DECLARATION ON THE PROTECTION OF PERSONAL DATA

EFFECTIVE SEPTEMBER 1, 2023

2023 EDITION

CIEPP
Caisse Inter-Entreprises
de Prévoyance Professionnelle
ZKBV - Zwischenbetriebliche Kasse für Berufliche Vorsorge
CIPP - Cassa Interaziendale di Previdenza Professionale

TABLE OF CONTENTS

1. PRINCIPLE

The Declaration on the protection of personal data applies to all personal data that we process in the framework of implementing the occupational provident scheme and its related activities.

The purpose of the present Declaration on the protection of personal data is to describe how the personal data collected or held by the CIEPP are used, and to whom these data can be communicated.

The CIEPP only collects and processes personal data for the purposes described in the Declaration on the protection of personal data and in the quantity required for this purpose, as well as in the framework of the legal regulations in force. In so doing, the CIEPP only keeps personal data to the extent that this is necessary and as long as its missions require.

In order to guarantee the security of its personal data and their protection against non-authorised or illicit processing, the CIEPP takes appropriate measures on both the technical level (e.g. pseudonymisation of the personal data or access restrictions) and organisational level (e.g. instructions given to members of staff, confidentiality clauses and checks).

2. RESPONSIBILITY FOR PROCESSING

Contact details:
Caisse Inter-Entreprise de Prévoyance Professionnelle – CIEPP
67, rue de Saint-Jean – Case postale – 1211 Genève 3
T 058 715 33 18 – ciepp@fer-ge.ch

Furthermore, the CIEPP may delegate the processing of personal or sensitive data to subcontractor processors. Nevertheless it remains ultimately responsible for delegated processing vis-a-vis the data subject and the monitoring authority. In this context the CIEPP ensures respect for article 9 of the Federal Act on Data Protection (LPD) (notably through the conclusion of a contract with its subcontractors).

3. DECLARATION RECIPIENTS

This declaration applies to all persons whose personal data is processed by the CIEPP, regardless of the means of communication used.

Processing may, in particular, affect the following categories of persons, insofar as the CIEPP processes their personal data: insured persons, benefits recipients, members of our bodies, contact persons at social security and private insurance organisations, pension funds and vested benefits institutions.

4. PURPOSE OF DATA PROCESSING AND LEGAL BASIS

Personal data are primarily processed for the purposes of managing occupational pensions (e.g. admission of insured persons, examination and processing of pension cases).

The legal basis arises from the occupational benefits legislation, in particular the Federal Law on Occupational Old-Age, Survivors› and Disability Pension Plans (LPP) and the Federal Law on Vested Benefits (LFLP), as well as the corresponding ordinances. As a federal body, the CIEPP processes the relevant personal data within the scope of its statutory processing powers (e.g. art. 85a ff. LPP). Regarding extra-mandatory pension plans, our data processing operations are not subject to the data protection provisions of the LPP, but rather to those of the LPD. However, as the CIEPP is a comprehensive fund, it has decided, as accepted by the PFPDT, to apply the requirements and obligations arising from the LPP to all its benefits.

5. THE BASES ON WHICH THE CIEPP COLLECTS AND USES DATA

5.1 LEGALITY (ART. 6 AND 34SS LPD)

As the CIEPP is a federal body, it can only process data if it has a formal or material legal basis pursuant to articles 34 and ff LPD. In the context of its occupational pension benefits, it is entitled to process data in accordance with the LPP, the LFLP and their implementing ordinances.

5.2 PROPORTIONALITY (ART. 6 PARA. 2, 4 AND 6 LPD)

The CIEPP only processes data that is strictly required for the intended purposes, while also minimizing the amount of data collected, in application of the LPP, LFLP and their implementing ordinances.

Data are destroyed or anonymised as soon as they are no longer required for the purpose of processing, unless the law stipulates that a retention period should be applied.

5.3 ACCURACY OF DATA (ART. 6 PARA. 5 LPD)

The CIEPP ensures that the data collected are accurate.

Appropriate measures are taken to correct, delete or destroy data that are inaccurate or incomplete, taking into account the type of processing, its scope and the associated risks for the data subjects.

5.4 GOOD FAITH (ART. 6 PARA. 2 LPD)

All personal data processing operations must be carried out for the purposes indicated to the data subjects, or those operations which arise from the law or the relevant circumstances.

5.5 PURPOSE (ART. 6 PARA. 3 LPD)

Personal data must be collected for specific purposes that are recognisable to the data subject, in application of the LPP, the LFLP and their implementing ordinances.

5.6 ACCESS TO PERSONAL DATA

The CIEPP's employees and subcontractor processors only have access to personal data which is necessary for the performance of their work.

5.7 TRANSFER OF PERSONAL DATA TO THIRD PARTIES

Processing of personal data may be entrusted to third parties (subcontractor processors) in accordance with article 9 of the LPD, provided that no legal or contractual obligation of secrecy prohibits it, and that data is processed only in the manner in which the controller itself is permitted to do it. A contract must be concluded when processing is done by a subcontractor processor.

5.8 SECURITY OF PERSONAL DATA

In accordance with Article 8 of the LPD, the CIEPP ensures that data security is guaranteed in terms of the risks involved, particularly for sensitive personal data. Personal data are therefore protected by technical and organisational measures which are appropriate to the type of data and the risks presented by processing, in order to maintain data security and, in particular, to prevent the destruction, loss, alteration, misuse of the data and unauthorised, accidental or unlawful disclosure of it or access to it, as well as any other form of unlawful processing.

The following technical and organisational security measures are applied to guarantee confidentiality, integrity, availability and traceability:

- Data minimisation measures;
- Data encryption measures;
- Access logging and traceability measures;
- Strict access and authorisation policies;
- Anonymisation measures;
- Archiving measures.

These safety measures are regularly monitored and reviewed, in particular those relating to:

- Information security management;
- Information security risk assessment;
- Physical checks;
- Logical access checks;
- Protection against malware and piracy;
- Data encryption measures;
- Data backup and restoration management measures.

5.9 RECORD OF PROCESSING ACTIVITIES

In accordance with article 12 of the LPD, the CIEPP is obliged to maintain a record of processing activities describing:

- The identity of the controller;
- The purpose of processing;
- The categories of data subject;
- The categories of personal data processed;
- The type of data;
- The categories of data subjects;
- The retention period and
- The measures taken to guarantee the security and protection of personal data in accordance with article 8 of the LPD.

The CIEPP has established this record and declared it to the Federal Data Protection Commissioner pursuant to article 12 para. 4 of the LPD.

5.10 TRAINING AND AWARENESS

Training, awareness-raising and informing CIEPP employees about current security and data protection rules are crucial in maintaining the security of personal data.

Scientific, technical and legal monitoring are essential for the CIEPP to guarantee an appropriate level of security and protection when confronted with ever-evolving cyber threats and new technical developments in information systems.

Awareness campaigns are carried out on a regular and iterative basis.

CIEPP data, including personal data, must be protected, in function of their classification, against all unauthorised internal and external processing through the application of appropriate organisational and technical measures.

5.11 OBLIGATION OF SECRECY

Persons who process personal data for the CIEPP under an employment contract or subcontractor mandate are obliged to maintain secrecy with respect to third parties, even after the contractual relationship has ended.

Exceptions are only made where there is a legal basis for doing so.

6. TYPES OF PERSONAL DATA PROCESSED

The CIEPP mainly processes the following categories of personal/sensitive data:

- AVS number;
- First name, surname;
- Sex;
- Date of birth;
- Date of marriage/start of a partnership;
- Civil status;
- Postal address;
- Email address;
- Phone number;
- Bank details;
- Income;
- Children;
- Employer's name and address;
- Start and end of employment;
- Rate of activity;
- Level of incapacity to work;
- Level of disability.

The CIEPP only processes the personal/sensitive data of its insured persons in the context of managing its occupational pension schemes. In particular, these processing purposes include (but are not limited to) the following:

- Affiliation of a self-employed person to the CIEPP;
- Obligations of policyholders within CIEPP;
- Changes to an insured person›s contractual data;
- Changes to an insured person›s personal data;
- Processing the insured person's exit/departure;
- Transfer of exit benefits;

- Cash payment of exit benefits;
- Notification of incapacity to work lasting more than 3 months;
- Application for benefits to encourage home ownership;
- Application for disability benefits;
- Application for death benefits;
- Application for retirement benefits;
- Division of occupational insurance benefits in the event of divorce;
- Processing a buy-in;
- Declaration of cohabitation;
- Transmission of information to the pension fund expert;
- Data hosting;
- Management of CIEPP staff.

7. SENDING PERSONAL DATA ABROAD

In the context of the management of occupational pension plans and related activities, the CIEPP may need to transfer personal/sensitive data to other countries. When personal/sensitive data must be transferred to a country that does not provide an appropriate level of protection, additional measures are taken to guarantee adequate protection levels in the destination country.

In this respect, the CIEPP relies on the Appendix to the OPDo which lists those states with adequate data protection levels.

Additional measures include those indicated in articles 16 and 17 of the LPD, and particularly the use of standard data protection clauses approved by the Federal Data Protection and Information Commissioner (PFPDT).

8. RETENTION OF PERSONAL DATA

The CIEPP processes personal data in accordance with the principle of proportionality: it does not collect more personal data than are required to carry out its legal tasks, and access authorisations are strictly limited to those employees who need them to carry out their duties.

With the exception of data pertaining to the granting of entitlements to CIEPP benefits (i.e.10 years following the expiry of the last entitlement to a benefit, if there are no other benefits that may be granted on the basis of these data / at most, until the insured person reaches the hypothetical age of 100), personal data are destroyed or anonymised as soon as they are no longer required for processing purposes.

9. RIGHTS OF DATA SUBJECTS

The LPD guarantees data subjects certain rights which they can assert vis-a-vis the CIEPP. These include the following:

- Right of access: the data subject may ask whether the processing body processes personal data concerning him or her, and if so, which data.
- Right of correction and destruction: the right to demand that inaccurate data be corrected or destroyed.
- The right to prohibit the communication of personal data under certain conditions.

  The CIEPP responds to these requests within 30 days of their receipt, except in specific cases.

The LPD also provides for the right to the receipt or transmission of personal data (or «data portability»). Under the terms of article 28 para. 1 of the LPD, data subjects may ask the data controller to deliver the personal data that they have disclosed to it in a conventional electronic format. The purpose of this provision is to give data subjects control over their data, and in particular to enable them to reuse them or pass them on to another data controller or processor. However, as the right to data portability can only apply if personal data are processed with due consent or in connection with a contract, it does not apply to federal bodies (including the CIEPP) which process personal data as part of their statutory duties or on a statutory basis.

10. DATA PROTECTION ADVISOR

In accordance with its legal obligations (article 10 para. 4 LPD and OPDo), the CIEPP has appointed an independent data protection advisor to ensure that all provisions relating to the protection of personal data are applied.

The CIEPP has appointed DPO Associates Sarl, in the person of Ms Isabelle Hering, a specialist in data protection, to assume the role of external Data Protection Advisor.

The Data Protection Advisor (DPA) is the main point of contact for data subjects. She can be contacted at the following email address: cieppdpo@fer-ge.ch.

11. DATE OF EFFECT

This Declaration on the protection of personal data is effective as of 1 September, 2023.

Rue de Saint-Jean 67 – P.O. Box – 1211 Geneva 3
Tel. 058 715 31 11 – E-mail : ciepp@fer-ge.ch
www.ciepp.ch