1]The information need not be provided if and to the extent that the data subjects already have the information, the provision of the information proves impossible or the information would require disproportionate effort, in particular if data is processed for statistical or scientific purposes or if stored data is taken from generally accessible sources and notification is disproportionate due to the large number of cases concerned. [2]Information need likewise not be provided if the data must be kept secret in accordance with a legal provision or its nature, in particular because of the overriding legitimate interest of a third party. [3]This applies, for example, in cases in life insurance in which the policyholder wishes that a beneficiary is not informed.

(5) Information in accordance with section 33 (1) no. 2 Federal Data Protection Act in conjunction with Art. 23(1)(j) may likewise be dispensed with if:

- It would prejudice the establishment, exercise or defence of civil law claims or involves the processing of personal data from civil law contracts and serves to prevent damage caused by criminal offences, unless the legitimate interest of the data subject in providing the information predominates; or
- Disclosure of the information would jeopardise prosecution by the authorities.

[2]Therefore, no information will be provided as a rule concerning data collection to clarify inconsistencies in accordance with Article 15 of this Code of Conduct.

(6) [1]In the cases referred to in paragraph (5), the company shall take appropriate measures to protect the legitimate interests of the data subjects (e.g. examination and, where appropriate, initiation of further access restrictions). [2]If the company refrains from providing information, it shall document the reasons for doing so.

V. PROCESSING PERSONAL DATA

Art. 9 Processing master data within the group of companies

(1) Where a company belongs to a group of insurance and financial services companies, the master data of applicants, insured persons and other persons and information relating to existing contracts may be used for the centralised processing of certain stages in the course of business (e.g. telephone calls, mail, collection) in a data processing procedure that can be shared by members of the group, if it is ensured that the technical and organisational measures comply with the data protection requirements in accordance with Art. 4 of this Code of Conduct (e.g. authorisation concepts) and that compliance with this Code of Conduct by the person or persons responsible for the procedure is guaranteed.

(2) Master data will only be processed further by jointly usable data processing procedures if this is necessary for the respective purpose. This must be guaranteed technically and organisationally.

(3) [1]If data is processed jointly in accordance with paragraph (1), the insured persons shall be informed in writing when the contract is concluded or when such a procedure is established. [2]To this end, the company shall keep an up-to-date list of all the companies in the group participating in centralised processing and shall make the list available in an appropriate form.

(4) Where a company carries out further data processing for another member of the group, or where joint processing is carried out by several members of the group, this shall be in accordance with Articles 21 to 22a of this Code of Conduct.

Art. 10 Statistics, tariff calculation and premium calculation

(1) [1]The insurance industry uses actuarial methods to calculate the probability and amount of claims based on statistics and experience and develops tariffs on this basis. [2]In addition to data from insurance relationships, benefits and claims, companies also evaluate other data from third parties (e.g. the Federal Motor Transport Authority).

(2) [1]The companies shall take appropriate technical and organisational measures to ensure that the rights and freedoms of the data subjects are safeguarded in accordance with the General Data Protection Regulation, in particular that the processing of personal data is limited to what is necessary for the relevant statistics. [2]These measures include the early anonymization or pseudonymization of data, if it is possible to fulfil the statistical purpose in this way.

(3) [1]The transmission of data to the Association of German Insurers (Gesamtverband der Deutschen Versicherungswirtschaft e. V.), the Private Health Insurance Association (Verband der Privaten Krankenversicherung e. V.) or other bodies for the calculation of cross-company statistics or risk classifications is only carried out in an anonymous or - if necessary for the statistical purpose - pseudonymized form. [2]These associations do not associate this data with any data subjects. [3]Paragraph (2) shall apply accordingly. [4]For motor vehicle and property insurance statistics, data records with personal data such as license plates, vehicle identification numbers or location data of risk objects such as buildings may also be transmitted.

(4) [1]For data processing for statistical purposes, companies may also process special categories of personal data, in particular health data, if this is necessary for the respective statistical purpose and if the interests of the company in the processing significantly outweigh the interests of the data subjects in an exclusion from processing. [2]This is the case, for example, regarding statistics for the development and review of tariffs or statutory risk management. [3]In such cases, the companies shall take appropriate and specific measures to safeguard the interests of the data subjects and in particular the principles laid down in Articles 3 and 4. [4]In light of the special need to protect this data, such specific measures include without limitation:

- Raising the awareness of the employees and service providers involved in the processing;
- The pseudonymization of personal data in accordance with paragraph (2), sentence 2;
- The restriction of access to personal data within companies or at the service provider; and
- Encryption when transporting personal data.

[5]All personal data will be made anonymous as soon as this is possible based on the statistical purpose unless the anonymization is contrary to the legitimate interests of the data subjects. [6]Until then, the identification features with which individual data could be associated with a data subject shall be stored separately. [7]These identifying features may only be combined with the individual details if the statistical purpose so requires.

(5) 1The data subjects may object to the processing of their personal data for statistical purposes if their personal situation gives rise to reasons which conflict with the processing of their data for this purpose. [2]The right of objection does not exist if the processing is necessary to fulfil a task in the public interest (e.g. answering inquiries from the Federal Financial Supervisory Authority).

(6) [1]Tariffs in accordance with paragraph (1) shall be applied to the individual situation of the applicant in order to determine the risk-based premium. [2]In addition, an assessment of the applicant's individual risk by specialised risk assessors, e.g. doctors, can be included in the premium calculation. [3]Personal data, including where applicable special categories of personal data, such as health data, which has been processed in accordance with this Code of Conduct, shall also be used for this purpose.

(7) The insurance industry processes personal data in accordance with the above paragraphs also for purposes of scientific research, for example accident research.

Art. 11 Scoring

Applicable statutory regulations apply to scoring.

Art. 12 Creditworthiness data

The statutory regulations apply to the collection, processing and use of creditworthiness data.

Art. 13 Automated individual decision-making

(1) Automated decisions which produce legal effects concerning the data subject or similar significantly affects them shall only be taken under the conditions set out in paragraphs (2), (3) and (4).

(2) [1]A decision necessary for the conclusion or performance of an insurance contract with the data subject or in the context of the provision of services may be taken by automated means. [2]Necessity includes the following cases in particular:

1. Decisions vis-à-vis applicants on the conclusion and conditions of an insurance contract;
2. Decisions vis-à-vis policyholders on benefit cases within the framework of an insurance relationship;
3. Decisions on the fulfilment of features of behaviour-related tariffs, e.g. discounts in motor insurance that reward driving behaviour.

(3) [1]Automated decisions regarding claims under an insurance contract, e.g. decisions vis-à-vis co-insured persons or injured parties in liability insurance, are also permissible if the claim of the person concerned is granted. [2]The decision may also be taken by automated means in the context of the provision of services under an insurance contract if the decision is based on the application of binding payment schemes for medical treatment and if the company takes appropriate measures to safeguard the legitimate interests of the data subject in the event that the application is not fully approved, including at least the right of the company to obtain the intervention of a person, to state its own position and to challenge the decision.

(4) In addition, an automated decision may be made with the express consent of the data subject.

(5) [1]Special categories of personal data are processed in the context of automated decision-making if the data subjects have given their consent. [2]Automated decisions concerning special categories of personal data are also possible without consent in the cases referred to in paragraph (3).

(6) [1]If automated decisions are taken at the expense of the persons concerned, the following shall be initiated at a minimum: The company shall inform the data subjects that an automated decision has been made. [2]If they have not already been informed, they shall be provided with meaningful information on the logic involved and the scope and intended effects of automated decision-making. [3]Upon request, data subjects shall also be informed and the main reasons for the decision shall be explained in order to enable them to express their views, for a person to intervene on the part of the company and for the decision to be challenged. [4]This also includes the types of data used and their significance for automated decision making. [5]The data subjects have the right to challenge the decision. [6]The decision will then be re-examined on this basis in a procedure which is not exclusively automated. [7]Article 28(1) of this Code of Conduct shall apply mutatis mutandis.

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

(8) [1]The companies shall ensure that technical and organisational measures are taken to ensure that factors leading to inaccurate personal data may be corrected and the risk of errors is minimized. [2]With regard to health data, the legal requirements of sections 37 (2), 22 (2) BDSG shall be complied with.

Art. 14 Notification and Information System (HIS)

(1) [1]The companies within the German insurance industry - with the exception of private health insurers - use an information system (HIS) to support risk assessment regarding applications, to clarify the facts of the case during the benefit check and to combat the misuse of insurance benefits. [2]The operation and use of the HIS are based on a balancing of interests and defined reporting criteria.

(2) [1]The HIS is operated separately by insurance line of business. [2]Within all lines of business, the data is processed separately in two data pools: in a data pool for the risk check query in the case of an application (A pool) and in a pool for the performance check query (L pool). [3]The companies set up access authorizations for their employees according to lines of business and tasks.

(3) [1]The companies shall report data on vehicles, real estate or persons to the HIS operator if there is an increased risk or if an anomaly has been detected, insofar as this is necessary for current or future disclosure or to prevent the improper obtaining of insurance benefits and there are no predominant legitimate rights and freedoms of the data subjects. [2]The

consent of the data subjects is not required. [3]Prior to reporting personal data, the interests of the companies and the data subject shall be weighed in relation to each other. [4]If the specified reporting criteria are met, it is generally assumed that the company has a predominant legitimate interest in reporting. [5]Such weighing of interests shall be adequately documented and special categories of personal data, such as health data, shall not be reported to HIS. [7]If increased personal insurance risks are reported as “aggravating”, this is done without stating whether they are based on health data or any other reason, e.g. a dangerous profession or hobby. [8]Personal data relating to criminal convictions and offences shall also not be reported to the HIS, unless processing is carried out under official supervision or is permitted under Union law or national law providing appropriate safeguards for the rights and freedoms of data subjects.

(4) [1]The companies shall inform the policyholders in a general form about the HIS at the time the contract is concluded, stating the person responsible and their contact details. [2]They shall provide the data subjects at the time of registration at the latest with the information relevant pursuant to Art. 8 (3). [3]Notification may be omitted in cases of Art. 8 (5) of this Code of Conduct.

(5) 1Data can be retrieved from HIS when an application is submitted and when benefits are paid, but not when an endowment policy is paid out in the event of survival. [2]Data retrieval is not the sole basis for a decision in individual cases. [3]The information is only an indication that the facts need to be examined more closely. [4]All data retrievals are carried out using the automated retrieval procedure and are logged for auditing purposes and for the purpose of randomly checking their authorization.

(6) [1]In so far as necessary for further clarification of the facts of the case, data may also be exchanged between the registering and the retrieving company in the event of a claim if there is no reason to assume that the data subject has a legitimate interest in the exclusion of the transfer. [2]For example, data and expert reports on damage to vehicles or buildings are requested from the company that reported the damage to HIS. [3]The data exchange shall be documented. [4]In so far as the exchange of data does not take place in accordance with Article 15 of this Code of Conduct, data subjects shall be informed of the exchange of data. [5]Information is not required as long as this would jeopardise the clarification of the facts or if the data subjects have otherwise gained knowledge of the exchange of data.

(7) [1]The data stored in the HIS will be deleted at the end of the 4th year after the prerequisite for reporting has been met. [2]An extension of the storage period to a maximum of 10 years shall be granted in life insurance in the benefits area or in the event of renewed registration within the regular storage period in accordance with sentence 1. [3]Data on applications for which no contract has been concluded shall be deleted from HIS no later than the end of the third year after submission of the application.

(8) The Association of German Insurers (Gesamtverband der Deutschen Versicherungswirtschaft) issues detailed guidelines on the use of HIS to companies in compliance with data protection regulations.

Art. 15 Clarification of inconsistencies

(1) [1]The companies may check at any time if there are relevant indications that incorrect or incomplete information was provided during the application process, or updates to application data during the insurance relationship, and thus influenced the risk assessment or that incorrect or incomplete information was provided when a loss was established. [2]For this purpose, companies shall collect and process data to the extent necessary to resolve the inconsistencies. [3]Companies have a margin of discretion when deciding which data they

need in order to make their decision on a sufficient factual basis.

(2) [1]In the event of a claim, the examination in accordance with paragraph (1) can also be carried out without any indications. [2]This includes obtaining preliminary information (e.g. periods during which treatments or examinations took place) that enables the company to assess whether and which information is actually relevant to the examination.

(3) [1]Data processing to verify the information for risk assessment at the time of application shall only take place within five years, for health insurers within three years of conclusion of the contract. [2]The information can still be checked after this period has expired if the insured event occurred before the expiry of the period. [3]This period is extended to 10 years to check whether the policyholder provided incorrect or incomplete information intentionally or fraudulently when submitting the application.

(4) If the collection and processing relates to special categories of personal data, in particular data on health in accordance with paragraph (1), the data subjects shall be informed in accordance with their declaration in the insurance application prior to data collection from third parties in accordance with section 213 (2) WG and informed of their right of objection or an independent declaration of consent and confidentiality shall be obtained in advance from the data subjects.

(5) [1]The possibility of refusing to submit a declaration of consent and confidentiality remains unaffected and the company shall inform the data subject accordingly. [2]If the data subject refuses to submit a declaration of consent and confidentiality, it is incumbent on the data subject to obtain and make available to the company all necessary information as a prerequisite for settling the claim. [3]In such a case, the company shall state what information it considers necessary in the event of refusal of the consent and confidentiality release.

Art. 16 Exchange of data with other insurers

(1) [1]Data shall may be exchanged between an adopting insurer and its successor insurer in order to collect information relevant to collective agreements or benefits in compliance with Article 8 (1). [2]This is particularly the case when the information is required:

1. In the context of risk assessments for the verification of no-claims bonuses, in particular the no-claims bonus classes in motor liability insurance and comprehensive insurance;
2. For the transfer of pension rights in the event of a change of provider or employer;
3. For the transfer of old-age provisions in health insurance to the new insurer;
4. to supplement or verify the information provided by applicants or insured persons.

[3]In the cases referred to in paragraphs (1) and (4), an exchange of data for the purpose of risk assessment is only permitted if the data subjects are informed of the possible data exchange and its purpose and subject matter when data is collected in the application. [4]After an exchange of data for the purpose of performance evaluation, the data subjects will be informed by the company collecting the data about an exchange of data that has taken place to the same extent. [5]Article 15 of this Code of Conduct shall remain unaffected.

(2) Data may also be exchanged with other insurers outside the provisions laid down for the notification and information system of the insurance industry (HIS), to the extent that this is necessary for the examination and provision of applications and benefits, including the settlement of claims in the case of joint, multiple or combined coverage of risks, the legal transfer of a claim against another person or for the settlement of claims between several insurers, concerning existing division and waiver of recourse agreements and there is no

reason to believe that the data subject has an overriding legitimate interest.

(3) The data exchange shall be documented.

(4) [1]Motor vehicle insurers use the loss class file maintained by GDV Dienstleistungs-GmbH as a joint system to prevent insurance abuse. [2]Reports are made to enable correct classification in the no-claims bonus system. [3]This is the case if a motor liability insurance contract is terminated, this prior insurance is not indicated when the contract is concluded and the unencumbered reclassification into the no-claims bonus classes would be contrary to the tariff system. [4]The motor vehicle insurer shall provide the name and address of the policyholder, the policy number, the registration number of the previously insured vehicle, the date of termination of the insurance contract with no-claims bonus class and the number of claims not yet taken into account in the reporting year. [5]This data will only be requested if a policyholder does not apply for a no-claims bonus from the preliminary contract. [6]Motor insurers shall inform policyholders of the class of loss file and contact details of the joint system in the insurance information at the time of conclusion of the contract. [7]If data is reported upon termination of the insurance contract, the motor vehicle insurers shall inform the policyholders of the type of data reported, the purpose of the report, the data recipient (name and registered office of joint system) and potential access to the data. [8]Data is retrieved from the damage class file by means of an automated procedure. [9]They are logged for auditing purposes and random authorization checks. [10]The data stored in the claim class file will be deleted no later than the end of the third year after the conditions for reporting have been met.

Art. 17 Data transfer to re-insurers

(1) [1]In order to be able to meet their obligations under insurance contracts at all times, companies pass on some of their risks under insurance contracts to re-insurers. [2]To further offset risks, in some cases these re-insurers themselves make use of additional re-insurers. [3]Data from the insurance application or relationship, in particular insurance number, premium, type and amount of insurance cover and risk as well as any risk surcharges, shall be passed on in anonymised or - if this is not sufficient for the aforementioned purposes - pseudonymized form for the proper establishment, performance or termination of the reinsurance contract.

(2) [1]Personal data shall only be received by re-insurers to the extent that

a) This is necessary for the conclusion or performance of the insurance contract; or

b) In order to ensure that the obligations of the company arising from the insurance relationships can be fulfilled and there is no reason to believe that an overriding legitimate interest of the data subject conflicts with an interest of the company.

[2]This may be the case if, within the framework of the specific reinsurance relationship, personal data is transferred to re-insurers for the following reasons:

a) The re-insurers carry out risk assessments and performance assessments in individual cases, e.g. in the case of high sums insured or a risk which is difficult to classify.

b) Re-insurers assist companies in assessing risks and claims and in assessing procedures.

c) Re-insurers receive lists of the portfolios of reinsurance contracts for the purpose of determining the scope of reinsurance contracts, including checking whether and to what extent they are involved in the same risk (accumulation control) and for

settlement purposes.

d) The risk and benefit assessment by the primary insurer is checked by the re-insurers on a random basis or in individual cases to check their benefit obligation to the primary insurer.

(3) [1]The companies agree with the re-insurers that personal data will be used by them only for the purposes specified in paragraph (2) and for compatible purposes (e.g. statistics and scientific research). [2]They shall also agree whether the re-insurer will provide the data subject with the information required by law or whether the company will pass on the re-insurer's information to the data subject. [3]In the case of forwarding they also agree on how the notification will be provided. [4]In so far as the companies are subject to a duty of confidentiality pursuant to section 203 StGB, they shall oblige the re-insurers to maintain confidentiality with regard to the data they receive pursuant to paragraph (2) and to oblige other re-insurers and bodies acting on their behalf to maintain confidentiality.

(4) Special categories of personal data, in particular health data, shall be received by re-insurers only if the conditions laid down in Article 6 of this Code of Conduct are met.

VI. PROCESSING PERSONAL DATA FOR SALES PURPOSES AND FOR MARKET AND OPINION RESEARCH

Art. 18 Use of data for advertising purposes

(1) Personal data will only be processed for advertising purposes on the basis of Article 6(1)(a) o (f) of the General Data Protection Regulation and in compliance with section 7 German Act against Unfair Competition (UWG).

(2) [1]The data subjects may object to the use of their personal data for direct marketing purposes. [2]Personal data will then no longer be processed for these purposes. [3]The company shall take appropriate technical and organizational measures implementation of the foregoing requirements.

Art. 19 market surveys

(1) The companies carry out market and opinion surveys, paying particular attention to the legitimate interests of the data subjects.

(2) [1]In so far as the companies commission other entities to conduct market and opinion surveys, such entities shall be selected upon proof of compliance with data protection standards. [2]Prior to the disclosure of data, the details of the project shall be laid down in a contract in accordance with Articles 21, 22 or 22a of this Code of Conduct. [3]The following shall be specified in particular:

a) That data transmitted and additionally collected is pseudonymized as soon as possible and anonymized as soon as possible according to the purpose of the survey;

b) That the evaluation of the data and the transmission of the results of the market and opinion surveys to the companies are as anonymous or pseudonymous as possible if this is necessary for the intended purposes (e.g. follow-up surveys).

(3) [1]If the companies themselves process or use personal data for the purpose of conducting market and opinion surveys, the data will be pseudonymized as soon as possible and anonymised as soon as possible based on the purpose of the survey. [2]The results will only be stored or used in anonymised or pseudonymized form if this is necessary for the intended purposes (e.g. follow-up surveys).

(4) Insofar as business activities are carried out within the framework of market and opinion surveys which are to be regarded as advertising, for example if promotional statements are also made during data collection, the processing of personal data shall be governed by the rules laid down in Article 18 of this Code of Conduct.

Art. 20 Data transmission to independent agents

(1) [1]Personal data will only be transferred to the respective agent if it is necessary for the preparation or processing of a specific application or contract or for the proper management of the insurance affairs of the data subjects. [2]The agents shall be made aware of their special confidentiality obligations.

(2) [1]Prior to the first transmission of personal data to an insurance agent, or in the event of a change from the relevant insurance agent to another insurance agent, the company shall, subject to the provisions of paragraph (3), inform the insured persons or applicants as early as possible, but at least two weeks before the transmission of their personal data, of the identity (name, registered office) of the new insurance agent and their right of objection. [2]No notification shall be given if the data subject themselves desires such a change. [3]Notice from the previous insurance agent is equivalent to notice by the company. [4]In the event of an objection, the data will not be transmitted. [5]In this case, support will be provided by another insurance agent or the company itself.

(3) An exception to paragraph (2) applies if the proper care of the insured in a specific case or the continuation of the contractual relationships is endangered in the event of an unexpected discontinuation support.

(4) [1]Personal data of insured persons or applicants may be transferred to an insurance broker or a service company comprising insurance brokers if the insured persons or applicants have granted the broker a broker's power of attorney or a comparable power of attorney covering the data transfer. [2]In the event of a change of broker, paragraph (2) shall also apply accordingly.

(5) [1]The company does not transfer health data to the acting broker unless the data subjects have given their consent. This is without prejudice to statutory powers of transmission.

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

Art. 21 Obligations related to contract processing

(1) [1]If a company has personal data processed by a processor in accordance with Article 28 of the General Data Protection Regulation (e.g. electronic data processing, scanning and assignment of incoming mail, address management, processing of applications and contracts, processing of claims and benefits, ensuring correct accounting of incoming payments, outgoing payments, disposal of documents), at a minimum, the processor shall be obliged in accordance with Article 28(3) of the General Data Protection Regulation. [2]Only contractors shall be selected who offer sufficient guarantees that appropriate technical and organisational measures will be taken to ensure that the processing is carried out in accordance with the General Data Protection Regulation and that the rights of the data subjects are protected. [3]The company requires all necessary information to prove and verify compliance with the technical and organizational measures taken by the contractor, for example by means of suitable certificates. The results are to be documented.

(2) [1]Any processing of data by the processor shall only be performed for the purposes and within the framework of the documented instructions of the company. Contract clauses should be submitted to the data protection officers, who will assist in an advisory capacity if

necessary.

(3) [1]The company shall maintain an up-to-date list of contractors. [2]If the automated processing of personal data is not the main object of the contract, or if many different contractors (e.g. service providers for the destruction of files at different company locations or regional workshops) are entrusted with similar tasks, contract processors may - without prejudice to internal documentation obligations - be grouped into categories, specifying their task. [3]This also applies to contractors who only perform services on an occasional basis. [4]The list shall be made available in an appropriate form. [5]If personal data is collected from the data subjects, they are fundamentally to be informed of the list when the data is collected.

(4) A contract or other legal instrument within the meaning of Art. 28(3) and (4) of the General Data Protection Regulation concerning contract processing shall be prepared in writing, which may also be in an electronic format.

Art. 22 Data processing by service providers without contract data processing

(1) [1]Without an agreement on contract data processing, personal data may be transferred to service providers for the independent fulfilment of tasks and processed by them, insofar as this is necessary for the purpose of the insurance relationship with the data subjects. [2]This is possible in particular when experts are commissioned to assess an insured event or when service providers are engaged to provide the contractually agreed insurance benefits in kind, e.g. ambulance services, domestic help, key services and similar service providers.

(2) [1]The transmission of personal data to service providers and its processing for the independent fulfilment of data processing or other tasks can also take place if this is necessary to protect the legitimate interests of the company and such interests are not outweighed by the legitimate interests of the data subjects. [2]This may be the case, for example, if service providers assume tasks that support the company's business processes, such as risk assessment, claims and benefits processing and debt collection, provided this is not contract data processing and the requirements of paragraphs (4) to (8) are fulfilled.

(3) [1]The transfer of personal data to service providers pursuant to paragraph (2) shall not take place if the data subject objects for reasons related to their particular personal situation and an examination reveals that there are no compelling grounds for processing on the part of service provider which would outweigh the interests of the data subject. [2]Transmission to the service provider shall also take place despite the objection if it serves to establish, exercise, or defend legal claims. [3]The data subjects shall be informed in an appropriate manner of their ability to object.

(4) The company shall conclude a contractual agreement with the relevant service providers in accordance with paragraph (2); the agreement must contain the following points at a minimum:

- Clear description of the service provider's tasks;
- Assurance that the transmitted data will only be processed or used within the scope of the agreed purpose;
- Ensuring a standard of data protection and data security that complies with this Code of Conduct;
- The service provider's obligation to provide the company with all the information necessary to fulfil any obligation to provide information applicable to the company or to provide information directly to the data subject.

(5) These outsourcing of tasks in accordance with paragraph (2) shall be documented.

(6) [1]In the cases referred to in paragraph (2), the companies and service providers shall additionally agree that data subjects who have suffered damage as a result of the transmission of their data to the service provider, or the processing of their data by the service provider, are entitled to assert damage claims against both parties. In relation to the data subjects, the company will have first priority for the compensation of damages. [3]The parties shall agree that they are jointly and severally liable and can only be released from liability if they can prove that neither of them is responsible for the damage suffered.

(7) [1]The company shall maintain an up-to-date list of the service providers referred to in paragraph (2) to whom tasks have primarily been delegated. [2]If the automated processing of personal data is not the main object of the contract, the service providers may be grouped into categories under the designation of their task. [3]This also applies to service providers who only perform a task on one occasion. [4]The list shall be made available in an appropriate form. [5]If personal data is collected from the data subjects, they must always be informed of the list when upon data collection.

(8) The company shall ensure that the rights of data subjects under Articles 23 to 24c are not prejudiced by the involvement of the service provider referred to in paragraph (2).

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

(10) [1]Special types of personal data may only be processed within this framework if the data subjects have consented or there is an applicable legal basis. [2]In so far as the companies are subject to a duty of confidentiality in accordance with section 203 of the German Criminal Code (StGB), they shall oblige their service providers to maintain confidentiality with regard to the data they receive in accordance with paragraphs (1) and (2) and to oblige other service providers and entities that work for them to maintain confidentiality.

Art. 22a Joint controllers

(1) A group of insurance and financial services companies may set up common data processing operations for common business purposes in accordance with Article 26 of the General Data Protection Regulation.

(2) 1 In the case of joint data processing operations with two or more data controllers, the companies shall determine in a transparent manner by contractual agreement which of them fulfils which obligation under the General Data Protection Regulation, in particular which body performs which functions in order to fulfil the rights of the data subjects. [2]The responsibilities for providing information to the data subjects shall be addressed as well.

(3) The company shall keep an up-to-date list of the purposes of the common data processing operations indicating the companies responsible and shall inform the data subjects of this in an appropriate form.

(4) Data subjects may exercise their rights under data protection law in relation to each individual controller.

VIII. RIGHTS OF DATA SUBJECTS

Art. 23 Right of information

(1) Data subjects have the right to know whether personal data relating to them are processed and they can request information about the data stored about them at the company.

(2) Where a company processes a large amount of information about the data subject or where a request for information is not specific to the personal data to be disclosed, it shall first provide information on the master data stored on the data subject and summary information

on the processing and shall ask the data subject to specify which information or which processing operations they require.

(3) [1]The data subject shall be provided with information in accordance with their request. [2]Information shall be provided in such a way that the data subject is made aware of the nature and scope of the processing and can verify its lawfulness. [3]It shall be ensured that the data subject receives all information required by law. [4]In the event of a (planned) disclosure, the data subject will also be informed of the recipients or categories of recipients to whom their data have (will be) been disclosed.

(4) [1]It shall be ensured that only authorized persons receive the information. [2]Therefore, even if an authorised representative so requests, the information shall be provided to the data subject or their legal representative.

(5) [1]Information shall be provided in writing or in another form, in particular also electronically, for example in a customer portal. In the case of an electronic request, information is to be provided in a common electronic format. [2]This is not the case if something else is desired or if the authenticity of the recipient or secure transmission cannot be guaranteed. [3]At the request of the data subjects, information may also be provided orally, but only if the identity of the data subjects has been proven.

(6) The rights and freedoms of other persons may not be affected by the information. Business secrets of the company may be taken into account.

(7) [1]Information may be omitted if the data must be kept secret in accordance with a legal provision or its nature, in particular because of the overriding legitimate interest of a third party, or if the disclosure of the information would endanger criminal prosecution. [2]Furthermore, no information will be provided on data which is only stored because it may not be deleted due to legal or statutory retention regulations or which serve exclusively the purpose of data protection or data protection control if the provision of information would require a disproportionate effort and processing for other purposes would be excluded by suitable technical and organisational measures. [3]Examples include data that is restricted as to its processing due to retention obligations and access-protected backups.

(8) [1]In the cases referred to in paragraph (7), the reasons for the refusal to provide information shall be documented. [2]The refusal to provide information shall be explained to the data subject. [3]The reasons shall not be given if the purpose of the refusal of information would be jeopardised by the disclosure of the factual or legal reasons for the refusal of information, in particular if the disclosure of the reasons would impair the overriding legitimate interests of third parties or criminal prosecution.

(9) In the case of reinsurance (Art. 17), data processing by service providers without contract processing (Art. 22) or processing by joint controllers (Art. 22a), the company shall accept the requests for information and also provide all information to which the re-insurer, service provider or all controllers are obliged or shall ensure the exchange of information by them.

Art. 23a Right to data portability

(1) The data subject shall receive the personal data provided by them from the company if the processing is based on their consent or on a contract with them and the processing is carried out by means of automated procedures.

(2) [1]The right includes the data that the data subject has provided to the company. [2]Without limitation, this comprises the data provided by the data subject in applications, such as name, address and information requested on the risk to be insured, as well as any other personal data provided in the course of the insurance relationship, for example in the case

of claims.

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

(4) Data subjects may also request that the personal data be transferred directly by the company to another controller, provided that this is technically feasible and the security requirements for the transfer can be met.

(5) The data will not be made directly available to another controller if the rights and freedoms of other persons would be affected.

Art. 24 Right to rectification

If the stored personal data proves to be incorrect or incomplete,

such will be rectified.

Art. 24a Right to the restriction of processing

(1) The company shall, at the request of the data subjects, restrict the processing of their data:

a) For as long as the accuracy of disputed data is being checked;
b) If the processing is unlawful and the data subject requests continued storage of the data;

c) If the company no longer needs the personal data for the purposes of the processing, but the data subjects need the data for purposes of the establishment, exercise or defence of legal claims; or

d) Where the data subjects have objected to the processing, until it is established whether the legitimate reasons of the company outweigh those of the data subjects.

(2) If the data subjects exercise their right of restriction on processing, the data may only be processed:

a) With the consent of the data subjects;

b) To establish, exercise, or defend legal claims;

c) to protect the rights of another natural or legal person; or

d) For reasons of important public interest of the European Union or a Member State.

(3) Data subjects who have obtained a restriction on processing shall be informed by the company before the restriction is lifted.

Art. 24b Erasure

(1) [1]Personal data shall be erased immediately if the collection or processing was unlawful from the outset, if the processing proves to be unlawful due to subsequent circumstances or if information concerning the data on the part of the company is no longer required to fulfil the purpose of the processing. [2]The data will also be erased if it is necessary to fulfil a legal obligation or if the personal data relating to information society services offered to a child have been collected in accordance with Art. 8(1) of the General Data Protection Regulation.

(2) [1]The database shall be reviewed at regular intervals, at least once a year, to determine whether erasure is necessary in accordance with paragraph (1). [2]If requested by the data subject, whether the data within the scope of the request should be deleted shall be examined without delay.

(3) [1]The data shall not be erased in accordance with paragraph (2) if the data is required:

a) To fulfil a legal obligation of the company, in particular to fulfil legal retention obligations;

b) For the processing operations for statistical purposes referred to in Art. 10;

c) For archiving purposes in the public interest, scientific or historical research purposes (e.g. reappraisal of the Holocaust); or

d) To establish, exercise, or defend legal claims.

[2]Data may likewise not be erased if the data is not processed automatically, cannot be erased or can only be erased with disproportionate effort due to the special type of storage and the interest of the data subjects in erasure may be regarded as minor. [3]In such cases, or if personal data only has to be stored for the fulfilment of legal retention obligations, its processing is limited according to the principle of data minimisation.

Art. 24c Notification of rectification, limitation of processing and erasure

(1) [1]The company shall notify all recipients, in particular re-insurers and insurance agents, of any rectification, limitation or erasure of data undertaken at the request of the data subject unless this proves impossible or involves a disproportionate effort. [2]This is also the case, for example, if the recipient was already required to erase the data due to a contractual agreement. [3]Upon request, the company shall inform the data subject of these recipients.

(2) If the data was rectified, erased or restricted at the request of the data subjects, they shall be informed of this after the relevant operation.

(3) This shall be without prejudice to other notification obligations in the event of rectifications or erasures of personal data and in the event of restrictions on processing without the data subject's request.

Art. 24d Time limits

[1]The company shall comply with the rights set out in Art. 23 to 24b of this Code of Conduct as soon as possible and in any case within one month of receipt of the request to exercise rights of the data subject. [2]The period may be extended by a further 2 months if necessary, taking into account the complexity and number of requests. [3]In such cases, the company shall inform the data subject of the extension of the time limit within one month of receipt of the request and indicate the reasons for the delay.

IX. COMPLIANCE AND CONTROL

Art. 25 Responsibility

(1) As controllers, the companies are responsible for ensuring that the requirements of data protection and data security are observed.

(2) [1]Employees entrusted with the processing of personal data shall be obliged to maintain confidentiality with regard to personal data, to comply with data protection and the company's instructions in this regard and to comply with statutory confidentiality obligations. [2]They shall be informed that violations of data protection regulations will also be punished or prosecuted as an administrative offence and may result in claims for damages. [3]Violations of data protection regulations by employees may result in sanctions under labour law in accordance with applicable law.

(3) The obligation of the employees under the first sentence of paragraph (2) shall also apply beyond the end of their employment relationship.

Art. 26 Transparency

(1) [1]Texts addressed to data subjects shall be formulated in an informative, transparent, comprehensible and precise manner using clear and simple language. [2]They shall be made available to the data subjects in an easily accessible form.

(2) [1]The companies shall keep a record of data processing methods in use (record of processing activities). [2]They shall make it available to the data protection supervisory authorities on request. [3]Furthermore, the record of processing activities is an internal basis for companies to fulfil their information and disclosure obligations in relation to the data subjects.

Art. 26a Data protection impact assessment

(1) The companies shall in particular check the necessity of a data protection impact assessment before the first or significantly extended use of the following processing operations:

a) Processes involving automated individual decision-making based on procedures for the systematic and comprehensive evaluation of several personal characteristics of the data subjects where they have legal effect vis-à-vis the data subjects or significantly affect them in a similar manner, such as automated risk or performance assessment procedures.

b) Processes involving extensive processing of specific categories of personal data, such as procedures for risk or benefit assessment in health insurance, risk assessment in life insurance or benefit assessment in occupational disability insurance; or

c) Processes for calculating premiums using behaviour-based data of data subjects (e.g. for so-called telematics tariffs in motor insurance or with data from wearables).

(2) [1]The decision whether or not a data protection impact assessment is to be performed and the reasons for doing so shall be documented. [2]Companies shall take appropriate organisational measures to ensure that the data protection officer is consulted when conducting data protection impact assessments.

Art. 27 Data Protection Officer

(1) [1]The companies or a group of insurance and financial services companies shall appoint data protection officers in accordance with legal requirements. [2]They are autonomous and monitor compliance with the applicable national and international data protection regulations and this Code of Conduct. [3]The companies are required to provide for this independence contractually.

(2) The data protection officers shall monitor compliance with the General Data Protection Regulation and other provisions of data protection law, including the concepts in place at the company for the protection of personal data, and shall be informed in good time for this purpose before the establishment of a procedure for the automated processing of personal data, or not just an insignificant change, and shall participate in an advisory capacity.

(3) [1]To this end, in consultation with management at the respective company, they can arrange for all company divisions to take the necessary data protection measures; in this respect, they have an unimpeded right of control within the company.

(4) The data protection officers shall inform and advise companies and employees involved in the processing of personal data on the specific requirements of data protection in each

specific case.

(5) [1]Any data subject may also contact the data protection officer at any time with suggestions, enquiries, requests for information or complaints in connection with data protection or data security issues. [2]Inquiries, requests and complaints shall be treated confidentially. [3]The data required to establish contact will be made available in an appropriate form.

(6) The management boards of the companies responsible for data protection shall support the data protection officers in the performance of their duties and work with them in a spirit of trust to ensure compliance with the applicable national and international data protection regulations and this Code of Conduct.

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

(8) [1]The data protection officers shall cooperate with the supervisory authority responsible for the company. [2]For this purpose, they may consult with the relevant data protection supervisory authority in confidence at any time and are available to the supervisory authority as contact persons in all data protection matters.

Art. 28 Complaints and response to violations

(1) [1]The companies will process complaints from insured persons or other data subjects concerning violations of data protection regulations and this Code of Conduct without delay and respond within a period of one month or give an interim decision. [2]A report on the measures taken may also be issued up to three months after the submission of the requests if this extension is necessary, taking into account the complexity and number of requests. [3]The data required to establish contact will be made available in an appropriate form. [4]If the responsible department cannot remedy the situation promptly, it must contact the data protection officer immediately.

(2) Management at the companies shall remedy legitimate complaints as quickly as possible.

(3) [1]If this is not the case, the data protection officers may contact the competent supervisory authority for data protection. [2]They shall inform the data subjects and indicate the competent supervisory authority.

Art. 29 Reporting personal data breaches

(1) [1]In the event of a personal data breach, e.g. if it has been unlawfully transmitted or unlawfully disclosed to third parties, the companies shall inform the competent supervisory authority without delay and if possible within 72 hours of becoming aware of the breach, unless the breach is not likely to pose a risk to the rights and freedoms of the data subjects. [2]Risks to the rights and freedoms of the data subjects exist in particular if it is to be feared that the violation will lead to identity theft, financial loss or damage to their reputation.

(2) [1]The company shall document personal data breaches including all related facts, effects and remedial measures taken. [2]This documentation will enable the regulatory authority to verify compliance with the provisions of this Article.

(3) [1]The data subjects shall be notified if the personal data breach is likely to entail a high risk to their personal rights and freedoms. [2]This shall be done immediately. [3]The decision as to whether measures should be taken first to secure the data or to prevent future injuries is made in accordance with the risk situation. [4]If notification would require disproportionate effort, e.g. because of the large number of cases concerned or if it is not possible to establish the persons concerned within a reasonable time or with reasonable technical effort, the

public would be informed instead.

(4) [1]The data subjects shall not be notified if the data controller has taken appropriate technical and organisational measures to ensure that the high risk to the rights and freedoms of the data subjects is unlikely to exist or no longer exists. [2]Notification of data subjects shall also be omitted where the notification would reveal information which, by law or by its nature, must be kept confidential, in particular because of the overriding legitimate interests of a third party, unless the interests of the data subjects in the notification, in particular taking into account imminent damage, outweigh the interest in secrecy.

(5) Notification of data subjects shall describe in clear and simple language the nature of the personal data breach and shall include at the least:

a) The name and contact details of the data protection officer or another contact point for further information;

b) A description of the likely consequences of the personal data breach;

c) A description of the measures taken or proposed by the company to remedy the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

(6) The companies shall require their contract processors to inform them without delay of incidents referred to in paragraph (1).

(7) [1]Companies shall develop a policy for dealing with personal data breaches. [2]They shall ensure that all breaches are brought to the attention of the respective company's data protection officer. [3]The company data protection officers report directly to the highest management level at the respective company.

X. FORMALITIES

Art. 30 Adoption

(1) [1]The companies that have adopted this Code of Conduct undertake to comply with them from the date of adoption. [2]Adoption by the companies is documented by the GDV and announced in an appropriate form.

(2) Policyholders whose contracts were already in place before the company adopted this Code of Conduct will be informed of their adoption of this Code of Conduct via the company's website and, at the latest, by the next contract mail in text form.

(3) [1]If a company has adopted this Code of Conduct, the then-current version shall apply. [2]Cancellation of the adoption is possible at any time by declaration submitted to the GDV. [3]If a company declares its withdrawal, this will be documented by the deletion of the company from the GDV adoption list and announced in the form of an updated adoption list in an appropriate manner. [4]The company shall also inform the data protection authority responsible for the company and the insured persons about the withdrawal.

Art. 31 Evaluation

These Code of Conduct will be evaluated in relation to any change in the law relating to their content, but no later than three years after application of the General Data Protection Regulation.

Art. 32 Effective date

This version of the Rule of Conduct is effective as of 1 August 2018 and replaces the version of 7 September 2012.