Legal Framework

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter as "GDPR"), with the effective date of 25 May 2018, and **Act No. 110/2019 Coll., on personal data processing** and on amendment of certain act, as amended, which came into effect on 24 April 2019, make up the legal framework for personal data processing in the European Union and, naturally, in the Czech Republic as well.

Personal data protection is further governed by other laws and regulations, such as:

- Convention on protection of persons with regard to automated processing of personal data No. 108, issued under No. 115/2001 Coll. of the Ministry of Justice.
- Act No. 277/2009 Coll., on insurance, as amended
- Act No. 170/2018 Coll., on insurance and reinsurance distribution, as amended
- Act No. 37/2004 Coll., on insurance policies and on amendment of related acts, as amended
- Act No. 253/2008 Coll., on certain measures against money laundering and terrorism financing, as amended
- Act No. 164/2013 Coll., on international cooperation in tax administration and on amendment of other related acts
- Act No. 480/2004 Coll., on certain information society services, as amended
- Act No. 89/2012 Coll., the Civil Code, as amended
- Act of the Czech National Council No. 582/1991 Coll., on organisation and implementation of social security, as amended
- Act of the Czech National Council No. 589/1992 Coll., on social security insurance premiums and on contribution to government employment policy, as amended
- Laws and regulations related to labour law and employment
- Laws and regulations related to social security and health insurance
- Accounting, tax, and controlling laws and regulations

Fundamental terms

In the context of insurance, the fundamental GDPR terms are as follows:

Personal Data (PD) – any information concerning a specific individual (data subject) whether these are identification and contact details (name, surname, date of birth, residential address, birth certificate number, business ID No./VAT ID, phone number, email, location data, descriptive physiological data (e.g.
height, weight, shoe size), information from photographs and CCTV records, sociodemographic data (age, sex, marital status, education, employment, income and spending, number of children), or data about the data subject's behaviour and preferences.

Special categories of personal data (formerly sensitive personal data) – certain personal data posing an especially high risk in terms of infringement upon guaranteed rights and freedoms of individuals, such as data about one's health condition, racial or ethnic origin, political views, religious or philosophical beliefs, and genetic and biometric data.

Data subject – any subject whose PD are processed.

Processing – any handling of personal data such as their collection, recording, publication, storage, arrangement, searching, alteration, use, distribution etc. Typical examples include keeping of files (digital and physical), keeping of records on insurance claims, AML-related documentation etc., both as part of the client agenda and the insurance company's administrative activities (e.g. HR matters).

Controller – any natural person or 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; in the case of insurance activities,

insurance companies act as controllers.

Processor – natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, if tasked with such processing by the controller, only to the extent determined by the controller and for the set purposes; one person may be both the controller (for instance in relation to such person's employees) and the processor (in relation to another controller).

Joint controllers – controllers who jointly determine the purposes and means of personal data processing.

Recipient – means any entity with whom personal data are shared (irrespective of whether such entity is directly a controller or by a processor upon a controller's instruction); in certain cases, public authorities are considered to be recipients.

Rights in personal data processing – to withdraw consent to the processing, right to demand access to one's PD, right to rectification or erasure of PD, restriction of processing, right to PD transfer, right to lodge a complaint with a supervisory authority.

Right to object – if processing is based on the controller's legitimate interest or performed in public interest or in exercise of public authority, the data subject is entitled to object to such processing at any time; the data subject is also entitled to object to processing for direct marketing processing, in which case the controller is obliged to terminate the processing of the PD concerned.

Consent to processing – any freely-given, specific, informed and clear expression of will by which data subjects, by a declaration or by any other clear confirmation, gives consent to the processing of their PD. The data subject has the right to withdraw such consent. Processing of PD without the data subject's consent is possible if such processing is needed to meet a legal obligation or fulfil a contract.

OPDP– Office for Personal Data Protection, a controlling and supervisory authority under GDPR in the Czech Republic, with its registered office at Pplk. Sochora 27, 170 00, Prague 7, phone: +420 234 665 111, web: www.uoou.cz.

Records of data processing activities – each controller of personal data is obliged to keep records on personal data activities such controller is responsible for. GDPR requires formal keeping of records on processing activities especially from large organisations (of more than 250 employees). However, as records must be kept by every controller and processor (irrespective of the number of employees), if

a) the processing of the PD is likely to pose a risk for the rights and freedoms of data subjects,
b) PD processing is not occasional, or
c) the processing includes processing of special categories of data or personal data concerning criminal convictions and criminal offences, such obligation to keep formal records will concern all insurance companies. In doing so, insurance companies must consider the context, sensitivity, and scope of the personal data kept on file, so that they can demonstrate their compliance with the GDPR in case of an inspection by the OPDP.

DPO – data protection officer is a sort of an internal auditor for personal data processing and protection; DPO oversees whether personal data are processed and protected in accordance with the GDPR. There is no general obligation to appoint a DPO (however, DPO may be appointed voluntarily). The insurance company's data protection officer may be contacted by any of the following means: by email at dpo@maxima-as.cz, in writing at the address Italská 1583/24, 120 00 Praha 2, and via the client line +420 273 190 400.

Reporting of security incidents – GDPR sets out the controller's obligation to report breaches of personal data security and integrity and to report losses of personal data to OPDP without undue delay and, if possible, within 72 hours after learning about such breaches or loss; only incidents of low-risk for personal data subjects are not subject to this reporting obligation. In addition, controllers must report such breaches immediately to all data subjects concerned if it is likely that the breach of personal data security will pose a high risk for the rights and freedoms of natural persons. Incidents may be are to be reported by email to po@maxima-as.cz or via the client line +420 273 190 400.