Code of Conduct for the Processing of Personal Data by Insurers

VERBOND VAN VERZEKERAARS

Content

Introduction and Structure of the Code

Every Dutch person and every company is a customer of an insurer, whether this concerns compulsory liability insurance, voluntary travel insurance, or life assurance. Insurances are based on one simple principle: by sharing risks with a large group of people, as a group we are better armed in case of adversity. This solidarity is the pillar on which insurance is built and is reflected in the core values of the 95% of Dutch Insurers who are members of the Dutch Association of Insurers (*Verbond van Verzekeraars*, hereinafter referred to as the *'Association'*).

For centuries, the analysis of information has been indispensable in making insurance effective, fair and affordable. Information about the customer and trends in society enables insurers to better assess risks, determine the premium of the insurance, assess insurance claims, prevent or limit damage, and provide a better and more tailored service to the customer. Insurers are also required by law to know the customer, to provide accurate information about products and to prevent and combat insurance fraud and money laundering.

These days, the processing of personal data, data that can be traced back to individuals, is increasingly important for insurers: new techniques, such as computer-controlled analysis of large amounts of data ('big data analysis'), enable insurers not only to recognise risks in society earlier and to operate more effectively, but also to provide their customers more tailor-made services. At the same time, the processing of information can have an impact on customer privacy. For insurers, the protection of privacy is not only a legal obligation, but also a prerequisite for consumer confidence and sound business operations.

The protection of personal data is becoming increasingly important. Insurers notice that customers are increasingly asking more questions about privacy and that the world around us is rapidly innovating and digitising. Virtually everything and everyone generates data all the time, whether it is by driving a new car or surfing the internet. New technology also offers opportunities to give customers more control over their personal data, make tailored offers, and prevent car accidents by giving customers discounts on their premium for responsible driving.

In recent years, the legislation and regulations governing the processing of personal data have changed drastically. The new European General Data Protection Regulation (GDPR) has improved and extended the rules for personal data protection standards. These new rules became applicable throughout Europe on 25 May 2018. In the Netherlands, financial legislation is also in a state of flux and insurers are required by law to know increasingly more about their customers and to actively guide their customers in their choices regarding insurance products.

This Code of Conduct for the Processing of Personal Data by Insurers ('Code of Conduct') translates general legislation and regulations for insurers into specific ground rules for the insurance industry. Because these general laws and regulations apply to all organisations that process personal data, the GDPR encourages the drafting of such codes of conduct to make it clear to companies and customers how personal data are processed in a certain industry. The Dutch Government welcomed the initiative taken by the Association to adopt a new Code of Conduct[1].

[1] In a letter submitted by the Minister of Finance to the Lower House of Parliament on 9 February 2018: https://zoek.officielebekendmakingen.nl/kst- 34616-3.html

By introducing this Code of Conduct, the Association aims to link up with these social, technological, and legal developments. This new Code of Conduct replaces the old Code of Conduct for the Processing of personal data by Financial Institutions, which applied to all financial institutions, including banks. This Code of Conduct, which only applies to the insurance industry, will not only enable the industry to work out exactly what the new legislation and regulations mean, but will also enable the industry to respond better to changes in society and to better inform customers about the handling of personal data.

Structure of the Code

The Code of Conduct is not intended as a summary of current legislation and regulations, but as an elaboration of these for the insurance industry. Certain subjects have not been taken into consideration because the legislation and regulations already clearly describe what insurers are required to do. One example of this is the reporting of data leaks. The GDPR, the Policy Rules of the Dutch Data Protection Authority (DPA) and financial legislation describe exactly in which situations Insurers must report IT Incidents, and to whom. These subjects are briefly described in this Code of Conduct, allowing insurers, the customer, and the rest of society to see that these subjects must also be complied with by insurers.

Other subjects in the Code of Conduct are dealt with in more detail because they are unique to the insurance industry. Two of the most important topics are the analysis of information by insurers to determine the premium and to ensure the security and integrity of the industry, for example to prevent insurance fraud. These topics are discussed in detail in Section 4 Code of Conduct. Because the topics can be complex for customers, the Code of Conduct also contains graphical road maps of what insurers do in this area. These 'infographics' on applying for insurance and preventing and combating insurance fraud and other forms of insurance crime are included in the appendix to the Code of Conduct.

As the Code of Conduct elaborates general standards and rules referred to in the legislation and regulations, the provisions sometimes need to be explained. That is why the Code of Conduct contains a detailed explanation, explaining the provisions one by one. In some cases, the Code of Conduct refers to definitions from laws and regulations, such as: ‘Controller’ and ‘Processor’. These terms are written with a capital letter and defined in Section 10 Code of Conduct.

Should you have any questions or comments after reading this Code of Conduct, the Association will be pleased to hear from you. In that case, please contact info@verzekeraars.nl.

1. Considerations

1.1.1 Insurers process Personal Data in accordance with applicable laws and regulations for the protection of Personal Data. This Code of Conduct for the Processing of Personal Data underlines the importance Insurers attach to transparent, safe, and careful Processing of Personal Data in their own industry. Insurers comply with the provisions of this Code of Conduct in their external and internal privacy policies and business operations.

1.1.2 The purpose of this Code of Conduct is:

(a) to further elaborate the applicable legislation and regulations for the Processing of Personal Data for Insurers and for data processing in the industry, and

(b) to provide transparency to customers and society about the Processing of Personal Data by Insurers.

1.1.3 This version of the Code of Conduct replaces all previous codes of conduct for the Processing of Personal Data for Insurers, including the 2010 Code of Conduct for the Processing of Personal Data by Financial Institutions.

2. Scope and Application

2.1 Insurers

2.1.1 The members of the Association are bound by this Code of Conduct when carrying on insurance business. Insurers who are not members of the Association may voluntarily declare that they adhere to this Code of Conduct. They will then also be bound by this Code of Conduct when carrying on their insurance business. When contracting out tasks to authorised representatives or other service providers, Insurers will impose compliance with this Code of Conduct in a mutual agreement. Healthcare Insurers bound by the Code of Conduct for the Processing of Personal Data by Healthcare Insurance Companies are subject to the latter Code of Conduct when the healthcare insurance company is conducting business.

2.2 Application

2.2.1 The Code of Conduct applies to the partly or fully automated Processing of Personal Data by Insurers as part of their business operations. The Code of Conduct also applies to the manual Processing of Personal Data by Insurers as part of their business operations, in so far as these data have been included in a file or is intended to be included therein.

2.2.2 The Code of Conduct does not apply to the Processing of Personal Data:

(a) in the Insurers' Incidents Register and related External Reference Register (EVR). The Incident Warning System Protocol for Financial Institutions (PIFI) applies to this.

(b) in the employment relationship of Insurers with their employees.

3. Principles

3.1 General

3.1.1 Insurers process Personal Data in accordance with applicable legislation and regulations. They respect the principles of proportionality, subsidiarity and confidentiality and process Personal Data in a transparent, proper and careful manner.

3.2 Processing principles

3.2.1 Insurers base each Processing of Personal Data on a principle laid down in applicable legislation and regulations. The Code of Conduct contains a more detailed elaboration of the legal bases laid down in legislation and regulations for the Processing of Personal Data by Insurers.

3.3 Collection of Personal Data

3.3.1 Insurers collect Personal Data for specific and explicitly defined purposes. Some of these purposes have been described in more detail in Article 4 of this Code of Conduct. In addition, Insurers may process Personal Data for other purposes in accordance with applicable legislation and regulations. Insurers state the purposes of Processing and the sources of Personal Data in a privacy policy.

3.4 Quality of Processing of Personal Data

3.4.1 Insurers limit the Processing to Personal Data that are reasonably necessary and relevant for the purposes of the Processing in question. They pursue a policy pertaining to the accuracy of Personal Data, the retention periods, the recording of Processing in a processing register intended for that purpose, and the removal of Personal Data.

3.5 Rights of the Data Subject

3.5.1 Insurers respect the rights of the Data Subject with regard to the Processing of Personal Data. These rights are set out in more detail in Article 6 Code of Conduct.

3.6 Urgent Reason

3.6.1 Insurers may deviate from these general principles if there is an Urgent Reason. This Urgent Reason is set out in more detail in Article 8 Code of Conduct.

4. Purposes

4.1 General

4.1.1 Insurers state the purposes of the Processing of Personal Data in their privacy policy. Article 4 describes in more detail the common purposes of the Processing of Personal Data by Insurers.

4.1.2 Insurers carry out a data protection impact assessment (DPIA) as referred to in Article 7.4 as soon as they further process Personal Data for purposes other than those set out in the privacy policy and such further processing is likely to pose a high risk to the rights and freedoms of natural persons with regard to the nature, scope, context, and purposes of processing. Such further Processing of Personal Data is only permitted if the new purpose is related to the original purpose of the Processing and if the nature of the Personal Data and the consequences for the Complainant do not preclude further Processing. Insurers

inform the Data Subject of the new Processing of Personal Data in accordance with Section 6 Code of Conduct.

4.2 Effecting and implementing insurance policies

4.2.1 Insurers process Personal Data to effect and implement insurance policies. Insurers may provide Third Parties with Personal Data to the extent reasonably necessary to effect and implement insurance policies. The Processing of Health Data and Criminal Records to effect and implement insurance policies will take place in accordance with Articles 5.1 and 5.2 Code of Conduct.

4.2.2 Insurers may carry out fully automated Processing of Personal Data, such as profiling, to be able to take a decision in respect of effecting or implementing insurance policies. Such Processing will only take place if the decision and the Processing:

(a) are necessary to effect or implement the insurance policy; or

(b) are based on the express consent of the Data Subject; or

(c) are to perform a public duty or a legal obligation.

The Insurer informs the Data Subject of the new Processing of Personal Data in accordance with Section 6 Code of Conduct. The Data Subject may: make its views known on the decision, challenge the decision, request the Insurer to explain a decision with human involvement, and have it reconsidered by a human being. Prior to the fully automated decision-making, an Insurer carries out a DPIA in accordance with Article 7.4 Code of Conduct. The Insurer periodically evaluates the automated decision-making process to ensure compliance with the general principles set out in Section 3 Code of Conduct.

4.3 Analyses for historical, statistical and scientific purposes

4.3.1 Insurers may process Personal Data for historical, statistical, or scientific purposes. In accordance with Article 7.4, Insurers carry out a DPIA to map out the impact on the privacy of the Data Subject and to take protective measures. Insurers may analyse archived Personal Data for this purpose in accordance with Article 7.5 Code of Conduct.

4.3.2 Insurers may use the results of historical, statistical, and scientific analysis to draw up group profiles. Insurers must anonymise or pseudonymise the Personal Data on which the analysis is based for the purpose of drawing up group profiles in accordance with Article 7.6 Code of Conduct.

4.3.3 Insurers may process Special Personal Data for scientific, historical and statistical purposes. The Processing must be necessary to carry out a specific analysis and to comply with the other conditions of Article 5 Code of Conduct. Furthermore, the Insurer also carries out a DPIA before the Processing in accordance with Article 7.4 Code of Conduct. The Insurer takes appropriate action to protect the privacy of the Data Subject.

4.4 Marketing activities and customer relationship management

4.4.1 Insurers may process Personal Data for marketing activities and customer relationship management. When Processing Personal Data for marketing purposes that Insurers have not collected directly from the Data Subject, they will inform the Data Subject in accordance with Article 6.1.1 of the Code of Conduct. The Insurer stops the Processing for marketing activities when the Data Subject indicates that its Personal Data may not be used for this purpose.

4.4.2 Insurers may approach the Parties Concerned through various channels for Direct Marketing.

(a) When using automatic calling systems without human involvement or electronic messages, Insurers may only contact Data Subjects directly for marketing purposes if the Data Subject has given prior consent ('opt-in') or if the Data Subject has provided contact details when purchasing a product or for the provision of a service.

(b) The use of other techniques, including 'regular' post for Direct Marketing, is permitted, unless the Data Subject indicates that it does not wish to receive such Direct Marketing ('opt-out').

The Data Subject may at any time grant or withdraw the aforementioned opt-in permission or opt-out free of charge.

4.4.3 Prior to the further Processing of Personal Data for Direct Marketing activities, Insurers must carry out a DPIA based on previously drawn up group profiles in accordance with Article 4.3.2. Code of Conduct if the criteria set out in Article 7.4. Code of Conduct have been met. If the result of the DPIA so requires, Insurers must anonymise or pseudonymise the Personal Data underlying the development of new products and services in accordance with Article 7.6 Code of Conduct.

4.4.4 Insurers will process Special Personal Data only for Direct Marketing purposes and after having obtained the explicit consent of the Data Subject.

4.5 Integrity and safety of services

4.5.1 Insurers process Personal Data to guarantee the integrity and security of the services provided by the Insurer, the Group to which the Insurer belongs and the insurance industry. To this end, they take measures, including carrying out an internal audit, setting up an Incidents Register, and possibly participate in other warning systems.

4.5.2 An audit focuses on the actions of Insurers or Third Parties they engaged. The Insurers must put appropriate safeguards in place to protect the Personal Data of the Data Subject during the investigation by the Insurer or the Third Parties it engaged. An audit report does not contain any Personal Data.

4.5.3 Insurers keep Incident Records to ensure the safety and integrity of services and the industry. Insurers inform the Parties Concerned about the existence and possibility of Processing Personal Data in this context. The IT Security department or another department designated for this purpose at an Insurer may decide to include the Personal Data from the Incident Records in an Internal Reference Register (IVR). In the Internal Reference Register Insurers only include Personal Data of natural or legal persons who pose a risk to the safety or integrity of the Insurer or the Group to which the Insurer belongs. If an incident meets the criteria of the

PIFI, Insurers must include the relevant Personal Data in an Incidents Register and, where applicable, the External Referral Register. In accordance with Article 2.2.2 of the Code of Conduct, the PIFI applies to this Processing.

4.6 Legislative and regulatory requirements

4.6.1 In certain cases, Insurers are required by law, regulations or industry supervisors to collect, process or share the Personal Data of a Data Subject with competent authorities.

5. Special Personal Data

5.1 Health Data

5.1.1 The Insurer only processes Health Data if:

(a) the Data Subject has given express consent; or

(b) this is necessary to assess and accept a Data Subject or Third Party and to implement an insurance policy. The Insurer may ask for Health Data in so far as these are reasonably necessary to effect and implement insurance policies. The Insurer may not use Health Data provided by the Data Subject to the Medical Adviser ('MA') in connection with an insurance for another insurance, unless the Data Subject has given explicit permission to do so; or

(c) to ensure the safety and integrity of the industry in accordance with Article 4.5 Code of Conduct; or

(d) the Processing relates to Health Data which the Data Subject appears to have disclosed itself; or

(e) this is necessary in view of an overriding public interest and the Insurer provides appropriate safeguards to protect the privacy of the Data Subject; or

(f) the Dutch DPA has granted a licence for the Processing; or

(g) this is necessary for historical, statistical or scientific purposes, in accordance with Article 4.3.3 of the Code of Conduct; or

(h) this is necessary for the establishment, exercise or defence of the Insurer's interests in dispute resolution; or

(i) compliance with legislation and regulations requires or permits this.

5.1.2 Prior to a category of new Processing of Health Data and major adaptations of an existing Health Data Processing category, the Insurer determines whether a DPIA should be carried out in accordance with the criteria set out in Article 7.4 Code of Conduct.

5.1.3 Only the Medical Adviser (MA) and the support staff to be appointed by the Adviser within the medical department or staff under the Adviser's direct functional and medical disciplinary responsibility may process Health Data for drawing up medical opinions. The MA, supported by their medical service or staff, may request additional Health Data for this purpose from the Data Subject. The MA may collect Health Data from other sources with the explicit consent and, if necessary, with the authorisation of the Data Subject. The authorisation is not of a

general nature but focuses on specific Processing for a specific case. The authorisation also contains information on the nature of the data to be requested, the purpose of the Processing, and the rights of the Data Subject in accordance with the provisions of Article 6 of the Code of Conduct.

5.1.4 The MA is responsible for the management of the Data Subject's medical file. The medical file may contain the following information:

(a) information provided by the Data Subject, such as the health certificate of the Data Subject, information from the treating physicians and other practitioners;

(b) the details of the occupational health and safety services or company doctor;

(c) the authorisation for the Processing of Health Data;

(d) reports drawn up by an examining physician in connection with the taking out or implementation of the insurance policies.

The MA and persons under their responsibility are not responsible for the Processing of Health Data by the (i) underwriter and Claims Handler (CH); (ii) persons within the Insurer who have obtained Health Data directly from the Data Subject at the same time as reporting a claim or damage, if these Health Data are necessary for further assessment of this, and (iii) the Data Subject who, due to its state of health, has requested the Processing.

5.1.5 In accordance with Article 6.2 Code of Conduct, the Data Subject is entitled to inspect the Processing of Personal Data in the medical file. The MA may block out passages from the medical file to protect the interests of Third Parties when complying with the request for inspection by the Data Subject.

5.1.6 Persons who process Health Data for or on behalf of Insurers are obliged to maintain confidentiality by virtue of their office, profession, statutory regulation, or by agreement.

5.2 Criminal Record Data

5.2.1 The Insurer only processes Criminal Record Data if:

(a) the Data Subject has given express consent; or

(b) this is necessary to assess and accept a Data Subject as an Insured and to implement an insurance policy. The Insurer may ask the Data Subject about the existence of criminal offences and a criminal past of the prospective Insured and co-insured persons (including directors and shareholders of legal persons); or

(c) to ensure the safety and integrity of the industry in accordance with Article 4.5 of the Code of Conduct; or

(d) the Processing relates to Criminal Record Data which the Data Subject appears to have disclosed itself; or

(e) this is necessary in view of an overriding public interest and the Insurer provides appropriate safeguards to protect the privacy of the Data Subject; or

(f) the Dutch DPA has granted a licence for the Processing; or

(g) this is necessary for historical, statistical, or scientific purposes, in accordance with Article 4.3.3 Code of Conduct; or

(h) this is necessary for the establishment, exercise, or defence of the Insurer's interests in dispute resolution; or

(i) compliance with legislation and regulations requires this.

5.2.2 Prior to a category of new Processing of Criminal Record Data and important adaptations of an existing category of Processing of Criminal Record Data, the Insurer must determine whether a DPIA should be carried out, in accordance with the criteria of Article 7.4 Code of Conduct.

5.2.3 Insurers can only provide Criminal Record Data to employees of Group companies if access to this data is necessary to perform their duties or to subsequently provide the data to investigative services. This provision within Group companies is limited to:

(a) Personal Data relating to offences committed, or based on facts and circumstances are expected to be committed, against the Group; or

(b) Personal Data that may prove unlawful acts against the Group.

5.3 Other Special Personal Data

5.3.1 Insurers are permitted to process Special Personal Data other than Health Data or Criminal Record Data only if:

(a) the Data Subject has given express consent; or

(b) the Processing is necessary to establish, exercise, or defend the Insurer's interests in court; or

(c) to ensure the safety and integrity of the industry in accordance with Article 4.5 of the Code of Conduct; or

(d) the Processing relates to Health Data which the Data Subject appears to have disclosed itself; or

(e) this is necessary in view of an overriding public interest and the Insurer provides appropriate safeguards to protect the privacy of the Data Subject; or

(f) the Dutch DPA has granted a licence for the Processing; or

(g) compliance with legislation and regulations requires this.

5.3.2 Prior to a category of new Processing of Special Personal Data and important adaptations of an existing category of Processing of Special Personal Data, the Insurer must determine whether a DPIA should be carried out, in accordance with the criteria of Article 7.4 Code of Conduct.

6. Rights of the Data Subject

6.1 Information on Processing Personal Data

6.1.1 Insurers inform the Data Subject about the Processing of Personal Data, allowing the Data Subject to assess the Processing and claim the rights referred to in this chapter. If Insurers collect Personal Data from the Data Subject, they will inform the Data Subject in full and before collecting Personal Data. If Personal Data are collected through other channels or from sources other than directly from the Data Subject, Insurers must inform the Data Subject within one month of the collection or prior to the collection in their external privacy statement.

6.1.2 The Insurer can only omit this obligation to provide information if this proves impossible in practice, requires disproportionate effort, or if the Data Subject is already aware of the Processing. Furthermore, the Insurer may have a reasonable interest in not yet informing the Data Subject or there may be an Urgent Reason in accordance with Article 8 Code of Conduct. Insurers will then assess on the basis of the general principles of Article 3.1 Code of Conduct whether they will still inform the Data Subject afterwards.

6.1.3 Insurers inform the Data Subjects on the Processing of Personal Data in a transparent manner and in understandable language. Insurers refer to this Code of Conduct in their external privacy statements. The external privacy statement can be consulted on the Insurers' website.

6.1.4 Prior to a Processing for a purpose other than that for which the Personal Data was collected, Insurers will inform the Data Subject of the other purpose and the Personal Data concerned.

6.1.5 As soon as the Insurers take a decision regarding a Data Subject that is based on automated processing of Personal Data and that may significantly affect the Data Subject, they will provide the Data Subject with information about the existence, importance, logic, and expected consequences of such Processing. The information provided is as concrete and practical as possible, allowing the Data Subject to develop a clear picture of the possible consequences of the decision.

6.2 Inspection Processing of Personal Data

6.2.1 Data Subjects have the right to request Insurers in writing to provide an overview of the Personal Data processed. In addition, Insurers provide the Data Subject with information on categories required by law, such as the purposes of processing, any recipients and sources of Personal Data, safeguards in place for the protection of Personal Data, the existence of fully automated processing operations and, if possible, the retention periods of Personal Data. If Personal Data are processed outside the European Union, Insurers must provide information on the safeguards in place for the protection of Personal Data. The overview also contains information about the other rights that the Data Subjects enjoy on the basis of this chapter of the Code of Conduct.

6.2.2 Insurers must respond to the request for inspection by the Data Subject with reasons and within one month. If the Insurer does not process any Personal Data of the Data Subject, the Insurer informs the Data Subject accordingly within one month of receipt of the request. If the Data Subject requests the summary electronically, the Insurer will send the summary to the Data Subject in electronic form, unless the Data Subject explicitly requests another form or the security of the Personal Data cannot be guaranteed. Insurers may charge a reasonable fee if

the Data Subject requests additional copies of the summary.

6.2.3 Insurers may refuse the request for inspection by a Data Subject if there is an Urgent Reason, if the protection of the Personal Data of Third Parties justifies it, or if intellectual property rights or trade secrets of the Insurers are disproportionately affected by the provision of the Personal Data.

6.2.4 If the Insurer is responsible for establishing the identity of the Data Subject, the Insurer will request the Data Subject to identify itself before complying with the request for inspection, unless identification has already taken place.

6.3 Correction, objection, restriction, and deletion of Personal Data

6.3.1 If the Insurer processes incorrect or incomplete Personal Data, the Data Subject has the right to correct or supplement the Personal Data concerned. If the Personal Data are processed in breach of this Code of Conduct or statutory regulations, the Data Subject will have the right to restrict or remove the Personal Data in question, unless the interests of an Insured or a Third Party are disproportionately harmed as a result. Insurers will respond to a written request from the Data Subject for correction, objection, restriction, or deletion, stating the reasons, and as a general rule within one month. The Insurer may ask the Data Subject to state the reasons for its request.

6.3.2 The Data Subject has the right to object in writing to the Processing of Personal Data by the Insurer or a Third Party to whom the Personal Data are provided. The right to object only applies if the Insurer processes Personal Data on the basis of the Insurer's legitimate interests. Insurers must respond to the objection by the Data Subject with reasons and within one month. If the Data Subject's objection is justified, the Insurer will terminate the Processing of Personal Data immediately. As long as it is not clear whether the Data Subject has submitted a justified request to the Insurer, the Insurer will restrict the Processing of the Personal Data concerned. If the Data Subject objects to Processing for Direct Marketing by an Insurer, the Insurer will refrain from such Processing. To this end, the Insurer will save the Data Subject's objection as a document in an internal register.

6.3.3 If the Insurer is responsible for establishing the identity of the Data Subject, the Insurer will request the Data Subject to identify itself before complying with a request based on this paragraph, unless identification has already taken place.

6.4 Data portability

6.4.1 At the request of the Data Subject, Insurers will assist the Data Subject in moving Personal Data to another Insurer or Controller. The Data Subject's request may relate to the Personal Data provided by the Data Subject to the Insurer and which the Insurer processes on the basis of the express consent of the Data Subject or to implement the insurance policy. Insurers will protect the rights of Third Parties when complying with a request to move Personal Data of the Data Subject.

6.4.2 Insurers will provide the Personal Data in a form that is comprehensible to the Data Subject and the receiving Controller. The sending Insurer will not send any Personal Data from which receiving Controller can trace profiles of the Data Subject or business secrets. The receiving Controller is responsible for the Personal Data received and is obliged to ensure the protection of the Data Subject's rights. Insurers undertake to develop common standards that promote

the right to move within the industry.

6.4.3 If the Insurer is responsible for establishing the identity of the Data Subject, the Insurer will request the Data Subject to identify itself before complying with a request based on this paragraph, unless identification has already taken place.

7. Special Subjects

7.1 Collecting data via equipment Data Subject

7.1.1 Insurers place data, including cookies, on the Data Subject's equipment to collect data from the Data Subject to provide a service that has been requested. In all other cases, an Insurer will only collect such data after the Data Subject has been informed in a transparent manner and in understandable language in accordance with Article 6.1.1 Code of Conduct. If an Insurer collects Personal Data of the Data Subject via such data for marketing activities, the Data Subject is given the opportunity to refuse the Processing. Insurers may only use the Personal Data collected for marketing activities in accordance with Article 4.4 Code of Conduct. Insurers will draw up a policy for the collection of Personal Data and other data on the Data Subject's peripheral equipment.

7.2 Security

7.2.1 Insurers are aware of the crucial importance of Personal Data security for the Data Subject. Personal Data of the Data Subject are secured by appropriate technical and organisational means which are set out in a security policy. Insurers not only comply with the requirements of applicable legislation and regulations regarding the protection of Personal Data, but also with the requirements of the Information Security Assessment Framework of the Dutch Central Bank (‘DNB’), which contains specific and strict security standards for the financial industry.

7.3 Data leaks

7.3.1 Insurers must report a data breach to the Dutch DPA without unreasonable delay and, if possible, within 72 hours of becoming aware of it. Insurers may, if necessary or desirable, report a data breach to the Data Subject based on the duty of care under the Dutch Financial Supervision Act (Wft).

7.4 DPIA

7.4.1 Prior to a category of new processes and major changes to an existing category of processes, Insurers determine whether they wish to carry out a DPIA. Insurers will make a DPIA if the Processing is likely to pose a high risk to the rights and freedoms of the Data Subject, considering the nature, scope, context, and purposes of the Processing.

7.4.2 A DPIA contains an analysis of the intended Processing, the purposes, necessity, principles, possible risks for the Data Subject, and guarantees issued by the Insurer to mitigate any risks. If appropriate, the Insurer seeks advice from the Data Protection Officer when carrying out a DPIA.

7.5 Policy on retention of Personal Data

7.5.1 Insurers have a policy with regard to the retention of Personal Data. They retain Personal Data

for specific purposes and until the retention periods set out in the retention policy have expired. After expiry of the retention period, Insurers will destroy, anonymise, pseudonymise, or transfer the Personal Data to a destination for archive management and to ensure dispute resolution. Insurers may analyse archived Personal Data for historical, statistical or scientific analysis. Insurers process such Personal Data in accordance with Article 4.3 Code of Conduct.

7.6 Pseudonymisation

7.6.1 After pseudonymisation of Personal Data, Insurers take measures to prevent unauthorised re-identification of the Data Subjects. Insurers keep the Personal Data that can be linked to information in the pseudonymous dataset separately, appoint the employees responsible for the pseudonymisation and specify these measures in a policy plan. If Insurers re-identify the Data Subjects included in the pseudonymous dataset for commercial purposes, this is a type of Processing that requires a new basis. The Code of Conduct applies in full to this new Processing.

7.7 Recording of electronic communications

7.7.1 Insurers may record electronic communications for in particular the following purposes:

(a) to effect and implement an insurance policy; or

(b) to provide proof and to assess differences of interpretation or disagreement about the content of the communication; or

(c) to detect and investigate fraud and other possible irregularities; or

(d) to evaluate the quality of the service; or

(e) for training, coaching and assessment purposes; or

(f) for marketing purposes; or

(g) to comply with legislation and regulations.

Electronic communication includes telephone calls, email, chat messages, and other forms of communication between the Insurer and the Data Subject via electronic media.

7.7.2 The recording of electronic communications by Insurers must meet the following criteria:

(a) Strict retention period. Insurers do not retain communications any longer than necessary for the purposes set out in Article 7.8.1 Code of Conduct. The retention period may differ for each purpose. In accordance with Article 7.5 Code of Conduct, Insurers will lay down the retention period in a policy.

(b) Suitable Security. Insurers ensure that communications are not accessible to unauthorised persons, cannot be manipulated and are traceable in secure information systems.

(c) Disclosure. Insurers will ensure that the way the communication is recorded is clearly disclosed to the Data Subject.

7.7.3 A Data Subject has the right to a copy or transcription of a recorded telephone conversation. To this end, the Data Subject must provide the Insurer with such sufficient information that the Insurer can trace the recording.

7.8 Camera surveillance

7.8.1 Insurers may use camera surveillance if this is required for the following purposes:

(a) to protect buildings, land, employees, goods, information and other significant interests of the Insurer, the Data Subject and Third Parties; or

(b) to prevent, detect and investigate criminal offences and breaches of company rules; or

(c) to support legal proceedings.

7.8.2 The use of camera surveillance by Insurers must meet the following criteria:

(a) Selectivity. Insurers select locations for the purposes set out in Article 7.7.1 Code of Conduct.

(b) Retention Period. Insurers do not retain the Personal Data and camera images obtained for longer than necessary for the purposes described in Article 7.7.1 Code of Conduct.

The retention period may differ for each purpose. In accordance with Article 7.5 Code of Conduct, Insurers will lay down the retention period in a policy.

(c) Suitable Security. Insurers guarantee that the information is included in secure information systems.

(d) Disclosure. Insurers guarantee that the use of camera surveillance is clearly indicated, unless this use is intended for the purposes referred to in Article 7.7.1(b-c).

7.8.3 In response to a request for inspection, the Insurer may ask the Data Subject to specify the place, date, and time of the recording. The Insurer will grant the request for inspection, unless there is an Urgent Reason as set out in Article 8 Code of Conduct.

7.9 Processing agreement

7.9.1 If Insurers engage Processors who process Personal Data for the Insurer, Insurers will ensure that these external organisations comply with the principles of this Code of Conduct and the applicable laws and regulations. Insurers must enter into a processing agreement for this purpose. This processing agreement will include all the obligations that a Processor must perform under the applicable laws and regulations.

7.10 Transfer of Personal Data outside the European Economic Area

7.10.1 If Insurers process Personal Data outside the European Economic Area, for example in the case of Processing by a Processor or a Group Company, the Insurer guarantees that the Personal Data of the Data Subject will enjoy adequate protection in accordance with applicable laws and regulations and the Code of Conduct.

7.11 Group companies

7.11.1 Insurers may process Personal Data within the Group, if the other provisions of the Code of Conduct are complied with. In particular in accordance with Article 6.1.1 Code of Conduct, the Data Subject must have received sufficient information that the Insurer and the Group Company are part of one and the same Group

8. Urgent Reason

8.1.1 Insurers may deviate from the general principles of the Code of Conduct if there is an Urgent Reason. Based on the specific facts and circumstances of the case, the Insurer will assess whether the Urgent Reason outweighs the protection of the rights and freedoms of the Data Subject. Insurers will apply this exception to the Code of Conduct strictly within the framework of:

(a) preventing, detecting, investigating and prosecuting breaches of laws, regulations or business rules of Insurers – including cooperation with relevant authorities.

(b) protecting and defending the rights and freedoms of the Insurer, the staff or other persons – including the Data Subject or a Third Party – such as:

(i) the safety of persons, Insurers, and the industry; or

(ii) trade secrets and Insurers' reputation; or

(iii) the continuity and integrity of the services of Insurers and of the industry; or

(iv) the involvement of advisers in such areas as law, taxation and insurance.

9. Compliance with Code of Conduct

9.1 Data Protection Officer

9.1.1 Insurers will, in principle, appoint a Data Protection Officer (DPO). The DPO is an expert, an independent professional who advises the Insurer from within on the protection of Personal Data and monitors compliance with the Code of Conduct and dispute resolution in accordance with Article 9.3.1. of the Code of Conduct. Insurers must enable the DPO to perform their duties properly. Insurers may refrain from appointing a DPO if the nature of the services or products gives cause to do so.

9.2 Internal Investigations

9.2.1 Insurers underline the importance of proper compliance with the Code of Conduct by periodically ordering internal investigations. These internal investigations relate to compliance with the Code of Conduct and the applicable laws and regulations on the protection of Personal Data, and also check the lawfulness of data processing. The DPO advises the Insurer on the structure and content of internal investigations.

9.3 Disputes

9.3.1 Insurers will set up an internal complaints procedure to ensure that a Data Subject can submit a complaint about the actions of an Insurer in case of a possible breach of the Code of Conduct

or applicable laws and regulations.

9.3.2 If a Data Subject has gone through the internal complaints procedure and takes the position that the Insurer has not dealt with the complaint adequately, the Data Subject may submit a complaint against the Insurer to the Financial Services Complaints Institute (Kifid), P.O. Box 93257, 2509 AG The Hague, the Netherlands. The Data Subject may also submit it directly to the Personal Data Authority or the court that has jurisdiction.

10. Definitions

The following applies in this Code of Conduct:

ACM is the Netherlands Authority for Consumers and Markets;

AFM is the Netherlands Authority for the Financial Markets;

AP is the Dutch DPA;

GDPR is the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;

Filing system is any structured set of Personal Data accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis;

The **Data Subject** is the person to whom the Personal Data relate;

Special Personal Data are Personal Data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or sexual orientation;

BSN is the citizen service number (*Burgerservicenummer*);

Third Party is any person other than the Data Subject, Controller, Processor, Insurer, or any other person who, under the direct authority of the Controller or the Processor, are authorised to process Personal Data;

Direct Marketing is the targeted transfer of information by an Insurer to a Data Subject to facilitate the conclusion of an agreement;

DNB is the Dutch Central Bank (*De Nederlandsche Bank*);

DPIA is a Data Protection Impact Assessment in accordance with Article 35 GDPR;

Urgent Reason is defined in Article 8.1.1;

External Referral Register (*EVR*) is the subset of the Incidents Register of a PIFI participant, which only contains referral data about natural or legal persons and is intended for use by participants or the organisations of participants in that protocol;

Data Protection Officer (DPO) is the data protection officer referred to in Section 4, Article 37 ff. of the GDPR;

Event is an incident that requires the attention of an Insurer because of a possible effect on the safety and integrity of the business operations, employees, customers, other business relations, and the insurance industry. This includes possible fraud or other reprehensible or unlawful conduct, potential and actual claims, including in respect of an agreement entered into with an Insurer and the non-performance of contractual obligations or other attributable failure;

Event Records is the Processing of Personal Data in connection with an Event;

Code of Conduct is the Code of Conduct for the Processing of Personal Data by Insurers;

Health Data are Personal Data relating to the physical or mental health of a natural person, including data on health services provided that give information on the person's state of health;

Group Company is an organisation with which the Insurer forms an economic unity of legal persons and companies;

Incident is an event that has, could have, or has had, the consequence that the interests, integrity, or safety of an Insurer, customers, or employees of an Insurer itself or the industry as a whole, are or could be at stake. For example, the falsification of invoices, identity fraud, embezzlement in employment, and deliberate deception;

Incidents Register is the Insurer's data collection that also participates in the PIFI, in which data are recorded as a result of or relating to a current or possible Incident;

Internal Referral Register (IVR) is the subset of the Insurer's Events Register, which contains only referral data relating to natural or legal persons and is intended for internal use within the Company or Group, in accordance with Article 7.11.1. of the Code of Conduct;

Kifid is the Financial Services Complaints Institute;

Medical Adviser (MA) is the doctor who, supported by the medical service or staff under their responsibility, processes Health Data to provide independent expert advice on the health status of the following Data Subjects: (i) the policyholder; (ii) persons who have submitted a claim to a policyholder; (iii) the person to be insured;

Personal Data are any information relating to an identified or identifiable natural person (the 'Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an on-line identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the natural person;

PIFI is the Protocol Incident Warning System for Financial Institutions;

Pseudonymisation is the processing of Personal Data in such a way that these Personal Data can no longer be attributed to a specific Data Subject without the use of additional data, provided that these additional data are kept separately and technical and organisational measures are taken to ensure that Personal Data are not attributed to any identified or identifiable natural person;

Criminal Records Data are Personal Data relating to criminal convictions and offences, or related security measures as referred to in Article 10 GDPR, as well as Personal Data relating

to a court order prohibiting unlawful or disruptive conduct;

Dutch GDPI Act is the Dutch General Data Protection Implementation Act (Uitvoeringswet Algemene Verordening Gegevensbescherming, UAVG);

IT Security department is the department or person within the Insurer responsible for the Processing of Personal Data within the framework of safeguarding the security and integrity of the Insurer or the industry and the prevention of fraud;

Association is the Dutch Association of Insurers (Verbond van Verzekeraars)

Processor is a natural person, legal entity, public authority, agency, or other body that processes Personal Data on behalf of the Controller;

Processing is any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Controller is the natural person, legal entity, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;

Urgent Reason is defined in Article 2.1;

Insured is the natural or legal person who, in accordance with the policy conditions, is to be regarded as entitled to compensation or payment, or the person whose life or health affects the insurance;

Wbp is the Personal Data Protection Act (*Wet bescherming persoonsgegevens)*;

Wft is the Financial Supervision Act (Wet op het financieel toezicht);

Wwft is the Money Laundering and Terrorist Financing Prevention Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*)

11. Article-by-Article Explanation

Section 1

Article 1.1.1.

The introductory considerations describe the raison d'être of this Code of Conduct and the underlying reason why the Association developed the Code of Conduct. The Processing of Personal Data by Insurers is regulated by a long series of laws and subordinate regulations. In addition to the Personal Data Protection Act ('Wbp'), which has been replaced by the much more extensive European GDPR and the Dutch GDPI Act, many other laws are relevant to the Processing of Personal Data by Insurers, such as the Financial Supervision Act (Wft), the Money Laundering and Terrorist Financing Prevention Act (Wwft) and the Telecommunications Act (Tw). Furthermore, the policy rules, decisions, guiding principles and other guidelines of supervisors such as the Dutch ADP (AP) the Dutch Central Bank (DNB) and the Netherlands Authority for the Financial Markets contain rules on all kinds of subjects to ensure the transparent, safe and careful Processing of Personal Data by Insurers.

There is a need for Insurers to work out these often general rules in detail for their own industry. At the same time, there is a need for Insured parties, Data Subjects, and the society at large to understand how Insurers handle Personal Data. The Code of Conduct aims to bring these two interests together and can count on broad support within the industry. Insurers comply with the provisions of this Code of Conduct in their business operations and privacy policy. The Code of Conduct does not automatically apply to authorised underwriting agents. These are financial service providers acting on behalf of Insurers towards the customer. Insurers covered by this Code of Conduct oblige authorised underwriting agents to comply with the Code of Conduct if and in so far as they engage them.

Article 1.1.2.

With this Code of Conduct, the Association aims to explain to Insurers the general laws and regulations for the Processing of Personal Data and to promote compliance with them. The Code of Conduct is not a complete copy of all laws and regulations applicable to the Processing of Personal Data but is intended to elaborate the legislation and regulations in more detail in specific provisions. The purpose of this Code of Conduct is for the industry to regulate the Processing of Personal Data. This does not make the Code of Conduct a formal code of conduct in line with the GDPR. After all, at the time of drafting this version of the Code of Conduct, the European privacy supervisors had not yet published their guidelines for formal codes of conduct.

The provisions of the Code of Conduct are worked out in greater detail in this explanation based on practical examples. In this way, the Code of Conduct creates clear frameworks within which Insurers can process Personal Data and helps Insured parties and the wider society to better understand this area

Article 1.1.3.

For Insurers, this Code of Conduct replaces all its predecessors, in particular the Code of Conduct for the Processing of Personal Data by Financial Institutions (GVPFI[2]), which came into force on 26 April 2010. As a result of changes in legislation and regulations, such as the introduction of the GDPR, and case law around data protection, the frameworks from the GVPFI are no longer adequate for Insurers in the Processing of Personal Data.

[2] The text of the GVPFI can be found at: http://wetten.overheid.nl/BWBR0033201/2010-04-26

Section 2

Article 2.1.1.

The Code of Conduct is widely supported within the insurance industry. This Article regulates which Insurers are bound by the Code of Conduct. All members of the Association are automatically bound by the provisions of the Code of Conduct in respect of their insurance activities. Units of Insurers that do not act as Insurers are not covered by the Code of Conduct.

Natural and legal persons who do not fall within the definition of Insurers, such as independent intermediaries, authorised underwriting agents, legal aid providers, and claims settlement offices may subscribe to all or parts of the Code of Conduct in their internal and external privacy policies. The Association encourages the broadest possible endorsement of the Code of Conduct. When Insurers outsource tasks to authorised underwriting agents, they are obliged to enforce compliance with the Code in the underwriting agency agreement.

Members of Zorgverzekeraars Nederland are subject to the Code of Conduct for the Processing of Personal Data by Health Insurers (*Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars*).

Article 2.2.1.

Paragraph 2.2. Code of Conduct regulates when the Code of Conduct does and does not apply. The purport of this provision is that an Insurer must follow the rules of the Code of Conduct with respect to virtually all Processing of Personal Data: from the collection to the destruction of Personal Data, and all acts in between these two, the Code of Conduct applies.

Article 2.2.2.

The Processing of Personal Data of the staff of an Insurer in its capacity as employer falls outside the scope of the Code of Conduct. Such Processing, for example in the context of payroll administration and application procedures, is of course subject to the general laws and regulations for the Processing of Personal Data. If an employee of an Insurer is also an Insured Person, Co-insured Person, or Data Subject vis-à-vis the Insurer, for example in case of personnel insurances, the Code of Conduct applies in full to that customer relationship. Nor will the Code of Conduct apply to the Processing of Personal Data recorded (i) in the Incidents Register, or (ii) in the External Reference Register. This Processing is subject to the Protocol on Incidents for the PIFI.

In addition to the Code of Conduct, the Association and the Insurers have developed additional codes of conduct, protocols, and covenants for specific cases. These specific instruments create detailed frameworks for Insurers for the Processing of Personal Data in specific cases and do not conflict with the Code of Conduct. All self-regulation in the industry can be consulted via the Association's website: https://www.verzekeraars.nl/branche/zelfregulering.

Section 3

Article 3.1.1.

This provision contains the overarching principles for the Processing of Personal Data by Insurers. In all types of Processing, Insurers take the privacy interests of the Data Subject into account. In cases not provided for by laws and regulations and the specific provisions of the Code of Conduct, Insurers will assess the Processing of Personal Data based on these general principles. It is important to place these

principles at the heart of the Code of Conduct. For example, existing rules may not be able to respond properly to new technological upheavals. It is conceivable, for example, that technological upheavals, such as artificial intelligence, will change the nature and extent of Personal Data Processing to a far-reaching extent. Insurers will always assess, on the basis of the overarching principles, whether an act has an impact on the privacy interests of Data Subjects. Are the consequences for the privacy of Data Subjects in proportion to the interests of the Insurer (principle of 'proportionality')? Are there less intrusive ways for the Insurer to achieve the same objectives (principle of 'subsidiarity')? Insurers will uphold these principles and those of confidentiality, transparency and due care in all their actions, even if laws and regulations, guidelines from relevant regulators and the Code of Conduct do not or do not yet provide clear legal frameworks.

Article 3.2.1.

Insurers base each Processing of Personal Data on one of the principles stated in the applicable laws and regulations. If none of the principles is applicable, the Processing of Personal Data is not permitted. In Sections 4 and 5, the Code of Conduct links these statutory principles – such as the express consent of the Data Subject or compliance with a statutory duty of care arising from financial regulations – to common purposes of the Processing of Personal Data in the industry.

Article 3.3.1.

Insurers collect Personal Data only for well-defined, explicit, and legitimate purposes. The Insurer will determine these purposes before the Processing. Well-defined means that the objectives must be clear. Article 4 Code of Conduct sets out the objectives for the Processing of Personal Data by Insurers. The objective in question largely determines the applicability of other provisions in the Code of Conduct, such as the permitted basis for the Processing, the security level, and the retention period of the Personal Data.

Insurers collect Personal Data from the Data Subject, for example through an application form or a health declaration, to effect an insurance policy. In addition, Insurers collect Personal Data via technological channels, such as cookies on a website, directly from the smart phone when using an app, the insurer's 'My Environment' and social media. The collection of Personal Data through technical channels is largely regulated by the Telecommunications Act and is further worked out in more detail in Article 7.1 Code of Conduct. Insurers also collect Personal Data through external organisations. For example, under financial legislation (such as the Financial Institutions Supervision Act (Wft) and the Market Conduct of Financial Institutions Supervision Decree (BGfo Wft)), Insurers are obliged to carry out Customer Due Diligence (CDD), i.e. customer research, and to keep customer databases up to date. They may also engage research agencies to assist the Insurer in marketing activities. Insurers will always consider Processing in the light of the objectives and basis of the Processing, will always inform the Data Subject how Personal Data have been collected (see Article 6.1 Code of Conduct), and provide appropriate safeguards for the protection and security of Personal Data, such as entering into a Processing Agreement (see Article 7.9 Code of Conduct).

Article 3.4.1.

There are two aspects to the quality of Personal Data. It follows from the word 'relevant' that Insurers may not process more Personal Data than is reasonably necessary for business operations. In doing so, Insurers implement the statutory principle of 'data minimisation' and the limitation of the storage of Personal Data. The purpose of the Processing largely determines the nature and scope of the Personal Data that Insurers are permitted to process, and for how long they may process these Personal Data.

These principles are worked out in concrete terms in this Code of Conduct, for example in the provisions on the purposes of the Processing of Personal Data (Section 4) and the retention policy (Article 7.5). Insurers must keep an overview of the Processing of Personal Data in a processing register intended for that purpose.

In addition, Personal Data must be 'correct'. The Controller must take such action as is reasonably necessary to ensure that Personal Data are accurate. This obligation, which also rests on Insurers on the basis of financial legislation, is not absolute, as Insurers are often dependent on the Personal Data provided by the Data Subject. Insurers will therefore draw the attention of customers and other Data Subjects to the importance of providing the correct Personal Data and passing on changes in the prescribed time.

Article 3.5.1.

Privacy legislation contains a number of important rights that enable the Data Subject to form an opinion about the Processing of the Personal Data relating to them by Insurers, such as the right of inspection and the right to object. The GDPR also contains a number of new rights, such as the right to data portability. Article 6 of the Code of Conduct formulates these rights in detail.

Article 3.6.1.

In exceptional cases, Insurers may deviate from the basic principles for the Processing of Personal Data and the provisions of the Code of Conduct. Insurers interpret these Urgent Reasons, such as the protection of the safety of persons, restrictively. These Urgent Reasons are listed in Article 8.

Section 4

Article 4.1.1.

This Section contains the main purposes of the Processing of Personal Data by Insurers. In principle, Insurers will not process Personal Data for purposes other than those for which they have collected the Personal Data (the principle of purpose limitation).

Article 4.1.2.

Applicable legislation and regulations (e.g. Article 6(4) GDPR) offers Insurers the option to process Personal Data for new purposes. Additional conditions are attached to this further Processing. The purpose of the new Processing must be compatible with the purpose for which the Personal Data were acquired originally. Besides this compatibility of the purposes, the nature of the data, the effects of the Processing on the Data Subject and the degree to which suitable safeguards with regard to the Data Subject have been provided play an important role. For instance, the more sensitive the Personal Data are, the more reticently the Insurer may assume that this is a permitted further Processing.

The Insurer has to assess and balance the above-mentioned factors in their interrelationship. None of the factors in itself is a decisive factor. If, for instance, there is a certain relation with the purpose of the acquisition but the Personal Data become more sensitive as a result of their use in a particular context and the effects on the Data Subject are significant, it is unlikely to be a case of compatible use. If the further Processing of Personal Data only relates to analyses for historical, statistical, and scientific purposes in accordance with Article 4.3 of the Code of Conduct, it is more likely to be a case of compatible use. Insurers may apply techniques such as pseudonymisation in accordance with Article 7.6 Code of Conduct, to render the Personal Data in a dataset less sensitive and to limit the effects on the Data

Subject's privacy. During the assessment of compatible use, the Insurer has to assess the open standards for each individual case to determine whether a certain data exchange is permitted. That is why Insurers must perform a DPIA during the assessment of such further Processing of Personal Data, in accordance with the criteria of Article 7.4 Code of Conduct.

Article 4.2.1.

One of the main purposes of the Processing of Personal Data by Insurers is effecting and implementing the insurance policy. To this end, Insurers process Personal Data in many practical situations, such as the settlement of premium payments, the verification of the identity of the Data Subject, the administration of the insurance, the handling of claims, or the determination of the premium. For instance, Insurers in a Group may verify whether in a different part of the Group another payment under a general insurance is payable and to maintain the customer base accurately. Insurers also process Personal Data during the pre-contractual phase, that is to say: before insurance is taken out. That means that they prepare a risk assessment of the Data Subject upon taking out insurance and determine the premium of insurance or reinsurance on that basis. At such time, Insurers are guided by the legislation and regulations, the directives of the relevant supervisory bodies, and their special role in social and economic life, in which they enable solidarity and the shared risks. The application process is shown graphically in the infographic 'Application of insurance' in the appendix to the Code of Conduct.

Insurers may provide Personal Data to the parties involved in the further Processing of Personal Data, in so far as these are reasonably necessary for verification or reconstruction purposes. In practice, this often occurs in the handling of claims. Before the Insurers effect an insurance policy, and in case of any concrete cause during the implementation of the insurance, Insurers may check whether certain Personal Data have been included in warning systems created for this purpose to safeguard the safety and integrity of the service and the industry. This purpose is explained in more detail in Article 4.5 Code of Conduct. In this respect, Insurers aim to follow the recommendations made by the European privacy supervisory bodies, such as algorithmic auditing to prevent discrimination[3].

Article 4.2.2.

Automated decision-making plays an important role in the insurance industry, as the assessment and analyses of large quantities of data are necessary to effect and implement an insurance policy. To this end, Insurers apply technologies, among which automated processing and profiling. These technologies enable Insurers to assess and cover the risks of millions of Dutch nationals.

Applying these technologies does not always comprise taking a decision on an individual's application for an insurance. Insurers may also use such technologies for other purposes, such as compliance with the statutory duties mentioned in the provision, for example to prevent money laundering and terrorist financing. Besides that, under the financial legislation, Insurers must know their customers (Customer Due Diligence) before they can buy certain products or services. Automated processing is essential in meeting this obligation. Insurers also apply such technologies when they have the explicit permission of the Data Subject to do so.

Insurers take appropriate measures to guarantee the transparency of such Processing. In doing so, they put the rights of the Data Subjects into effect and limit the impact on their private life. Insurers also take care of periodical evaluations of the automated decision-making, and the general principles of Section 3 of the Code of Conduct are therefore not only safeguarded at the time of the system's set-up, but also during its use.

[3] See Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251, p. 30

Insurers assess a written request of the Data Subject with regard to fully automated processing and decision-making with the help of human judgement, even if the Data Subject has not asked for this human check.

Article 4.3.1.

Insurances exist to share risks with each other. For their business operations and often also in accordance with financial legislation, Insurers have to conduct historical, statistical and scientific analyses to be able to offer effective, honest and affordable insurances. To that end, Insurers use new technologies, such as data mining, big data analytics, and artificial intelligence. For instance, Insurers can analyse existing information in a database (such as a customer base) to discover new links that reveal developments in for instance insurance risks, business processes, or the price of a product. Insurers may use archived information and data from external sources for this purpose. For instance, data from public registers (such as the Commercial Register of the Chamber of Commerce and the Land Register), public sources (such as newspapers), or data from research agencies. This kind of research results, among other things, in commercial indicators and data regarding the use of products and services. An example of this is research into the claim causes relating to smart phones. There is a relatively large number of claims in this domain. Insurance data are then processed to signal a claim trend, to name a cause, and subsequently to make changes in the product or the application process. With such historical and statistical insights Insurers prevent the improper use of insurance products and the claims burden for other insured parties will be limited.

Insurers take appropriate measures to limit the impact on the Data Subjects' private life (the 'privacy by design' principle). In accordance with Article 7.4 Code of Conduct, Insurers, where necessary, carry out a DPIA to explore this impact. The protective measures relate to the purpose and the impact of the analysis. Insurers can carefully select the data to be used, for instance, and isolate them in a separate data set, to ensure that only the information that is important to the analysis will be used (data minimisation). In addition, Insurers can guarantee that only those employees who need to have access to the data set to perform the analysis will have access to the data set, rather than all employees of the Insurer (functional separation of access).

Insurers can also anonymise the data set to ensure that the data set no longer contains Personal Data, or apply pseudonymisation. Pseudonymisation and other appropriate technical and organisational measures are worked out in more detail in the following provisions.

Article 4.3.2.

Insurers differentiate between compiling group profiles for historical, statistical, or scientific purposes and attributing a score or reference to a person based on a group profile. During the compilation of group profiles, Personal Data may be processed on the entry side, if appropriate safeguards have been provided to minimise the impact on one's privacy. A DPIA must show which measures are appropriate and safeguard that the data involved in the analysis will be used only for historical, statistical, or scientific purposes. These measures could consist of the pseudonymisation of the data set in accordance with Article 7.6 Code of Conduct. If the Insurers subsequently wish to link a person to that profile, it may be considered a further Processing or a new Processing of Personal Data. A further Processing is a Processing that is compatible with the purposes for which the data were originally collected. To this end, the Insurer checks whether, for instance, marketing activities are compatible with the purpose for which the Personal Data are obtained (see Article 4.4.3. Code of Conduct) and whether the Data Subject has

been informed adequately of this Processing at the time of obtaining (see Article 6.1 Code of Conduct). Processing for other purposes may require a different principle than the principle of the original Processing. A practical example of the latter is the investigation into Incidents regarding a Data Subject. This is usually aimed at one or only a few Data Subject or Data Subjects and in that case it is not easy to qualify as a Processing to compile group profiles, but as a Processing to safeguard the integrity and safety of the business operations or the industry (see Article 4.5 Code of Conduct). The same applies to such analyses in the framework of financing, bookkeeping, investments, taxes, implementation of company control measures, risk analyses and audits, reinsurance activities, IT maintenance and company strategies. In addition, in certain cases, Insurers are obliged to carry out similar analyses on the basis of financial legislation, such as the calculation of the cost of products based on historical data (based on Solvency II legislation).

Article 4.3.3.

Insurers limit the use of Special Personal Data to perform historical, statistical, and scientific analyses, Sometimes the use of Special Personal Data is required after all to perform such analyses, for instance the Processing of Healthcare Data during the discovery of trends in occupational incapacity insurances[4]. Insurers will provide the necessary safeguard to such Processing, to safeguard the privacy rights of the Data Subject[5].

Article 4.4.1.

Marketing activities and customer relationship management (CRM) are closely related because both regard the communication with current and potential customers. That is why both purposes are mentioned in this provision. Marketing has a purely commercial purpose; CRM is about service. As a result, within this Code of Conduct, a lighter regime applies to CRM. The Insurer processes these Personal Data to implement the insurance with the Data Subject. Furthermore, Insurers have a have a legitimate interest in in the Processing of Personal Data for marketing purposes[6]. They provide additional safeguards for marketing activities in order to accommodate the privacy rights of the Data Subject and to comply with the general principles of proper and careful Processing. That is why Insurers prefer to use Personal Data provided by the Data Subject. If the Personal Data are not provided by the Data Subject, the provisions of Article 6.1 Code of Conduct apply with regard to the duty of disclosure. In case of third-party acquisition of Personal Data to contact the Data Subject by letter, the Data Subject will be informed of this before the collection of the Personal Data. If this would require a disproportionate effort, for instance because the Insurer does not have an email address, the Insurer can inform the Data Subject of this later on and record the source of the Personal Data.

Marketing and service notifications can be closely connected with the performance of historical, statistical, and scientific research by an Insurer. An Insurer could develop an on-line tool, for instance, with which the Data Subject can understand the pension insurance taken out and whether this insurance is the most advantageous. The Insurer could also perform aggregated research with respect to pension trends. Based on characteristics of large groups of people, it will then be examined how the insured in general can be better informed about their pension. Such research data are used in a pseudonymised form. If the Data Subject has given express consent to this, the Insurer can contact the Data Subject after the analysis for personalised information regarding other pension insurances. In addition, Insurers can cooperate with Third Parties in the framework of continuing the customer relationship. This could be

[4] See Article 30(3)(b) under 1 Dutch GDPI Act.
[5] See Article 24(d) Dutch GDPI Act
[6] See recital 47, Dutch GDPI Act

beneficial to the Data Subject, for instance in the form of a discount on an entry ticket to an amusement park or musical. This cooperation does not require express consent of the Data Subject. The Insurer can 'remember' the Data Subject's completed data in the tool for service purposes, to ensure that the Data Subject does not have to complete the data again every time.

Article 4.4.2.

Direct Marketing is described in the definitions as the transfer of information by an Insurer to a Data Subject to facilitate the conclusion of an agreement. This provision differentiates between the various channels for Direct Marketing in accordance with the current legislation and regulations. For instance, various obligations ensue from the Telecommunications Act that apply to commercial communications with a Data Subject via telephone, smart phone, email, or internet. The use of automatic call systems without human intervention for Direct Marketing, for instance, is only permitted if Data Subjects have given their prior unambiguous consent ('opt-in'). The less strict regime applies to telemarketing and marketing by post ('opt-out'), that is to say: Processing is allowed as long as Data Subjects have not indicated that they want to terminate this use. Data Subjects do have to be informed of the 'opt-out' option each time their Personal Data are used for marketing purposes, however. After an 'opt-out', Insurers terminate the Direct Marketing immediately. In case of directly contacting a Data Subject by telephone, the Insurer must have obtained the Data Subject's prior consent ('opt-in').

If an Insurer used the Data Subject's contact details to offer products and services by telephone (telemarketing), the Insurer will check the Don't-Call-Me register (*Bel-me-niet register*) before this use to see whether the Data Subject, not being the Insured, has indicated not to want such contact. The mandatory check of the Don't-Call-Me register does not apply when contacting existing customers regarding similar products or services that the customer has acquired from the Insurer before. The Insurer maintains an in-house register, in which the Data Subjects' opt-out is registered. After the completion of every telemarketing call the Data Subject must be informed of the possibility of opting out and being included in the Don't-Call-Me Register.

If the Data Subject makes use of that right, the Insurer must ensure timely inclusion in the Don't-Call-Me Register and prevent the Data Subject from being approached again for telemarketing purposes.

If an Insurer has obtained electronic contact details for electronic messages (such as email, text messages, MMS messages) in the context of the sale of a product or the provision of a service within the Group, the Insurer itself or a Group Company may use these Personal Data for Direct Marketing of similar products or services ('soft opt-in'). This applies, for example, if an Insurer has taken out cover for a building insurance policy and a Group Company subsequently points out a savings product or disability insurance to the Data Subject. The Insurer must always point out the right to terminate this Processing ('opt-out') to the Data Subject, also in accordance with Article 6.3 Code of Conduct. In addition, the Insurer must always clearly inform the Data Subject of the Group to which a Group Company belongs.

Article 4.4.3.

This provision is the mirror provision of Article 4.3.2. Code of Conduct and a further elaboration of the general provision on further Processing of Article 4.1.2. Code of Conduct. If an Insurer has developed a group profile on the basis of a historical, statistical or scientific analysis, the Insurer may only use previously pseudonymised data to approach Data Subjects included therein for marketing purposes after carrying out a DPIA. Depending on the effects on the Data Subject's privacy, which must be apparent from the DPIA carried out, Insurers must assess whether there is a new Processing and whether Insurers

must base this new Processing on the explicit consent of the Data Subject or on the legitimate interest of the Insurer. The answer to this question is closely related to the purpose for which the Personal Data were originally collected, the connection of this purpose with the purpose of the further Processing, and the time elapsed between the collection and this further Processing. The other provisions of the Code of Conduct also apply in full to this further Processing, such as the obligation to provide information and other rights of those Data Subjects (Section 6).

Article 4.4.4.

Insurers restrict the use of Special Personal Data to marketing activities and CRM. The Insurers will provide additional safeguards for such Processing, in accordance with the stricter regime for Special Personal Data set out in Article 5 Code of Conduct.

Article 4.5.1.

Safety and integrity are essential to Insurers. In addition, Insurers are required by law to have controlled and honest business operations. That is why Insurers must take protective measures. This is how insurance fraud and other crime can be prevented and combated and Insurers can guarantee safety, integrity, and quality. The Processing of Personal Data in this context is graphically represented in the infographic 'Preventing and Combating Insurance Fraud and Crime' in the appendix to the Code of Conduct.

The Insurer’s IT Security department deals with matters relating to safety and integrity. In view of the sensitivity of the work and the information processed, the IT Security department is often a separate unit within the company. If any irregularities arise during the application process or the performance of an agreement, the Insurer's employees may pass on Personal Data regarding the agreement to the IT Security department in relation to the irregularities found. This department may further process Personal Data in the context of combating insurance crime, such as insurance fraud, and, subject to the conditions set forth in the PIFI, include the data or have them included in the Incidents Register and the External Reference Register EVR. This is elaborated further under Article 4.5.3. Insurers that are not members of the Association may subscribe to the Code of Conduct in accordance with Article 2.1. but will not automatically be granted access to these systems. Access to these systems is subject to the additional terms and conditions of the PIFI.

A separate Processing of Personal Data regards the Personal Investigation by Insurers. The Personal Investigation may, for example, be necessary to prevent the wrongful payment of a claim for compensation, or to investigate the correctness of the circumstances of a claim. The legitimacy of a claim is then checked, for example, by carrying out a neighbourhood survey or camera registration. The Code of Conduct 'Personal Investigation' also applies to these forms of investigation.

Article 4.5.2.

One of the measures to guarantee the quality, safety and integrity of the company and the industry is to carry out an audit. To demonstrate the correct functioning of processes, it is inevitable that these audits provide insight into Personal Data and in some cases even Special Personal Data. These Personal Data are subsequently not used to give an opinion about the Data Subject, but only to demonstrate that the Insurer conducts its business with due care. Where possible, no Personal Data will be included in an audit or investigation report.

The audits do not necessarily have to be carried out by an Insurer's audit department, but can also be outsourced to external organisations. Examples are the Insurers Assessment Foundation (Stichting Toetsing Verzekeraars) and the Insurers' Institute on Personal Injury Claims (Stichting Personenschade Instituut van Verzekeraars). These two organisations carry out an independent assessment of compliance with self-regulation by the members of the Association. In all cases, appropriate measures are taken to protect the privacy of those involved, such as entering into a Processing Agreement in accordance with Article 7.9 Code of Conduct. The Insurer also informs the Data Subject of the fact that Personal Data may be used for this purpose by way of privacy statements or other communications.

Article 4.5.3.

One of the safety measures taken by Insurers is to record Incidents that may be important for the safety and integrity of the company and the industry. Insurers record these Incidents in an administration. This part of the administration is called the Incident Records. In these records, information is kept that, in the opinion of the Insurer, may be important for the quality, safety and integrity of the Insurer, the Group to which the Insurer belongs, and the insurance industry. This may involve a variety of incidents. For example, the results of screening requests, complaints from customers, potential/established insurance fraud, or non-compliance with agreements, including structural non-payment behaviour or bankruptcies. The Incident Records consist of a collection of data and form the memory of the Insurer. Insurers do not have access to each other's Incident Records, unless they are part of the same Group. Companies that belong to a Group can also keep joint Incident Records.

The IT Security department or a designated department of the Insurer may decide to enter the referral details of persons whose details have been recorded in the Incident Records in an Internal Referral Register (IVR). In this way, a small part of the information from the Incident Records becomes verifiable. The IVR exists to prevent access to Personal Data by a broad group of employees and to facilitate its safe use within the Group to which the Insurer belongs. This register, just like the Incident Records, cannot be consulted by other Insurers.

An IVR contains reference data: i.e. identifying data (such as address details and date of birth) of persons who pose a certain risk. Therefore, the IVR does not contain any additional information about the person or the Incident. The Insurer always makes a careful assessment before including reference data, during which the importance of the Incident plays an important role (immediately or for the future). To share an Incident in this way within a Company or Group, one of the factors that might play a part is whether there is a reasonable suspicion of intentional damage by the Data Subject. This may involve, for example, improper use of an Insurer's products, services and facilities, or attempts to do so. Or, for example, the internal signalling of a reasonable suspicion of the commission of criminal or reprehensible conduct, or a violation or attempt to violate legislation or regulations directed against the Insurer, its customers, or its employees.

Insofar as relevant for their work, an employee of the Insurer may consult the IVR. For example, if a person wants to become a customer or during job application procedures. A test is carried out based on the address details and date of birth of the person in question. The system of assessment works on a hit/no-hit basis. The employee who performs the test does not see why a hit has been made but does see that a natural person or legal entity has been included. In the event of a hit, the employee must always call in the IT Security department or a department of the Insurer designated for this purpose, which will then advise the employee. The advice can be, for example, whether or not to enter into a contract with the applicant. Special conditions may be agreed with regard to a customer, such as additional policy conditions or cover restrictions. Relevant departments or employees can be informed in

this way that certain people or matters require extra attention.

In addition to having Incident Records and an IVR, an Insurer must also have an industry-wide early-warning system, i.e. a system that allows Insurers to warn each other. As in this case Personal Data are shared outside the Group, special additional rules apply. The rules relating to the early-warning system are laid down in the Protocol Incident Warning System for Financial Institutions (PIFI).

In certain cases, Insurers may also record Personal Data in connection with cancellations, claims, the filing of a claim, and other Incidents in registers maintained by an independent legal entity, for example the Foundation Central Information System (*Stichting Centraal Informatie Systeem, or CIS*), which acts as the Controller for the Central Information System in the insurance industry. This Code of Conduct applies to the provision and consultation of Personal Data in these systems. The Processing of Personal Data in the actual systems falls outside the scope of the Code of Conduct. The CIS Foundation has its own privacy and user regulations for this purpose, which can be consulted via its website: https://www.stichtingcis.nl/nl-nl/regelgeving.aspx.

Article 4.6.1.

The last couple of years have shown an increase in the number of obligations to collect and make available Personal Data based on statutory regulations. Some examples are given below. In addition, there are many other statutory regulations under which an Insurer is obliged to process certain Personal Data.

Financial legislation increasingly obliges Insurers to process Personal Data. In addition to regulations from general insurance legislation, for example, obligations from the Financial Supervision Act (Wft) with regard to Customer Due Diligence are on the increase. Insurers have a duty of care to know their customers and to fully inform them about existing risks and payment obligations. The obligations in the area of fraud prevention and terrorism financing are also increasing, which follow, for example, from European Directives 2005/60/EU and 2006/70/EU of the Money Laundering and Terrorist Financing Prevention Act (*Wwft*). The Wwft requires that the information contained in the document, used to establish the identity, must be recorded. The Wwft is what is referred to as a risk-based legislation, meaning that the Insurer must tailor the Customer Due Diligence to the risk sensitivity for money laundering, financing of terrorism, the type of customer, business relations, product, or transaction. This allows the institution to make its own choices, taking risks and existing control measures into account. Supervisors play a key role in the Wwft. Insurers will cooperate with relevant supervisors and authorities in the further implementation of this task.

For Insurers, the Wft also prescribes that in some cases information must be obtained about a customer's financial position, knowledge, experience, objectives, and risk appetite, for example when Insurers advise on complex products (such as life insurance). Background data of current or prospective customers must also be collected and checked. Within the framework of tax legislation, the citizen service number must be exchanged with the Tax and Customs Administration. In addition, Insurers exchange Personal Data with the Tax and Customs Administration in the context of reporting information to the tax authorities (the statutory obligation for Insurers to provide certain prescribed data and information to the Tax and Customs Administration). The BSN is also exchanged with the UWV within the framework of the assessment of possible occupational incapacity.

The Sanctions Act requires Insurers to check the Personal Data of Policyholders and Insured Persons against national and international sanction lists when entering into the insurance contract, during the term of the insurance policy and when making a payment. Investigative authorities may submit data

claims to Insurers under the Dutch Code of Criminal Procedure. If a data claim meets the required legal criteria, an Insurer must cooperate with a claim.

Section 5

Article 5.1.1.

The general assessment framework for the Processing of Personal Data is set out in Section 4 of the Code of Conduct. This Section of the Code of Conduct contains specific rules on the Processing of Health Data. A more strict regime applies to Health Data in addition to the general assessment framework. At the same time, current legislation and regulations provide Insurers wider powers to process and further process Health Data than companies in other industries[7]. This is due to the fact that insurances have social significance. As a result, Insurers are often compelled to process Health Data.

An Insurer may process Health Data if this is necessary for the assessment, underwriting, or the effecting and implementing of an insurance policy in which a Data Subject or Third Party is involved. The criterion 'effecting and implementing an insurance' includes the assessment of the risk (e.g. occupational incapacity during the term of the insurance) and whether that risk should be normalised with, for example, cover-limiting clauses or an increased premium.

Once the insurance has been effected, the Insurer will ask for health information to assess entitlement to a benefit. If necessary, the Insurer will ask the Data Subject to complete a health statement (*Gezondheidsverklaring*). In the health statement, the Insurer will, among other things, ask questions about complaints, illnesses, or disorders. The statement may contain questions about the use of medication, doctor's visits, whether or not one smokes, the use of alcohol and whether the prospective insured wears glasses or contact lenses. The Data Subject completes the health statement and in doing so gives permission to the Insurer and the Medical Adviser (MA) to process their Health Data. The Insurer may also ask the Data Subject for a medical authorisation in case the MA has to request additional information from other authorities.

The MA plays a key role in the assessment of the state of health and the associated risks in connection with the acceptance of or entitlement to insurance of a current or prospective Insured. This role is explained in more detail in Article 5.1.3 Code of Conduct. The Insurer may ask the Insured to undergo a medical examination. This examination is often carried out by a General Practitioner (GP), not being the Data Subject's GP, and may consist of a medical examination and a blood test.

The MA may share Health Data with a reinsurer’s MA before effecting and implementing a Health Insurance policy. Like Insurers, the reinsurer makes a strict distinction between advice on acceptance and on claim settlement, employs a MA, and processes only the Health Data necessary to effect and implement the insurance policy in accordance with Article 4.2 Code of Conduct.

In some situations, Insurers may reprocess Special Personal Data as part of the implementation of the insurance. In practice, further processing of Special Personal Data is rare. An example is the settlement of a second claim under the same insurance policy. This Processing does not require explicit permission if the Insurer reprocesses the Health Data provided by the Data Subject based on a first claim. If, for example, a Data Subject has submitted a claim under an occupational disability insurance and an orthopaedic assessment is being carried out, the Insurer may use this assessment six months after the termination of the first claim when settling a second claim, if the Data Subject submits a second claim

[7] See Article 30(3)(b) under 1 Dutch GDPI Act

regarding the same back problems. However, if the second claim concerns a different insurance policy, the Insurer can only process the Health Data with the explicit consent of the Data Subject. The explicit consent of the Data Subject is therefore not required for the processing of multiple insurance claims under the same insurance policy, but the explicit consent of the Data Subject is required for the processing of multiple claims under different insurance policies, unless the insurances cover the same risk (e.g. in case of a Wia insurance followed by a Wia additional income insurance).

Insurers are legally obliged to guarantee the safety and integrity of their business operations and the industry, in accordance with Article 4.5. Code of Conduct. A concrete example that often occurs in the context of Health Data is the non-performance of the legal obligation to provide information, also known as 'withholding of facts' or 'concealment'. If the Insurer has a reasonable suspicion that a Data Subject has concealed a medical condition, the Insurer has the duty to analyse the Health Data and claims history to evaluate whether there were any previous indications of concealment by the Data Subject.

The provision also lists the other purposes of the Processing of Health Data. Insurers are reluctant to process Health Data based on the other purposes listed in this Article.

Article 5.1.2.

This Article clarifies that Insurers must properly identify the privacy interests of the Data Subject in the Processing of Health Data and carry out a DPIA for this purpose. Based on this, Insurers assess, among other things, which protective measures they take and whether further Processing is permitted.

Article 5.1.3.

The MA occupies a special place in the Processing of Health Data. After all, the Insurer decides on the acceptance or settlement of claims on the basis of the MA's advice. For that reason, the Code of Conduct separates the assessment of the state of health in the form of an advice from the MA on the one hand and the decision by the underwriter or Claims Handler (CH) of the Insurer on the other. Health statements or medical data from the handling industry must be sent to the MA. It is also the MA's task to assess which additional Health Data are required for an adequate assessment and through which channels these Health Data can be collected. These additional Health Data can only be collected with the explicit consent of the Data Subject. If information is requested from a GP or medical specialist or other care provider, this needs to be done with the consent of the Data Subject concerned.

It may also be necessary for the underwriter and CH to receive certain Health Data from the MA. In this way, the CH and the underwriter can decide, with reasons, whether to adopt the advice of the MA.

The MA determines which relevant Health Data needs to be provided to the Insurer's underwriter or CH. The underwriter and CH may only use these data for that underwriting or claims handling. In case of sick leave insurances, the MA will assess the medical opinion and the compliance with the proposed policy by the UWV. In the context of the performance of the agreement, the MA will advise the sick leave insurer exclusively in the capacity as reintegration company/department, i.e. for the purposes of reintegration. The Code of Conduct applies in full to an occupational consultant, the person who within an insurance company determines the extent to which a person can perform work. The occupational therapist will only ask the Data Subject the questions necessary for the proper performance of the duties. When informing the Data Subject, the Insurer will specifically point out the importance of identification to prevent the exchange of persons, and the possibility of submitting a request to receive the result and conclusion of a medical advice in writing.

Article 5.1.4.

The MA is responsible for the management of the medical file. This provision contains a non-exhaustive list of Personal Data that may be included in the medical file. When assessing or reassessing a claim or insurance application, the MA will pass on the relevant Health Data together with the medical advice to the CH and the underwriter. In this way, the CH and the underwriter can decide, with reasons, whether to adopt the advice of the MA. Insurers record the division of roles and internal responsibilities in the processing register in accordance with Article 3.4 Code of Conduct.

The MA is not responsible for the Processing of Health Data by the CH and the underwriter. Nor is the MA responsible for the Processing of the Health Data relating to a person's health if necessary within the framework of drawing up declarations or within the framework of legal proceedings or the handling of complaints. Health data provided by or on behalf of the Data Subject in connection with the management of the Insurer's relationship with the Data Subject are also not the responsibility of the MA.

The Insurer may not simply record Health Data provided by a Data Subject by telephone in its records, and in such a situation strictly applies the conditions for the Processing of Health Data set out in Article 5.1.1 Code of Conduct. This may involve, for instance, an Urgent Reason in accordance with Section 8 Code of Conduct, whereby the Insurer takes measures with regard to investments or asset management on the basis of its duty of care. For example, forms of serious illness, such as dementia, in which the Insurer protects Data Subjects against their own medical situation. If the occupational consultant spontaneously receives Health Data from the Data Subject, the consultant will not provide these to the underwriter or the CH but will entrust these Health Data to the MA and inform the Data Subject accordingly. If the CH spontaneously receives Health Data from the Data Subject, the CH may not record these data, but will pass these Health Data on to the MA and inform the Data Subject accordingly.

Article 5.1.5.

This provision is a specific elaboration of the general right of inspection in the Processing of Personal Data, which is further elaborated in Article 6.2 Code of Conduct. Regarding Health Data, the Data Subjects are entitled to inspect their medical records. The right of inspection relates to the Personal Data itself and is intended to enable the Data Subject to check the Insurer's and the MA's Processing of the Personal Data. The right of inspection is not intended to assess the creation of the medical advice, and does not include, for example, the MA's internal notes or work notes[8]. Data Subjects may also request access to their medical files through a confidential doctor. An Insurer must also respect the protection of the rights and freedoms of Third Parties when assessing a request for inspection. To comply with a request for inspection, the MA may take appropriate measures (such as obscuring passages in a medical file).

Article 5.1.6.

The Insurer must agree a confidentiality obligation with the underwriter and CH based on applicable legislation and regulations. This provision expresses this obligation.

Article 5.2.1.

An Insurer may process Personal Data of a criminal nature. The underlying purpose of such Processing

[8] See Gelderland District Court, 1 Nov. 2016, ground 2.11, ECLI:NL:RBGEL:2016:6508

is usually the underwriting or implementation of an insurance policy or to safeguard the integrity and security of business operations and the industry. These and other purposes are listed here.

During an application for an insurance, the Insurer will ask about the criminal record of the applicant and others, in so far as this is necessary to effect an insurance policy. The facts requested relate to a period of eight years prior to the application for insurance, under Book 7, Article 928 of the Dutch Civil Code. The Data Subject is obliged to answer the question truthfully. Insurers may only use the reported criminal record to assess the insurance application and to invoke incomplete performance of the applicant's obligation to provide information.

Article 5.2.2.

This Article clarifies that Insurers must properly identify the privacy interests of the Data Subject in the Processing of Criminal Records Data and must carry out a DPIA for this purpose. Based on this, Insurers assess, among other things, which protective measures they take and whether further Processing is permitted. In addition, Insurers always process Criminal Records Data in accordance with the general assessment framework of Article 4.1. of the Code of Conduct.

Article 5.2.3.

Personal Data relating to offences (such as fraud) that have been or are expected to be committed against a Group Company on the basis of facts and circumstances, may be provided by the Insurer within the Group. This also applies to Personal Data that serve to establish possible criminal behaviour towards a Group Company, provided that the data are only provided to officials who need the data to perform their duties, such as Security Matters, as well as to the police and Justice. Such Personal Data may only be provided to organisations outside the Group if they subscribe to and comply with the PIFI.

Article 5.4.1.

In addition to Health Data and Criminal Records Data, Insurers may process other Special Personal Data for the purposes referred to in this provision. The categories of Special Personal Data are listed in Chapter 3 of the Dutch GDPI Act. In the insurance industry, the Processing of Special Personal Data takes place for, among other things, the purpose of archiving the original documents or electronic copies of these. It may also involve Personal Data relating to ethnicity, which may only be used for marketing activities with the explicit consent of a Data Subject. The use of biometric data for identification or authentication purposes may also involve the processing of Special Personal Data, for example for access control purposes. Furthermore, in some cases the Insurer will include the BSN in its administration. This is only done if the Insurer has a legal basis for doing so.

Article 5.2.2.

This Article clarifies that Insurers must properly identify the privacy interests of the Data Subject in the Processing of Criminal Records Data and must carry out a DPIA for this purpose. On the basis of this, Insurers assess, among other things, which protective measures they take and whether further Processing is permitted.

Section 6

Article 6.1.1.

This Article describes the rights of the Data Subject in the Processing of Personal Data by Insurers. The obligation to provide information applies regardless of the purpose or means of the Processing, the underlying reason, and the technology used. In the Dutch GDPI Act, these rights have been improved and extensively listed. As regards the obligation to provide information, which is contained in Articles 12 to 14 of the Dutch GDPI Act, the new legislation provides an extensive list of information that the Insurer must communicate to the Data Subject when Processing Personal Data. These obligations have not been copied in full in Article 6.1 but have been elaborated in more detail in the context of subjects relevant to Insurers and Data Subjects.

The underlying idea of the obligation to provide information is that the Data Subject knows which Personal Data are being processed for which purposes and can thus hold the Controller liable for this Processing. Insurers continually express this obligation to provide information, for example by including an external privacy policy (such as a privacy statement) on the website and by jointly developing this Code of Conduct. The obligation to provide information applies even if the Insurer does not collect the Personal Data directly from the Data Subject, unless the Provider already informed the Data Subject, for example by a privacy statement on the website. This Code of Conduct has already discussed various examples of collecting Personal Data from Third Parties, such as Customer Due Diligence and verifying customer data with Third Parties in the context of Insurers' statutory duty of care under the Wft, Wwft, and other financial legislation.

Article 6.1.2.

The standard is that the obligation to provide information applies unless the Data Subject is 'already aware'. Depending on the circumstances, the Controller may assume 'being aware', for example because the relevant information has been handed over or sent to the Data Subject or because the behaviour of the Data Subject shows that they are aware. Informing the Data Subject may also be omitted if the Insurer cannot reasonably be expected to inform the Data Subject. This may be the case, for instance, in the event of a suspicion of insurance fraud. Insurers must restrictively apply exceptions to the main rule of the duty to provide information. Furthermore, in such exceptional situations, Insurers will make every effort to inform the Data Subject afterwards, for example after a Personal Investigation in the context of possible insurance fraud has been completed.

Article 6.1.3.

In addition to the requirements of applicable legislation and regulations, Insurers recognise the importance of transparent, open, and honest information provision to Data Subjects. The reliability of the business and the industry as a whole will benefit from this. In addition, Insurers can offer several layers of information to Data Subjects, to ensure that the first layer provides clear and concise information on each subject and the underlying layers provide more detailed information. Insurers value the innovative provision of information to those involved, for example via internet portals such as 'My Environment'.

Article 6.1.4.

This provision endorses the importance of the Code of Conduct's obligation to provide information in the further Processing of Personal Data. A common example in practice is the use of collection agencies to collect the premium. If this is the case, the Insurer informs the Data Subject accordingly.

Article 6.1.5.

The Data Subject is entitled to obtain information on all elements of Processing referred to in this Article which are based on fully automated decision-making. If, for example, Insurers use a credit scoring system established by external investigating agencies, they will inform the Data Subject of this and of the categories of Personal Data on which the decision is based. They will also inform the Data Subject of their right to object, to have the decision reviewed by a human being and of the factors underlying the automated decision-making process. The publication of this 'logic' of automated decision may not prejudice any business-sensitive information or the intellectual property rights of the underlying software and algorithms. However, Insurers cannot use these grounds for exception to limit the disclosure of information to the Data Subjects and seek to strike a reasonable balance in this regard.

The starting point remains the provision of comprehensible and relevant information on the automated decision-making process, which enables the Data Subject to assess the decision-making process and exercise the rights granted by Section 6 Code of Conduct.

Article 6.2.1.

A Data Subject is entitled to ask an Insurer in writing for an overview of the Processing of Personal Data. This overview must contain a description of the purpose of the Processing, the categories of Personal Data to which the Processing relates, the recipients or categories of recipients, and the available information on the origin of the Personal Data.

This provision describes the information that an Insurer must provide in response to a valid request for inspection. As described in Article 5.1.5 Code of Conduct, the right of inspection relates to the Personal Data itself[9]. The right of inspection does not extend to files on the Data Subject, entire documents, reports of internal deliberations, internal notes, or work notes. Nor does it include electronic communications between the Insurer and the Data Subject.

Article 6.2.2.

The Controller must provide this summary to the Data Subject within one month of the date of receipt of the request. In the event of complex requests for inspection, the Insurer may postpone the response to the request by two months. These periods will be put on hold for as long as the Data Subject does not enable the Insurer to comply with the request for inspection, for instance if the Insurer still needs to identify the Data Subject but does not receive proof of identity. For a request for inspection, the Controller may demand reimbursement of the costs if the request is manifestly unfounded or excessive, for example because of its repetitive nature. For the time being, this amount has been set at €0.23 per page up to a maximum of €5.00 per insurance policy. This amount may rise to a maximum of € 22.50 in case of processing that is difficult to access due to its nature or in case of multiple insurances.

Article 6.2.3.

An Insurer does not have to comply with a request for inspection if there is an Urgent Reason. An Insurer may refuse inspection if, for example, the safety of the Insurer and the prevention, investigation, and prosecution of criminal offences are at stake. In addition to the provisions of Section 8 Code of Conduct, the request for inspection may be refused if there is any misuse by the Data Subject, if it results in a

[9] See Gelderland District Court, 1 Nov. 2016, ground 2.11, ECLI:NL:RBGEL:2016:6508

disproportionate burden on the Insurer, or if it affects the rights or interests of a Third Party who may have objections to the granting of inspection. In that case, an Insurer may decide not to provide such Personal Data or to block them out.

Article 6.2.4.

Under applicable legislation and regulations, the Controller must ensure a proper determination of identity to ensure that the correct person has access to their own Personal Data. In the event of written requests for access appropriate measures must therefore be taken, such as the obligation to enclose a copy of a passport or driving licence to be able to compare the signatures, possibly with signatures already present. The Data Subject may block the citizen service number and cover the photograph. Insurers can also use generally accepted identification methods to establish the identity of a Data Subject, such as the IDIN.

Article 6.3.1.

The Data Subject may request the Insurer to correct, supplement, remove, or limit the Personal Data if they are factually incorrect, incomplete, or irrelevant for the purpose or purposes of the Processing, or are processed in any other way in breach of a statutory provision. The limitation concerns situations in which the Personal Data cannot be removed because, for example, they may have to be used in a procedure. In that case, appropriate measures must be taken to prevent any other use. If an Insurer has complied with a request to correct, supplement, delete, or limit data, it is obliged to inform Third Parties who have previously become aware of the Personal Data concerned of the changes made, unless this is impossible or requires a disproportionate effort. The Insured must also take the interests of Third Parties into account when responding to the request. In case of employer insurance plans, for example, in which the employer is the Insured and the Insurer's customer, while the employee is the Data Subject, an Insurer cannot simply delete the Personal Data of the Data Subject.

Article 6.3.2.

The Data Subject has the right to object to the Processing of Personal Data if the legal basis of the Processing is to protect the legitimate interests of the Controller. The Data Subject may then request to terminate the Processing of their Personal Data on the basis of their particular personal circumstances. In that specific case, the Controller must reconsider the Processing and weigh its interest against the interest or special interest of the Data Subject. Even if Personal Data are processed for scientific, historical, or statistical purposes, Data Subjects have the right to object to the Processing of Personal Data relating to them for reasons relating to their specific situation.

If a Data Subject objects to Processing for marketing purposes, Insurers must terminate the Processing immediately. Insurers will periodically check whether the Data Subject has been included in the register referred to in Article 11.7(6) Telecommunications Act.

Article 6.3.3.

Under applicable legislation and regulations, the Controller must ensure a proper determination of identity to ensure that the correct person has access to their own Personal Data. The Insurer may ask for a copy of a passport or driving licence to be enclosed to be able to compare the signatures, possibly with existing signatures. The Data Subject may block the citizen service number and cover the photograph. Insurers can also use generally accepted identification methods to establish the identity of a Data Subject, such as the IDIN.

Article 6.4.1.

This Article expresses the new right to data portability from the GDPR. In the insurance industry, this right to move Personal Data will primarily be aimed at taking out an insurance policy with another Insurer. In addition, the GDPR requires that Personal Data can also be moved to other service providers or to the Data Subject. These are, in fact, Personal Data generated by the Data Subject when taking out the insurance. Data portability does not apply to profiles, credit scores and information resulting from analyses carried out by the Insurer.

Personal Data processed on a basis other than consent and in connection with effecting or implementing the insurance policy, for example, to ensure the integrity and security of the industry and to prevent possible fraud, are excluded from the scope of this provision.

Article 6.4.2.

The receiving Controller will have to assess whether the sending Insurer has sent the correct Personal Data and whether the data file received is not excessive. On 23 April 2018, SIVI, the Knowledge and Advice Centre for the Insurance Industry (*Stichting Standaardisatie Instituut voor Verzekeringen in de Intermediairbranche)* published a safe and machine-readable standard for data portability for the insurance industry. The '*Poliskluis van het Verbond*', a tool for viewing and moving Personal Data, is a way for the Data Subject to move Personal Data between Insurers and can be a way for Insurers to make moving Personal Data easy for the Data Subject.

Article 6.4.3.

Under applicable legislation and regulations, the Controller must ensure a proper determination of identity to ensure that the correct person has access to their own Personal Data. The Insurer may ask for a copy of a passport or driving licence to be enclosed to be able to compare the signatures, possibly with existing signatures. The Data Subject may block the citizen service number and cover the photograph. Insurers can also use generally accepted identification methods to establish the identity of a Data Subject, such as the IDIN.

Section 7

Article 7.1.1.

Storing on or accessing information in the Data Subject's peripherals is subject to legal regulations. The Data Subject here means the user (natural person or legal entity) who, within the meaning of the Dutch Telecommunications Act, uses or requests a public electronic communications service. The starting point of the Telecommunications Act is that it is not permitted to read or copy personal information from, for example, the Data Subject's computer or smart phone, without the knowledge and informed consent of the Data Subject. There are also exceptions to this rule. For example, it is permitted to place or read technically necessary cookies and cookies that have hardly any impact on the Data Subject’s privacy. If Personal Data are processed during storage on or access to information in the user's peripheral equipment, the rules of the applicable privacy legislation apply in full in addition to the provisions of the Telecommunications Act.

Technology relating to the use of cookies is changing rapidly. It cannot be ruled out that technical and other developments during the term of this Code of Conduct will lead to changes in the regulations on cookies. Insurers will ensure that they keep abreast of and comply with these changes.

Insurers will provide information on the purposes of the collection of the data on the Data Subject's peripheral equipment in a transparent manner and in understandable language. For each purpose, Insurers will specify the categories of data, the retention period, the basis for processing Personal Data, and the rights of the Data Subject in accordance with Article 6 Code of Conduct. The Data Subject will receive a clear notification about the collection of data via peripherals with a direct link to the policy referred to in this provision.

Article 7.2.1.

Insurers attach great importance to the careful security of Personal Data. Each Insurer develops a security policy, which specifically indicates which organisational and technical measures have been taken to protect Personal Data against unauthorised access. In determining the appropriate security level, the state of the art, the costs of implementation, the risks involved in processing, and the nature of the Personal Data to be protected are taken into account. In doing so, Insurers follow the Personal Data Security Guidelines of the Dutch DPA and the Information Security Assessment Framework of DNB. Periodic audits and quality controls also form part of the security policy. Insurers ensure compliance with this policy in accordance with the Plan-Do-Check-Act methodology of the Dutch DPA's Personal Data Security Guidelines. The Association has also drawn up a Responsible Disclosure Guide to stimulate the security of Personal Data in the industry.

Article 7.3.1.

In accordance with applicable legislation and regulations and the Policy on the Duty to Report Data Leaks, Insurers report data leaks to the Dutch DPA. Insurers are excluded in privacy legislation from the obligation to report data leaks directly to those involved but may be obliged to do so under the Wft and regulations on financial supervision. The relevant regulator of the duty of care under the Wft is DNB. Insurers regularly consult with DNB in the context of financial supervision. This provision is short, because the legislation and the policy rules on the duty to report data breaches in the Dutch DPA clearly describe the legal requirements.

Article 7.4.1.

The word '*gegevensbeschermingseffectbeoordeling*' is the Dutch translation in current legislation and regulations for the better-known professional term 'data protection impact assessment'. Recently, European regulators have further elaborated on the new statutory obligations for carrying out a DPIA. Insurers will implement these further explanations of the supervisors in their business operations. In short, Insurers must assess the effects of a Processing if the Processing might pose a high risk to the privacy of the Data Person or Data Persons. This might be the case in systematic profiling (such as the risk assessment of prospective Insured Persons), large-scale processing of Special Personal Data and further Processing of Personal Data, for example for marketing purposes, if these Personal Data were originally collected prior to taking out an insurance policy (and not after valid express consent of a Data Subject for this purpose). In their explanation, the European regulators listed nine factors that Insurers will weigh in their decision to carry out a DPIA[10].

[10] These nine factors can be found at: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

Article 7.4.2.

As soon as Insurers carry out a DPIA, they seek advice from the DPO. In the analysis, they take into account at least the aspects listed in this provision.

Article 7.5.1.

Insurers draw up a precise policy with regard to the retention and archiving of Personal Data. In view of the nature of insurance and the importance of historical and statistical data for risk assessment and the settlement of claims, Insurers are often required to keep Personal Data longer than companies in other industries.

Insurers should always ask themselves whether there are any reasons why Personal Data should be retained. Personal Data are not kept longer than necessary for achieving the objectives for which they were collected or subsequently processed. Examples of retention objectives are to comply with legal retention obligations, to provide evidence in the event of disputes and to have access to data for carrying out investigations. An Insurer draws up a policy with regard to the retention periods of the Personal Data, the removal of the Personal Data, and the possible transfer of these Personal Data to an archive destination. In the latter case, the Personal Data is only to be used for archive management, the handling of disputes, and to conduct scientific, statistical, or historical research.

Article 7.6.1.

With pseudonymisation, Insurers replace directly identifying data of a Data Subject with other means of identification, such as an IP address, user name, or customer number. For example, by replacing the name of a Data Subject by a meaningless customer number, Insurers make it more difficult to re-identify the Data Subject, both for its staff and for cyber criminals after a cyber-attack. Pseudonymised data are still Personal Data, because a pseudonym can indirectly identify a natural person. By pseudonymising, Insurers protect the privacy of the Data Subject and for that reason Insurers may use an adequately pseudonymised dataset, for example, to make historical, statistical or scientific analyses, in accordance with Article 4.3 Code of Conduct. Pseudonymisation is also an important tool for data file security. The Insurer should keep the original dataset separate from the pseudonymised dataset, restrict access to the original dataset, both technically (via e.g. encryption) and organisationally (only a limited number of staff members).

Article 7.7.

Insurers may make use of camera monitoring for the purposes referred to in this provision. For example, camera monitoring is permitted when it is necessary for the security of an Insurer or its business relations and employees, for the detection of offences or the determination of violations of (company) rules, and to support legal proceedings. Furthermore, recordings must be selective, the data must not be kept longer than necessary, and the necessary organisational and technical measures must be taken to protect Personal Data. If the Data Subject so requests, further information will always be provided. Inspection can also be understood to mean requesting inspection of the images referred to here. In that case, however, an applicant may be required to indicate the date and time of the contact. If the images also contain information about other natural persons, these images will not be provided to the Data Subject.

Article 7.8.1.

Insurers may record communications for the purposes referred to in this provision. Insurers record communication data on various occasions. The main reason to record communication is that instructions are increasingly being given by means other than the traditional written and oral means. Electronic means of communication play an increasing role, such as the internet and chat. These include entering into contracts, issuing orders, making notifications, or requests for information. The recording of telephone conversations is permitted to perform a legal obligation, to provide evidence, for fraud and other investigation and detection, to evaluate the quality of service, and for training, coaching and assessment purposes. Often the recording of a telephone conversation is the result of a legal obligation. Other examples of reasons for recording telephone calls are that the Insurer may subsequently determine the content of the assignment, if this is necessary in the context of a dispute with a Data Subject, for example, or to determine the exact time at which the loss or theft of an asset was reported, or to deal with threats directed against the Insurer or its staff members.

Article 7.8.2.

Insurers will inform the Data Subject of the recording of this communication at the time of acquisition. Insurers will also instruct staff to provide information about the recording of communications. If the Data Subject so requests, further information will be provided at all times. Furthermore, the data will not be kept longer than necessary and the necessary organisational and technical measures must be taken to protect the Personal Data.

Article 7.8.3.

Inspection may also include requesting inspection of communications referred to herein. In that case, however, an applicant may be required to specify the day and time of the conversation or contact, the telephone number used by the Data Subject and an indication of the telephone number called by the Data Subject. The Insurer is not required to grant inspection if the conditions referred to in Section 8 Code of Conduct are met.

Article 7.9.1.

Insurers can outsource the Processing of Personal Data to Processors. For example, Insurers frequently use IT service providers for maintenance and support functions. These IT service providers are to be regarded as Processors as soon as they have no independent control over the Personal Data made available to the IT service provider as part of the provision of services. In that case, the Insurer must make arrangements with the Processor, which arise on the one hand from applicable privacy laws and regulations and on the other hand from legislation and regulations in the area of financial supervision. An important part of the agreements concerns the security of the Processing of Personal Data. In the event of outsourcing, the Insurer generally remains the Controller. However, there are also conceivable situations in which both parties remain the Controller. In case of pension agreements entered into by the employer for the benefit of their employees, the employer, and the Insurer (and, where applicable, the intermediary) are independent Controllers.

Regulations in the field of financial supervision also set requirements for the quality of data processing. Financial supervisors such as DNB supervise the quality of outsourcing. If the Processor is established outside the European Economic Area (EEA), the outsourcing Insurer must also comply with the additional requirements for the transfer of Personal Data in accordance with Article 7.11 Code of Conduct. If the Processor uses cloud technology, the Insurer will identify where the Personal Data will ultimately be

processed, and will therefore make arrangements with the Processor that offer certainty with regard to compliance with the agreements and the agreed level of security. This obligation also applies to any sub-processors, i.e. the suppliers to whom the Processor outsources parts of the services. The Insurer must lay down these agreements in a Processor Agreement, in addition to the categories referred to in Article 28 GDPR.

Article 7.10.1.

As a rule, Insurers process Personal Data within the EEA and the GDPR applies in full to such processing. Sometimes Insurers process Personal Data of the Data Subject outside the EEA, for example because a Processor or a Group Company is established outside the EEA. In such cases, Insurers will take the safeguards required by law to guarantee an adequate level of protection. The stratification of the regulations for the transfer of Personal Data to countries outside the EEA is different for Insurers than for other Controllers. Processing outside the EEA is often necessary for, among other things, the performance of an agreement between a Data Subject and the Controller, or the conclusion or performance of an agreement to be concluded in the interest of the Data Subject. This may involve, for example, reinsurance or the exchange of information in connection with damage or an accident abroad. It may also be passed on if clear consent has been obtained from the Data Subject or if it is necessary in connection with an overriding public interest. As a rule of thumb, the Insurers assume that the Personal Data of the Data Subject outside Europe enjoy the same level of protection as in the case of Processing by the Controller itself, within Europe.

Article 7.11.1.

Data Subjects who purchase products from one part of a Group may be approached by that part, but also by other parts of that Group, for service messages, marketing or other purposes. All provisions of the Code of Conduct will of course continue to apply. If the activity does not result from the purpose of the activity for which the Personal Data has been collected, it must be verified whether the intended Processing is compatible with it. In addition to the customer's interests, the extent to which the customer is informed about the composition of the Group also plays a role in this assessment. This can be done, for example, by using commercials or by mentioning the composition of the Group in communications to the customer. If it is made sufficiently clear to a customer that the Insurer is part of a Group, the customer may be approached by any of the Group's entities for marketing activities. Marketing of products or services offered in the market by the same Group may therefore be regarded as related. The customer always has the right to object to the processing by a Group Company.

Section 8

The principles and provisions set out in the Code of Conduct, such as the purpose-limitation principle, the principle of transparency, and the rights of those concerned, should give way in special cases where there is an urgent need to do so. These Urgent Reasons are listed in Article 8.1.1. This applies, for example, if an Insurer is subject to investigation by a competent supervisory authority or the tax authorities. Even in case of an incident investigation of a Data Subject by the Insurer, the interests of the investigation may outweigh the privacy interests of the Data Subject, since informing the Data Subject at an early stage may frustrate an incident investigation. Insurers apply the ground for exception of the Urgent Reason restrictively. The need to deviate from the general provisions of the Code of Conduct must always clearly outweigh the rights and freedoms of the Data Subject.

Section 9

Article 9.1.1.

In principle, Insurers appoint a DPO within their organisation. The DPO advises the Insurer on the structure and content of the privacy policy and the Processing of Personal Data in business operations. The DPO may be employed by the Insurer or hired externally, as long as the DPO operates independently and receives no instructions from the Insurer in connection with the performance of their duties.

The DPO does not affected negatively in the performance of the duties and is protected against dismissal or termination of the contract for the provision of services due to a difference of opinion. The DPO has the required knowledge and capacities to perform the task properly, in particular, relevant work experience in the field of Personal Data Protection. The DPO has access to all systems where any Personal Data may be processed. The DPO may also be the first point of contact for the Data Subject in the event of complaints about compliance with the Code of Conduct, which may be submitted in accordance with Article 9.3.1. Code of Conduct.

An insurer may refrain from appointing an DPO if the provision of services or the range of products gives cause to do so. The 'apply or explain' principle applies here. Deviating from the obligation requires a careful balancing of interests, in accordance with the GDPR and the relevant opinions of the (national) privacy supervisor. It is important to take the fact into account that an insurer that processes medical data is often subject to the obligation to appoint a DPO.

Article 9.2.1.

Insurers ensure compliance with this Code of Conduct and applicable laws and regulations. Insurers take the following specific measures to ensure compliance:

(a) The Insurer designates a department (e.g. the audit department) to periodically, preferably annually, assess compliance by self-assessment.

(b) The Insurer's management takes responsibility for compliance.

(c) The supervising department (e.g. the compliance department or the DPO) is responsible for compliance.

Where the DPIA checks the Processing of Personal Data for specific Processing, Insurers can also carry out internal investigations (such as audits) to assess compliance. Depending on the results of these audits and the nature and scope of the individual Processing of Personal Data, such internal audits will determine which parts of the investigation need to be supplemented.

To promote compliance, an Insurer is also required to draw up and implement an internal privacy policy. This policy indicates the manner in which Personal Data must be processed. The instructions in any event cover those subjects of which the internal investigation establishes that further policy is desirable. In practice, these documents are security manuals in which the technical and organisational measures for the security of Personal Data are described. Another common example is an internal regulation on the recording of telephone calls, in accordance with Article 7.8 Code of Conduct.

Article 9.3.1.

Every Insurer has an internal procedure for handling complaints. The time limit provided in applicable legislation and regulations applies to the response to complaints. The entire procedure is explained in more detail below.

Article 9.3.2.

The Association is a member of the Financial Services Complaints Institute (Kifid) The aim of this independent institute is to provide a one-stop shop for resolving conflicts with financial institutions. The Ombudman and the Disputes Committee working within Kifid offer an alternative to going to court. In a relatively short time an attempt is made, in consultation with the service provider concerned, to find a solution or to decide on the matter.

If the Data Subject has submitted a complaint to the Insurer and the complaint is not, or not satisfactorily, settled, the Data Subject may submit the dispute to Kifid within three months of such settlement. If the dispute relates to the right of inspection or correction and is submitted to Kifid within six weeks of the decision of the Insurer's internal dispute procedure, the six-week period within which the Data Subject has the right to submit the case to the Dutch DPA or to apply to the court will be suspended (counting from the date of submission until the end of the procedure with Kifid) under applicable legislation and regulations. If the Data Subject only submits a dispute to Kifid after the expiry of the six-week period, the Data Subject can no longer make use of the procedure laid down in the applicable privacy laws and regulations.

A Data Subject may also choose to ignore the Insurer's internal dispute resolution. The Data Subject may submit a dispute directly to the Dutch DPA or to the court that has jurisdiction. The right to resort to the Insurer's internal dispute procedure, and subsequently Kifid, will lapse as a result.

For more information about the Kifid we refer to the following website: www.kifid.nl or Klachteninstituut Financiële Dienstverlening, P.O. Box 93257, 2509 AG The Hague. If you have any questions about the Code of Conduct you can also contact the Association: Verbond van Verzekeraars, P.O. Box 93450, 2509 AL The Hague, telephone 070 – 333 8500 or by email: Gedragscode_Privacy@verzekeraars.nl.

Section 10

The terms used in this Code of Conduct are consistent with the terms used in applicable legislation and regulations. In addition to the definitions included in the Code of Conduct, the definitions in applicable legislation and regulations apply in full when interpreting the Code of Conduct. Some terms are specific to the insurance business and are not defined by law, such as MA, Safety Matters and Insured. For the proper understanding of this Code of Conduct, some key terms from Section 10 below have been elaborated in more detail below.

Data Subject

The Data Subject is the person to whom certain Personal Data relate. The Data Subject is often the same person as the policyholder with whom the Insurer has effected an insurance policy. However, there are also many situations in which this is not the case. Simply including the term Insured in this Code of Conduct would therefore not be a good idea. Take the situation in which the employer takes out employer insurance on behalf of all employees. The employer is then the Insurer's customer, but the Personal Data of employees must also be protected. In addition, the Processing of Personal Data in the context of an insurance often affects more than one person. Tink of current or prospective Insured persons, beneficiaries, co-insured persons (e.g. family members) and persons holding an Insured Person liable.

By using the broader concept of Data Subject, this Code of Conduct expresses the fact that Insurers also protect the Personal Data of this wider circle. The Data Subject is therefore a flexible concept and may include, depending on the facts and circumstances of the case:

(a) persons with whom an insurance has been effected (the policyholder) or those insured under the agreement (Insured Persons);

(b) persons with whom an insurance policy has been effected in the past (including Insured Persons) and whose Personal Data still have to be processed;

(c) persons approached to take out insurance;

(d) persons who approach an Insurer themselves by requesting information or a quotation;

(e) persons of whom an Insurer has to process Personal Data on the basis of a statutory regulation (for example the consent of the spouse under Book 1, Article 88 Dutch Civil Code) or because of applicable statutory limitation periods;

(f) persons involved in an Incident (e.g. the injured party in case of damage);

(g) persons in respect of whom an Insurer is required to process Personal Data in connection with contractual or statutory obligations;

(h) a visitor to the company premises.

Group/Group Company

Insurers may attribute responsibility within the company to a party (e.g. the parent company) that is not directly involved in the operational Processing of Personal Data (e.g. a subsidiary). If an Insurer is part of a Group, another legal entity within the Group may therefore be the Controller. In that case, by means of articles of association or an agreement, a specific legal entity within the Group is granted the authority to determine the purpose and means of the Processing of Personal Data within the Group. If the Controller is not determined, the entity that must be attributed the Processing of Personal Data in accordance with the standards in force in society acts as the Controller.

Processor

The Processor processes Personal Data on behalf of the customer, the Controller. The Processor has no control over the Processing, but merely follows the instructions of the Controller. Insurers have, for example, invested the storage of Personal Data to a large extent with cloud providers. These cloud computing service providers usually have no independent power to use the Personal Data entrusted to them for other purposes. A cloud provider is therefore usually a Processor. Another example of a Processor is the Foundation Central Information System (*Stichting Centraal Informatie Systeem*).

The Controller

The Controller is the legal entity that determines the purpose and means of the Processing and has formal authority to take decisions on the Processing of Personal Data. The Controller is also the legal person who is liable if the current legislation and regulations are not or incorrectly complied with. In principle, the Insurer with which the Data Subject takes out insurance acts as the Controller.

12. The Association

The Association is the interest group of general and life Insurers in the Netherlands. It also includes companies that specialise in bank savings for old age and premium pension institutions. Together, the members of the Association represent more than 95 percent of the insurance market. The Association acts on behalf of the affiliated Insurers as a discussion partner for politicians, the media and other relevant parties on issues that affect Insurers.

As an industry organisation, the Association has the following four main objectives:

1. Representing its Members

The Association is primarily a representative of private Insurers and companies involved in bank savings and premium pension institutions. On behalf of its members, the Association acts as an interlocutor for politicians, the government, and other national and international organisations. Together with these other parties, the Association seeks common ground to find solutions to problems.

2. Promoting the image of the insurance industry

Communication plays an important role in the promotion and maintenance of the good name of the insurance industry in the Netherlands. The Association coordinates the PR of the entire industry, expresses its policy to the media and responds to developments.

3. Providing a platform

To carry out the role of representative of the industry, support is, of course, required. The Association creates this support by, for instance, organising meetings for representatives of the industry. The Association regularly holds full day events for its members on topical issues that require the attention of Insurers. The general policy is discussed during the members' meetings. All these meetings also have a social function: members can meet each other.

4. Services

Advocacy also means being there for your members. Because of its representative role, the Association is aware of relevant developments and therefore acts as a knowledge centre for its members. The members are kept informed through various channels. Because the Association coordinates the collective interests that affect the entire industry, it has an advisory function for the policy to be pursued. Would you like to know more about the kinds or service we have to offer our members? Visit our website: www.verzekeraars.nl.