Version as of 7 September 2012

Code of conduct
for the handling of personal data
by the German insurance industry[1]

I. INTRODUCTION

The Berlin-based German Insurance Association (*Gesamtverband der Deutschen Versicherungswirtschaft e.V. - GDV*) is the federation 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 is working towards a regulatory framework that enables insurers to fulfil their tasks in optimal fashion.

The insurance industry has always relied on using a large amount of personal data of insureds. These are collected, processed or used within the scope of handling applications and contracts as well as settling claims and benefits, in order 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 can only fulfil their tasks by means 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 rules not only have to be in line with the provisions of the European Data Protection Directive, of the German Federal Data Protection Act (*Bundesdatenschutzgesetz – BDSG*) and with all sector-specific regulations on data protection, but the undertakings of the insurance industry having joined this code of conduct shall also commit themselves to meet the principles of transparency, of necessity of the data processed and of data avoidance and data minimization to a particular extent.

For this purpose, the GDV, in consultation with its member companies, has established the following code of conduct for handling personal data of insureds. It creates standards for the insurance industry, which are as uniform as possible and promotes compliance with data protection regulations. The supervisory authorities in charge of member companies have agreed to this code of conduct. Thereupon, it has been submitted to the Berlin Commissioner for Data Protection and Freedom of Information (*Berliner Beauftragter für Datenschutz und Informationsfreiheit*) being the supervisory authority in charge of the GDV according to Sect. 38a BDSG, who has declared it consistent with applicable data protection law. Thus, GDV member companies joining this code of conduct according to Article 30 shall undertake to comply with it.

[1] The English version of the data protection codes of conduct / consent clause is not an official translation. It has not been coordinated with the German data protection authorities.

The code of conduct is to ensure to insureds of undertakings having joined it that data protection and data security concerns are considered in designing and adapting products and services. GDV assures these undertakings of its support with regard to this concern. 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. As a matter of 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 of market and opinion research. For the processing of particularly sensitive types of personal data – such as data on health – the GDV, in cooperation with the competent supervisory authorities, has prepared model declarations together with notes on their use. The undertakings having joined this code of conduct are called upon by the data protection authorities to use – adjusted to their business processes – texts of consent which correspond to the model clause.
The present code of conduct specifies and supplements the rules of the Federal Data Protection Act for the insurance sector. As special rules for GDV member companies having joined this code of conduct, it covers the most important types of processing of personal data used by the undertakings in connection with the establishment, performance, termination or acquisition of insurance contracts or to meet legal obligations.

Since the code of conduct has to be capable of regulating the data processing of all undertakings having joined it, it has been worded in a general way, wherever possible. Therefore, it may be necessary that the individual undertakings specify it in undertaking-specific rules. The data protection and data security level achieved by the code of conduct shall not be fallen short of. Beyond that, 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 there are special agreements or arrangements on especially appropriate procedures in terms of data protection with the competent supervisory authorities, these shall of course remain in force even after the undertaking concerned has joined this code of conduct.

Notwithstanding the rules stipulated in this code of conduct, the regulations of the 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 Federal Data Protection Act shall apply to the code of conduct.
In addition:

undertakings:
shall mean GDV member companies having joined this code of conduct, provided they carry out insurance business as primary insurers,

insurance relationship:
shall mean the insurance contract including the related obligations similar to legal transactions,

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 persons, witnesses or other persons whose data are collected, processed or used by the undertaking in connection with the establishment, performance or termination of an insurance relationship,

data collection:
shall mean the procurement of data on data subjects,

data processing:
shall mean the recording, alteration, transfer, blocking or erasure of personal data,

use of data:
shall mean any use of personal data unless considered to be processing,

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

master data:
shall mean general customer data of insureds: name, address, date of birth, place of birth, customer number, insurance policy number(s) and comparable identification data as well as bank details, telecommunication data, exclusions from advertising, consent to advertising and blocking for the purposes of market and opinion research,

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

processors:
shall mean other undertakings or persons that bound by instructions collect, process or use personal data on behalf of the 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*).

III. GENERAL PROVISIONS

Art. 1 Scope

(1) The code of conduct shall apply to the collection, processing and use of personal data in connection with the insurance business carried out by the undertakings. This shall include – in addition to the insurance relationship – the fulfilment of legal claims, even where no insurance contract is concluded or where no insurance contract exists or where an insurance contract does no longer exist.

(2) Notwithstanding the rules stipulated in this code of conduct, the regulations of the Federal Data Protection Act shall apply.

Art. 2 Principle

(1) As a matter of principle, the collection, processing or use of personal data shall take place only 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 according to Sect. 6 VVG, for checking the insurer's obligation to perform or for internal checking of the settlement of accounts receivable in due time. It shall also take place to combat abuse or to fulfil legal obligations or for purposes of advertising or of market and opinion research.

(2) As a matter of principle, personal data shall be processed or used within the scope of the purpose known to the data subjects. Any alteration or extension of the purpose shall only take place if it is legally permitted and if the data subjects have been informed about it or if the data subjects have given their consent.

Art. 3 Principles regarding the quality of the collection, processing and use of data

(1) The undertakings shall collect, process or use all personal data in a lawful manner which meets the legitimate interests of the data subjects.

(2) The collection, processing and use of data shall be oriented towards the aim of data avoidance and data minimization, in particular, the possibilities of anonymization and pseudonymization shall be used where possible and where the effort involved is not disproportionate with regard to the purpose of protection pursued. In this respect, anonymization is to be preferred to pseudonymization.

(3) The controller shall ensure that existing personal data are stored accurately and kept up to date. Adequate measures shall be taken to ensure that inaccurate or incomplete data are rectified, erased or blocked.

(4) The measures taken according to paragraph 3, sentence 2 shall be documented. The relevant principles shall be included in the data protection concept of the undertakings (Article 4, paragraph 2).

Art. 4 Principles of data security

(1) To ensure data security, the required technical and organizational measures shall be taken with regard to the state of the art. The measures taken shall be suitable to ensure that

1. only authorized persons may gain knowledge of personal data (confidentiality),
2. personal data remain intact, complete and up to date during processing (integrity),
3. personal data are available in a timely manner and are processed properly (availability),
4. personal data may be attributed to their source at any time (authenticity),
5. it can be ascertained who has processed what personal data at what time and in which way (capability of revision),
6. the procedures used in processing personal data have been documented completely, in an up-to-date manner and in such a way that they can be reconstructed within a reasonable time (transparency).

These shall in particular be the measures contained in the Annex to Sect. 9, sentence 1 of the Federal Data Protection Act.

(2) The measures initiated at the undertakings shall be incorporated into a comprehensive data protection and data security concept, which regulates responsibilities and shall be developed with participation of the data protection officers of the undertakings.

Art. 5 Consent

(1) Where the collection, processing or use of personal data, in particular health data, is based on consent and – where required – on a declaration on release from confidentiality made by the data subjects, the undertaking shall ensure that this consent or declaration is based on the data subject's free decision, is effective and has not been revoked.

(2) Where the collection, processing or use 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. These declarations shall be obtained from the minor him- or herself, at the earliest after reaching the age of 16 years, provided the minor has the required capacity of discernment.

(3) The consent and the release from confidentiality can be revoked at any time with future effect. Where the consent is required for the performance of the contract or for claim settlement, any withdrawal shall be excluded according to the principles of good faith or shall result in the fact that the contractual obligation cannot be fulfilled. This restriction of the possibility of withdrawal shall not apply to any consent given orally.

(4) 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 collection, processing or use of data as well as about the possibility of refusing and revoking consent and the consequences thereof.

(5) As a matter of principle, the consent shall be obtained in writing in accordance with Sect. 126 of the German Civil Code (*Bürgerliches Gesetzbuch*). Where the consent is to be given together with other declarations, it shall be made distinguishable in a way that it catches the eye. In cases of special circumstances, such as in urgent situations or where the communication has been requested by the data subjects, and when obtaining consent in this manner is especially in the interest of the data subjects, the consent may also be given in

any form other than in writing, such as in text form (pursuant to Sect. 126b for example by means of e-mail, fax, text message, CD, USB stick, etc.) or orally.

(6) Where the consent is obtained orally, this shall be documented and confirmed to the data subjects with the next notification either in writing or in text form, if this is in line with the contract or the enquiry of the data subject. Where the confirmation is made in text form, the contents of the confirmation must have reached the data subject in a form that is reproducible without change.

(7) The consent may be given electronically, provided the contents of the declaration are confirmed in writing or – in accordance with paragraph 6, sentence 2 – in text form. In the case of electronic consent for the purpose of advertising, the confirmation may be omitted if the consent is recorded, if the data subjects may retrieve its contents at any time and if the consent may be revoked at any time with future effect. In the case of other forms of electronic consent, particularly for the purpose of the conclusion of a contract, the confirmation may be omitted if the submission of the declaration is recorded and if the contents have reached the data subjects in a form that is reproducible without change, such as through download, and if the data subjects have confirmed their receipt and their readability immediately afterwards, such as by clicking a box.

(8) Confirmation of the consent for advertising purposes in oral or electronic form shall be given no later than with the next notification. Any other consent given orally or electronically shall be confirmed in a timely manner.

Art. 6 Special categories of personal data

(1) As a matter of principle, special categories of personal data as defined in the Federal Data Protection Act (especially details on health) shall be collected, processed or used with the consent of the data subjects in accordance with Article 5 and – where required – on the basis of release from confidentiality. In this case the consent must explicitly refer to these data.

(2) In addition, special categories of personal data shall be collected, processed or used on a legal basis. This shall be admissible especially where it is necessary for the purpose of preventive medicine or health care within the scope of the accomplishment of tasks by private health insurance undertakings or where it is necessary to assert, exercise or defend legal claims – also within the scope of a legal dispute – and if there is no reason to assume that the data subject has an overriding legitimate interest in excluding such collection, processing or use.

IV. COLLECTION OF DATA

Art. 7 Collection of data from the data subjects, information requirements and rights, and collection of data from other persons

(1) As a matter of principle, personal data shall be collected from the data subjects themselves and subject to Sections 19 and 31 VVG.

(2) The undertakings shall ensure that the data subjects are informed about the identity of the controller (name, location), the purposes of the collection, processing or use of data and the categories of recipients. This information shall be provided prior to or at the latest at the time of the collection, unless the data subjects have already gained knowledge of it in some other way.

(3) The data subjects shall be advised of their rights laid down in Section VIII.

(4) Personal data of other persons within the meaning of this code of conduct shall be collected only where this is necessary for the establishment, performance or termination of the insurance relationship and if there are no indications that overriding legitimate interests of such persons are affected.

Art. 8 Data collection without participation of the data subjects

(1) By way of derogation from Article 7 paragraph 1, data shall be collected without participation of the data subjects only where this is necessary for the establishment, performance or termination of the insurance relationship or where the collection from the data subjects would involve disproportionate effort and if there are no indications that overriding legitimate interests of the data subjects are affected, especially if in the case of group insurance the policyholder permissibly supplies data of the insured persons or if in the case of life insurance the policyholder supplies data of the beneficiaries.

(2) The collection of health data from third parties shall take place – where required – with an effective declaration on release from confidentiality made by the data subjects and subject to Sect. 213 VVG.

(3) An undertaking which collects personal data without participation of the data subjects shall ensure that the data subjects are informed about the storage of data, the type of the data, the purpose of the collection, processing or use and the identity of the controller at the time of the first storage of such data. This information shall not be provided if the data subjects have gained knowledge of the storage in some other way, if data recorded for the controller's own purposes have been taken from generally accessible sources and if any notification would be disproportionate due to the multitude of cases concerned or if the data have to be kept secret according to a legal provision or by virtue of their nature, particularly because of the prevailing legal interest of a third party.

V. PROCESSING OF PERSONAL DATA

Art. 9 Joint processing of 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 and insureds as well as details on the type of existing contracts may be collected, processed or used for the purpose of centralized handling of specified procedural stages within the business process (e.g. telephone calls, mail, cash collection) within the scope of a data processing procedure jointly usable by members of the group, provided it is ensured that the technical and organizational measures meet the requirements under data protection law and that the controller responsible for the joint procedure complies with this code of conduct (particularly Articles 21 and 22).

(2) Master data of other persons shall be collected, processed and used within the scope of jointly usable data processing procedures only where this is necessary for the respective purpose. This shall be ensured both technically and organizationally.

(3) By way of derogation from paragraph 1, the insurance undertakings in the group may also use other data taken from applications and contracts of other undertakings in the group. This shall presuppose that this is necessary for the purpose of assessing the concrete risk of a new contract prior to its conclusion. The data subjects must have mentioned the existence of data in another undertaking in the group or must have assumed the existence of their data in another undertaking in the group in an apparent manner and given their consent to the data retrieval.

(4) Where a joint collection, processing or use of data takes place in accordance with paragraph 1, the insureds shall be informed of this in textual form upon conclusion of the contract or upon the establishment of such a procedure.

(5) The undertaking shall hold available an up-to-date list of all undertakings in the group participating in centralized handling and make it known in an appropriate form.

(6) Where an undertaking does any collection, processing or use of data on behalf of another member of the group, it shall comply with Article 21 or 22 of this code of conduct.

Art. 10 Rate and premium calculation

(1) The insurance industry calculates the probability of occurrence of insurance claims and their amounts of loss on the basis of statistics and empirical values and by means of actuarial methods and develops rates on this basis. For this purpose, the undertakings shall evaluate data from insurance relationships solely in an anonymized or – where this is insufficient for the aforementioned purposes – pseudonymized form.

(2) 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 calculation of intercompany statistics or for the purpose of rate calculation shall take place only in an anonymized or – where required – pseudonymized form. Any inference to the data subjects shall be ruled out.

(3) To determine the risk-appropriate premium, these rates are applied to the individual situation of the applicant. In addition, any assessment of the individual risk of the applicant by specialized risk assessors, such as physicians, may be included in the calculation of the premium. For this purpose, personal data collected within the scope of this code of conduct are also used.

Art. 11 Scoring

Scoring is governed by legal regulations, particularly Sect. 28b BDSG.

Art. 12 Data on creditworthiness

The collection, processing and use of data on creditworthiness is governed by legal regulations.

Art. 13 Automated individual decisions

(1) As a matter of principle, decisions which entail a negative legal or economic consequence for the data subjects or affect them significantly shall not be based exclusively on automated processing of personal data that serves to evaluate individual personality characteristics. This shall be ensured at the organizational level. As a matter of principle, information technology shall be used only as an aid to decision-making without being its only basis. This shall not apply where a request of the data subjects is fully met.

(2) If automated decisions are taken to the detriment of the data subjects, the data subjects shall be notified of this by the controller with reference to the right of access. Upon request, the logical structure of the automated processing and the essential reasons for this decision shall be communicated and explained to the data subjects so as to enable them to put forward their position. The information about the logical structure shall comprise the types of

data used as well as their relevance for the automated decision. The decision shall be reviewed on this basis in a procedure which is not exclusively automated.

(3) The use of automated aids to decision-making shall be documented.

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

(1) The undertakings of the German insurance industry – with the exception of private health insurers – use a detection and information system (*Hinweis- und Informationssystem - HIS*) to support risk assessment in the case of an application, for establishing the facts within the scope of claims assessment and for combating insurance fraud. The operation and use of HIS takes place subject to the regulations of the German Federal Data Protection Act on commercial data collection und recording for the purpose of transfer (information bureau).

(2) HIS is operated separately for each insurance line. In each line the stored data are processed separately in two data pools: in one data pool for retrieval for the purpose of risk assessment in the case of an application (*Antragsfall* = A pool) and in another pool for retrieval for the purpose of claims assessment (*Leistungsprüfung* = L pool). Accordingly, access authorizations are established by the undertakings for their staff members separately for each line or task.

(3) The undertakings shall report data on persons, vehicles or real estate to the operator of HIS according to defined reporting criteria if there is an increased risk or if there is a conspicuous fact which might suggest insurance fraud. Prior to any reporting of data concerning persons, the interests of the undertakings and those of the data subject shall be weighed against each other. If the defined reporting criteria are met, it may generally be assumed that the undertaking has a prevailing justified interest in the reporting. Special types of personal data, such as health data, shall not be reported to HIS.

(4) Upon conclusion of the contract, the undertakings shall already inform their policyholders in generalized fashion about HIS, indicating the controller and its contact details. At the time of the reporting, they shall notify the data subjects of the type of the data reported, the purpose of the reporting, the recipient of the data and the possible retrieval of the data.

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

(6) 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 the exclusion of the transfer. The data exchange shall be documented. Unless the data exchange takes place according to Article 15, the data subjects shall be informed about the data exchange. No information shall be required as long as the clarification of facts would be jeopardized by this or if the data subjects have gained knowledge of the data exchange in a different manner.

(7) Data recorded in HIS shall be erased no later than at the end of the 4th year after the prerequisite for the reporting has been met. The length of recording shall be extended to a maximum of 10 years in life insurance in the area of benefits or in the case of renewed reporting within the regular recording period according to Sentence 1. Data on applications where no contract has been concluded shall be erased in 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 shall publish a detailed manual on the use of HIS for the undertakings with due regard to the requirements under data protection law.

Art. 15 Clarification of contradictions

(1) If upon or after conclusion of the contract there are concrete indications for the insurer that inaccurate or incomplete data were provided at the time of the application or when data in the application were updated during the insurance relationship, thus influencing risk assessment, or that incorrect or incomplete details of the facts were provided at the assessment of a loss which has occurred, the undertaking shall carry out supplementary operations of data collection, processing or use where this is necessary to resolve contradictions.

(2) Supplementary data collection, processing or use to verify the details for risk assessment provided upon filing the application shall only take place within five years, in the case of health insurance within three years, of the date of conclusion of the contract. This period may be extended if the indications for a breach of the duty of disclosure do not become known to the undertaking until this period has expired by investigating a loss having occurred during this period. If there are concrete indications that the policyholder has intentionally or maliciously provided inaccurate or incomplete details upon filing the application, this period shall be extended to 10 years.

(3) If the supplementary collection, processing or use 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 declaration in the insurance application – prior to any data collection according to Sect. 213, paragraph 2 VVG 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.

Art. 16 Data exchange with other insurers

(1) A data exchange between a previous insurer and its subsequent insurer shall take place for the purpose of collection of rate-relevant or indemnity- or benefit-relevant details subject to Article 8, paragraph 1. This is particularly the case if the details are 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 provisions for increasing age in health insurance to the new insurer,
4. for complementing or verifying details provided by applicants or insureds.

In cases subject to 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 at the time of collection of the data. Following a data exchange for the purpose of claims or benefits assessment the data subjects are informed to the same extent. This shall be without prejudice to Article 15.

(2) In addition, any data exchange with other insurers outside the rules stipulated for the Detection and Information System of the Insurance Industry (HIS) shall take place where it is necessary for the assessment and handling of the 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 subrogation agreements and if there is no reason to assume that an overriding legitimate interest of the data subject conflicts with this.

(3) The data exchange shall be documented.

Art. 17 Data transfer to reinsurers

(1) To be able to meet their obligations arising from insurance relationships at any time, undertakings cede part of their risks from insurance contracts to reinsurers. In some cases, for

the purpose of further risk spreading, these reinsurers on their part make use of other reinsurers. 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 loadings, are disclosed in an anonymized or – where this is insufficient for the aforementioned purposes – pseudonymized form.

(2) Reinsurers are provided with personal data only where this is necessary and if there is no reason to assume that an overriding legitimate interest of the data subject conflicts with this. 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:

1. Risk and claims assessment are carried out by reinsurers in individual cases, e.g. in the case of high sums insured or in the case of a risk which is difficult to classify,
2. reinsurers assist undertakings in the area of risk and loss assessment and in evaluating procedures,
3. reinsurers are provided with lists of the portfolio of contracts covered by reinsurance to determine the scope of reinsurance contracts, including the check as to whether and to what amount they participate in the same risk (control of accumulation of risk) and for purposes of clearing,
4. risk and claims assessment carried out by the primary insurer is controlled by reinsurers by means of random checks to check their payment obligation vis-à-vis the direct insurer.

(3) The undertakings shall agree with reinsurers that personal data shall be used by these only for the purposes stated in paragraph 2. 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 controllers acting on their behalf to maintain silence with respect to such data.

(4) Special categories of personal data, especially health data, shall be transferred to reinsurers only if the prerequisites of Article 6 are met.

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

Art. 18 Use of data for purposes of advertising

Personal data shall be collected, processed or used for purposes of advertising only on the basis of Sect. 28, paragraphs 3 to 4 BDSG and subject to Section 7 of the German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb - UWG*).

Art. 19 Market and opinion research

(1) The undertakings shall engage in market and opinion research with special regard to the legitimate interests of the data subjects.

(2) Where the undertakings entrust other controllers with market and opinion research, the recipient shall be selected with proof of compliance with the data protection standard. Prior to the disclosure of data, the details of the research project shall be stipulated by contract subject to the requirements of Article 21 or 22. It shall be laid down, in particular:

a) that the data transferred and additionally collected shall be anonymized at the earliest possible date,

b) that the evaluation of the data and the transfer of the results of market and opinion research to the undertakings shall take place solely in anonymized form.

(3) Where the undertakings process or use personal data for the purpose of market and opinion research themselves, such data shall be anonymized at the earliest possible date. The results shall be recorded or used solely in anonymized form.

(4) Where commercial actions considered to be advertising take place within the scope of market and opinion research, for instance, where statements are made in the process of data collection for the purpose of sales promotion, the collection, processing and use of personal data is subject to the rules stipulated in Article 18.

Art. 20 Transfer of data to self-employed intermediaries

(1) Any transfer of personal data to the intermediary serving the customer shall take place only where it is necessary for the purpose of needs-based preparation or handling of a concrete application or contract or for the purpose of proper handling of the insurance matters of the data subject. Intermediaries shall be advised of their specific obligations of secrecy, such as professional or data secrecy.

(2) 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 insureds or applicants prior to 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. Any information by the previous insurance agent shall be considered equivalent to information by the undertaking. In the case of objection, the transfer of data, as a matter of principle, shall not take place. 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 if the proper service to insureds in individual cases or – due to an unexpected discontinuation of the service – the continuance of contractual relationships is at risk.

(4) Personal data of insureds or applicants may be transferred to an insurance broker if power of attorney has been conferred on the broker by such persons. For the case of change of the broker paragraph 2 shall apply accordingly.

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

VII. DATA PROCESSING ON BEHALF AND DELEGATION OF FUNCTIONS

Art. 21 Obligations with respect to data collection and processing on behalf

(1) Where an undertaking has personal data collected, processed or used on its behalf in accordance with Sect. 11 BDSG (e.g. electronic data processing, scanning and assigning of incoming mail, address administration, claims and benefits handling without independent leeway in decision-making, ensuring the correct booking of incoming payments, outgoing payments, non-autonomous cash collection, disposal of documents), the contractor shall be bound by contract at least in accordance with Sect. 11, paragraph 2 BDSG. The undertaking shall select only those processors that ensure all technical and organizational requirements and safeguards necessary for processing by taking appropriate measures. Prior to placing the order and thereafter at regular intervals, the undertaking shall make sure that the con-

tractor complies with the technical and organizational measures taken by it and shall document the results.

(2) Any data collection, processing or use shall only be admissible within the scope of the instructions issued by the undertaking. Contractual terms shall be submitted to the data protection officers, who shall provide advice, where required.

(3) The undertaking shall keep an up-to-date list of processors available. Where the systematic automated processing of personal data is not the main subject of the order, processors may be grouped into categories, specifying their task. This shall also apply to processors that act only once. The list shall be published in an appropriate form. Where personal data are collected from the data subjects, these shall, as a matter of principle, be informed about the list upon collection.

Art. 22 Delegation of functions to service providers

(1) The transfer of personal data to service providers for the fulfilment of tasks on the service provider's own responsibility shall take place where it is necessary for the purpose of the insurance relationship with the data subjects. This shall particularly be the case where experts are entrusted with the assessment of an insurance claim or where service providers are involved for the provision of contractually agreed insurance services comprising a benefit in kind (so-called assistance).

(2) The transfer of personal data to service providers for the accomplishment of tasks in the area of data processing or other tasks on the service provider's own responsibility may also take place where it is necessary to protect the justified interests of the undertaking and if there is no reason to assume that an overriding legitimate interest of the data subject conflicts with this. This may, for instance, be the case where service providers take over tasks which serve the purpose of carrying out transactions of the undertaking, such as risk assessment, claims and benefits handling, autonomous cash collection or handling legal cases, and where the prerequisites of paragraphs 4 to 7 are met.

(3) The transfer of personal data to service providers in accordance with paragraphs 1 and 2 shall be refrained from where the data subject objects to it and where it results from a check that the legitimate interest of the data subject overrides the interest of the transferring undertaking due to his or her specific personal situation. The data subjects shall be advised of this in an appropriate manner.

(4) The undertaking shall enter into a contractual agreement with service providers acting on its behalf, 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 a data protection and data security standard complying with this code of conduct;
- commitment of the service provider to provide the undertaking with any information required to fulfil an obligation to provide information, which remains with the undertaking, or to furnish information directly to the data subject.

This outsourcing of tasks shall be depicted in the register of procedures.

(5) The undertaking and the service provider shall additionally 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. The undertaking shall be held liable in the first instance for the damage vis-à-vis the data subjects. The parties shall 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.

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

(7) The undertaking shall ensure that the rights of access of the data subjects according to Article 23 are not curtailed due to the involvement of the service provider.

(8) Special categories of personal data may only be collected, processed or used in this context if the data subjects have given their consent or if the prerequisites according to Article 6, paragraph 2 are met. Where the undertakings are subject to an obligation of secrecy according to Sect. 203 StGB, they shall require service providers to maintain discretion 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 discretion with respect to such data.

VIII. RIGHTS OF DATA SUBJECTS

Art. 23 Right to information

(1) Data subjects may request information about data stored about them with the undertaking in writing, by telephone, by fax or electronic mail. They shall then be provided with information, in accordance with their request, as to what personal data are stored about them by the undertaking, their source and the purposes for which they are stored. In the case of an (envisaged) transfer, the data subjects shall also be provided with information about the third parties or the categories of third parties to which their data are (to be) transferred.

(2) This information may only be omitted if it would significantly jeopardize the business purposes of the undertaking, especially if due to specific circumstances there is an overriding interest in keeping a business secret, unless the interest in the information outweighs this threat or if the data have to 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.

(3) In the case of reinsurance (Article 17) or a delegation of functions to service providers (Article 22), the undertaking shall receive the requests for information and shall also furnish any information which the reinsurer or service provider is required to furnish or it shall ensure the provision of information by this entity.

Art. 24 Rights to rectification, erasure or blocking

(1) If personal data which have been stored prove to be inaccurate or incomplete, these shall be rectified.

(2) Personal data shall be erased without undue delay if the collection or processing has been inadmissible from the start, if the processing or use proves to be inadmissible due to circumstances having occurred subsequently or if knowledge of the data is no longer necessary for the controller to fulfil the purpose of the processing or use.

(3) The checking of the stored data with regard to the necessity of erasure according to paragraph 2 shall take place at regular intervals, at least once a year.

(4) Erasure shall be substituted by blocking where erasure conflicts with retention periods prescribed by law, statutes or contracts, where there is reason to assume that erasure would impair legitimate interests of the data subjects or that erasure is not possible or is only possible with disproportionate effort due to the specific type of storage. Personal data shall also be blocked if the data subject disputes that they are correct and it cannot be ascertained whether they are correct or incorrect.

(5) The undertaking shall notify the recipients, in particular reinsurers and insurance agents, of any rectification, erasure or blocking of data that is necessary.

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

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) Employees entrusted with the collection, processing or use of personal data shall be required to comply with data secrecy in accordance with Sect. 5 of the Federal Data Protection Act. 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. Any violations of data protection regulations for which specific employees may be made responsible may entail sanctions under labour law in accordance with applicable law.

(3) The obligation of employees to observe data secrecy shall extend beyond the end of the employment relationship.

Art. 26 Transparency

(1) Details about the automated data processing procedures used, which are subject to the obligation to notify vis-à-vis the data protection officers of the undertakings and have been recorded with these in the register of procedures, shall be made accessible upon request (Sect. 4e, sentence 1, no. 1 to 8 BDSG).

(2) Any information according to paragraph 1 and any information on data processing bodies, data processing procedures used or accession to this code of conduct which has to be made known in an appropriate form (Article 9, paragraph 5; Article 21, paragraph 3; Article 22, paragraph 6; Article 27, paragraph 5; Article 28, paragraph 1, sentence 2; Article 30, paragraph 1) shall be published on the Internet; in any case it shall be sent upon request either in writing (letter post) or in text form in line with the request (telefax, electronic mail). Article 23, paragraph 2, sentence 1 shall apply accordingly.

Art. 27 Data protection officers

(1) Every undertaking shall appoint a data protection officer in accordance with the regulations of the German Federal Data Protection Act as a body not bound by instructions and working towards compliance with applicable national and international data protection regulations and this code of conduct. The undertaking shall provide for the independence by contract.

(2) The data protection officers shall monitor the proper use of data processing programs used in the undertaking and for this purpose they shall be informed in time prior to the establishment or any significant alteration of a procedure used for automated data processing of personal data and shall collaborate in this in an advisory manner.

(3) 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. In this respect, they shall have an unrestricted right to monitor within the undertaking.

(4) The data protection officers shall familiarize persons engaged in the collection, processing or use of personal data with the respective special requirements in terms of data protection by taking appropriate measures.

(5) In addition, all data subjects may approach the data protection officers at any time by presenting suggestions, enquiries, requests for information or complaints related to issues of data protection or data security. Enquiries, requests and complaints shall be treated as confidential. 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 activity and trustfully cooperate with them to ensure compliance with applicable national and international data protection regulations and this code of conduct. To this effect, the data protection officers may trustfully consult with the respective responsible data protection authority at any time.

Art. 28 Complaints and reaction in cases of infringement

(1) The undertakings shall handle 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 14 days or send an interim notice. The contact details shall be made known in an appropriate form. If the responsible division is unable to take remedial action in a timely manner, it shall approach the data protection officer without delay.

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

(3) If this should exceptionally not take place, the data protection officers may approach the responsible data protection authority. They shall notify the data subjects of this specifying the competent supervisory authority.

Art. 29 Obligation to report unlawful access to data

(1) Where personal data have been unlawfully transferred under the conditions laid down in paragraph 2 or have been unlawfully revealed to third parties, the undertakings shall inform the responsible supervisory authority without undue delay. The data subjects shall be notified as soon as appropriate measures have been taken to protect the data or have not been taken without undue delay and criminal prosecution is no longer at risk. In cases where notification would require disproportionate effort, 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.

(2) Notification shall take place where personal data

a) are subject to professional secrecy, in particular data of an undertaking carrying on life, health or accident insurance, which are protected under Sect. 203 StGB,

b) are special categories of personal data, in particular health data,

c) relate to criminal acts, such as insurance fraud, or regulatory offences, such as under the German Road Traffic Act (*Straßenverkehrsgesetz*), or any suspicion in this respect or

d) concern bank or credit card accounts

and where there is a threat of serious harm to the data subjects' rights or legitimate interests. This can normally be assumed where these are in danger of suffering financial losses or significant social disadvantages.

(3) The undertakings shall require their data processors according to Sect. 11 BDSG to inform them without undue delay about any incidents covered by paragraphs 1 and 2.

(4) The undertakings shall develop a concept for handling incidents covered by paragraphs 1 and 2. They shall ensure that these become known to the management and to the data protection officer of the undertaking.

X. FORMALITIES

Art. 30 Requirement of accession and transitional provisions

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

(2) Where changes to data processing procedures are required within the undertakings to comply with this code of conduct, the undertakings shall submit to the competent supervisory authority within one year following accession a timetable for its implementation and shall report the completion following termination of the technical implementation by the end of the second calendar year following the year of accession.

(3) Policyholders whose contracts already existed prior to the accession of the undertaking to this code of conduct shall be informed about the entry into force of this code of conduct through the website of the undertaking and no later than with the next mail in text form.

Art. 31 Evaluation

This code of conduct shall be evaluated on the occasion of any change of law relating to its regulatory content concerning this change, but no later than five years following the completion of the review according to Sect. 38a, paragraph 2 BDSG as a whole.