AXA Foundation
for Occupational Benefits

Occupational benefits

Data protection regulations

AXA Foundation for Occupational Benefits, Winterthur

L1287.004-09.23

These data protection regulations were issued by the Board of Trustees of the AXA Foundation for Occupational Benefits, Winterthur, ("Foundation") on the basis of section 2 of the deed of foundation and section 10 of the applicable organizational regulations.

Purpose

1

Employees, customers, insureds, benefit recipients, and other persons whose personal data is processed by the Foundation, expect it to use their personal data in a responsible and lawful manner.

When processing personal data, the Foundation complies with the applicable law and with these data protection regulations. These regulations establish general principles for the handling of personal data and are binding on all the Foundation's governing bodies, and on the employees delegated to the Foundation or directly employed by the Foundation ("**employees**").

Legal framework

2

The most important laws applicable to the handling of personal data are:
- the Federal Act on Data Protection (FADP) and the associated ordinance,
- the Federal Act on Occupational Old Age, Survivors' and Invalidity Pension Provision (BVG/OPA) and the associated ordinances, and
- the Federal Act on the Vesting of Occupational Old Age, Survivors' and Invalidity Benefits (FZG/VBA) and the associated ordinances.

Duty of confidentiality in relation to occupational benefits

3

The duty of confidentiality applies to all knowledge gained regarding the personal and financial circumstances of the insureds and the employers. The disclosure of data relating to occupational benefits complies with the specific requirements of Art. 86a OPA.

Definitions

4

The terms "personal data" and "processing" are of central importance in data protection. The provisions on data protection in these regulations must be complied with whenever **personal data is processed**.

Personal data
Personal data is information ("data") relating to an identified or identifiable natural person ("data subject"). It thus presupposes a reference to an individual, which may only become clear in the specific context. It makes no difference whether personal data is stored electronically or on a physical medium.

Personal data includes, for example:
- Contact details such as last names, first names, address, email address, telephone number
- Information about characteristics, behavior, performance, sensitivities, preferences, personality, opinions, and about social, family, or economic interactions
- Identification data such as IP addresses, passport number, AHV number, insured person number, or fingerprints
- Images or recordings that could be traced back to individuals.

Processing
Broadly speaking, processing personal data means handling personal data in any way (electronically or physically). Examples:
- Preservation, storage, and archiving
- Collecting/procuring
- Access
- Forwarding/transmitting to third parties (such as use of a cloud solution or data access by an external service provider)
- Evaluation/analysis
- Publication
- Deletion/destruction
- Anonymization/pseudonymization.

Personal data is processed online using tracking tools, social media, and cookies, in particular. Applications such as application platforms, e.g. those used for elections to the Board of Trustees, will always contain personal data. Personal data is also processed when personnel files are kept.

Especially sensitive personal data
Personal data that falls into the (definitive) category of personal data requiring special protection is subject to stricter processing rules (see below).

Especially sensitive personal data relates to:
- Health
- Religion
- Ethnicity/race

– Political/philosophical beliefs
– Private life (sexual orientation/sex life)
– Trade union-related opinions or activities
– Genetic/biometric data
– Social assistance measures
– Criminal proceedings/offenses[1].

Profiling
Any kind of automated processing of personal data that consists of using this data to assess specific characteristics of a natural person, particularly when this is done in order to analyze or predict aspects relating to this natural person's performance at work, financial situation, health, personal preferences, interests, reliability, behavior, place of residence, or change of location.

High-risk profiling
Profiling that incurs high risk for the data subject's privacy and fundamental rights because it leads to data being linked in such a way as to permit the evaluation of essential aspects of a natural person's personality.

Principles 5

Fairness
Personal data is processed fairly and only in the manner that the data subject is entitled to expect.

Transparency
When personal data is obtained from the data subject or from other sources, the data subject is informed about the processing of their data in an active, timely, detailed, and comprehensible way.

Purpose
Personal data may only be obtained for a specific purpose that is evident to the data subject; it may only be processed in a manner consistent with this purpose. (Example: The email address entered in a contact form may not be used for sending a newsletter.)

Data minimization
The collection of personal data must be limited to the amount necessary. In addition, personal data should be anonymized or pseudonymized where possible. (Example: When responding to a broker's request for a quotation on behalf of an employer, it is not routinely necessary to pass on the first names and last names of the insureds.)

Storage period
Personal data may only be stored for the period that is necessary in order to carry out the processing purpose. (Example: A deletion policy ensures that personal data is deleted after a specific period has expired.)

Correctness
Personal data must be factually correct and kept up to date.

Security
Personal data must be treated confidentially and protected from unauthorized destruction, loss, alteration, or disclosure by means of appropriate technical and organizational measures. (Examples: keeping logs, hardware encryption of mobile devices)

Legal basis
Data processing needs to be founded on a specific legal basis when one of the above-mentioned principles is breached, particularly sensitive personal data is disclosed to a third party, or personal data is processed against the explicitly declared wishes of the data subject.

Specific legal bases include:
– legal provisions (e.g. statutory retention periods for accounting documents)
– a direct connection with the conclusion or performance of a contract with the data subject concerned
– our overriding interest in processing the data when this interest is so serious that it outweighs the opposing interests of the data subject
– the consent of the data subject.

In the field of occupational benefits, personal data may generally only be processed if a legal basis for this exists. An exception to this principle arises in situations where the data subject has consented to such processing in a particular instance, or has made their personal data generally accessible and has not expressly forbidden its processing. Consent must be explic-

[1] Incl. administrative prosecutions/sanctions.

itly granted (i) each time especially sensitive personal data is processed; (ii) for high-risk profiling outside the area of mandatory occupational benefits; and (iii) for every case of profiling in the area of mandatory occupational benefits.

The Foundation's Data Protection Consultant must be involved whenever doubts arise as to whether there is a required legal framework or a sufficient legal basis for data to be processed (and/or whether such a framework or basis is needed).

Privacy policy

6

Data subjects must be informed in a comprehensible and easily accessible form that their personal data is being processed, unless, for example, there is a legal requirement for it to be processed.

The information supplied to the data subject must contain the following information at least:
- Contact details of the legal entity responsible for the data
- Purpose of processing
- Recipients or categories of recipients
- Details of countries if transmitted abroad
- Data categories in the case of indirect data collection (not from data subject)
- Processes used for making significant, fully automated decisions.

Contracted-out processing of personal data

7

The processing of personal data may be transferred to a service provider as processor. The Foundation remains responsible towards the data subject for the processing of the personal data. In order for a processor to be used, the following conditions must be met:
- When the processor is selected, care is taken to ensure that it can guarantee the protection and, in particular, the security of the data.
- The transfer of personal data to the processor does not breach any legal or contractual confidentiality obligations.
- A data processing agreement is concluded in writing or in another form of text before any personal data is transferred.
- If a processor based abroad is commissioned, the conditions listed in section 8 must also be met.

The data processing agreement must require the processor to process personal data only in accordance with its assignment and the Foundation's instructions, not to use it for any other purpose, and to ensure that the data is processed securely. Subcontractors may be appointed only with the Foundation's consent.

Transmission to another country

8

Personal data may be transferred abroad only if the receiving country has an appropriate level of data protection or special protective measures such as contractual guarantees have been imposed.

Privacy by design: notification of new, discontinued, or significantly altered data processing

9

In order to ensure that a process, application, project, or other undertaking complies with data protection requirements and to be in a position to encourage the necessary measures, the management of the Foundation must involve the Data Protection Consultant as soon as possible by completing the data protection impact assessment checklist.

Examples of new or significantly altered data processing include:
- Roll-out of a new software program/application, or specific functions thereof
- Altered marketing measures
- Altered or new analysis/evaluation/linking of existing data relating to an individual
- Use of existing software/application to collect additional personal data or for purposes other than those specified hitherto
- Creation of new data collections
- Granting remote access to personal data.

Reporting of incidents

10

Suspected and actual data protection breaches must be reported to the Foundation's Data Protection Consultant as quickly as possible and without delay (examples of incidents: smartphone or notebook without hardware encryption has gone missing, email sent to wrong recipient). The Data Protection Consultant verifies that the authorities and data subjects have been notified and other measures taken.

Data Protection Consultation of the Foundation:
Swiss Infosec AG
Centralstrasse 8A
6210 Sursee
Tel.: +41 (0)41 984 12 12
E-mail: datenschutzberater@infosec.ch

Forwarding of requests from data subjects

11

Requests from data subjects regarding, for example, access, rectification, objections, data portability, or the examination of automated individual decisions with reference to their personal data must immediately be forwarded to the Data Protection Consultant, who makes arrangements for the cross-departmental compilation of data and communicates with the data subjects, among other tasks.

Organization

12

Governing bodies and employees
Within their own areas of responsibility and activity, governing bodies and employees are responsible for compliance with the principles laid down in these regulations regarding the handling of personal data.

Data owners
Data owners bear primary responsibility for compliance with data protection legislation and these regulations during the related data collection and data processing. They ensure that the related data processing is documented and perform a data protection impact assessment when required.

IT
The IT department implements the required technical and organizational measures in the information systems to ensure the security of personal data.

Data Protection Consultant
The task of the Foundation's Data Protection Consultant is to provide independent advice and coordinate compliance with data protection rules throughout the organization. The Data Protection Consultant relies on a seamless, rapid flow of information from all governing bodies and employees, since mandatory deadlines must be met in order to fulfill certain requirements under data protection law.

The Data Protection Consultant supports the legally required performance of a data protection impact assessment, provides advice on maintaining the register of processing activities and on creating the processing policy, coordinates the reporting of incidents, and ensures that data subjects can exercise their rights. Furthermore, the Data Protection Consultant checks whether data subjects are kept sufficiently informed about the processing of their data in the interests of transparency. Where necessary, the Consultant formulates and updates the data protection information.

Sanctions

13

Breaches of these regulations may lead to disciplinary measures or to civil or criminal proceedings.

Final provision

14

These regulations may be supplemented by other rules or regulations relating to the handling of personal data (e.g. IT user instructions) and come into effect on September 1, 2023.

L1287.004-09.23