

PROCESSING OF PERSONAL DATA

Context and definitions

The General Data Protection Regulation (“GDPR”) lays down a number of rules concerning the protection of natural persons with regard to the processing of personal data.

For the purposes of the GDPR, any data or information relating to an identified or identifiable natural person shall be considered as personal data.

Processing refers to any operation or set of operations that is performed upon personal data or sets of personal data, whether or not by automatic 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, blocking, deletion or destruction.

A controller is a natural or legal person, public authority, agency or any other body who or which, alone or jointly with others, determines the purposes and means of the processing of personal data.

The processor is a natural or legal person, public authority, agency or any other body who or which processes personal data on behalf of the controller.

The controller shall implement appropriate technical and organisational measures, taking into account the nature, scope, context and purposes of the processing, as well as the varying degrees of probability and seriousness of the risks to the rights and freedoms of natural persons with regard to the processing operation, in order to implement the data protection methods effectively and to incorporate the necessary safeguards into the processing in order to comply with the requirements of the General Data Protection Regulation and to protect the rights of data subjects.

The controller shall take appropriate technical and organisational measures to ensure that, in principle, only personal data necessary for each specific purpose of the processing are communicated.

Purpose of the processing

Cohezio asbl/vzw is a recognised external service for prevention and protection at work. The tasks and responsibilities of the external services are set out in Book II, Title 3 of the Welfare at Work Code.

Within the framework of its obligations under the Welfare at Work Code, an employer can always call on an external service for prevention and protection at work, **Cohezio asbl/vzw**. The employer hereby concludes an agreement with **Cohezio** in which the nature, scope and minimum duration of the services are specified.

As an external service for prevention and protection at work, **Cohezio** is responsible for processing data as part of its statutory responsibilities relating to the prevention and welfare of employees at work, and for processing personal data. As controller, **Cohezio** also collects and processes the data that an affiliated employer entrusts for the execution of its assignments.

The processing of personal data

All personal data must:

- be processed in a lawful, proper and transparent manner;
- for specified, explicit and legitimate purposes;
- be adequate, relevant and necessary for the purposes for which they are processed;
- be accurate and up to date
- be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- be processed, by taking appropriate technical or organisational measures, in such a way as to ensure that they are adequately protected.

Personal data shall be processed within the framework of the provisions concerning the welfare of employees at work as set out in the Welfare Act of 4 August 1996 and Books 1 to 10 of the Welfare at Work Code.

The processing of special and sensitive personal data

The processing of special personal data, such as data relating to the (physical and mental) health of a person, shall be carried out in accordance with Article 9(2) of the General Data Protection Regulation.

Processing shall take place within the framework of:

- recording personal and medical data in the medical file: indicating ability or inability to perform a function and recommendations, specifying tests and additional examinations and any other medical data useful to the occupational health physician (Book 1, Title 4 - Measures relating to the health surveillance of employees of the Welfare at Work Code).
- recording personal data in the context of psychosocial files (Welfare Act of 4 August 1996 and Book 1, Title 3 - Prevention of psychosocial risks at work of the Welfare at Work Code).
- recording personal data in the context of other areas of welfare (statutory responsibilities of prevention advisor Books 1 to 10 of the Welfare at Work Code).

What data are processed?

All personal data that are processed are done so within the framework of the statutory or entrusted assignments of **Cohezio**.

Cohezio shall keep a health file on the employee for whom medical surveillance was organised within the framework of Book 1, Title 4 (measures relating to the health surveillance of employees) of the Welfare at Work Code. The health file shall include all relevant information concerning the employee, enabling the prevention advisor-occupational health physician to carry out health surveillance and to measure the effectiveness of prevention and protection measures applied within the company. The processing of these data shall be carried out in compliance with the General Data Protection Regulation.

The following personal data shall be processed:

Personal identification details: name, address, telephone number, national registry number.

Data relating to personal characteristics: age, sex, date and place of birth, marital status, nationality.



External Service for Prevention and Protection at Work

Cohezio asbl/vzw · Registered office: Bisschoffsheimlaan 1-8 -1000 Brussels
T. +32 (0)2 533 74 11 · F. +32 (0)2 538 79 32 · info@Cohezio.be · www.Cohezio.be
RPM/RPR Brussels · IBAN BE54 8777 94 38 02 97 · BIC BNAG BE BB · 0410.623.764

Information on profession and occupation: description of post, date of recruitment, place of work, terms and conditions of employment.

Medical data (occupational medicine – health file): professional history, specific data established by the occupational health physician during the preventive medical examinations, exposure data, request for health surveillance of the employee, date and type of preventive medical examination carried out and the results, results of the targeted examinations or of the targeted functional tests, results of the biological surveillance, radiographies and reports of the radiological examination, any other documents or information relating to the targeted examinations that the employee has undergone and which have been carried out by an outside doctor or service, the health assessment form, the date and nature of vaccinations, results of tuberculin tests, vaccination cards, any other medical or medico-social documents, declaration of occupational disease, copy of the accident at work card, reintegration plan and reports on reintegration.

Individual file on psychosocial aspects: document informative personal interview, type of intervention, statements from the persons involved, opinions.

Transfer of personal data

The data shall not be disclosed by **Cohezio** to third parties, except for the application of statutory or regulatory provisions (competent officials of the supervision of welfare at work administration), or for the performance of its tasks as an external service for prevention and protection at work.

Medical data and data relating to an individual file on psychosocial intervention or other personal data of a sensitive nature may be communicated only in accordance with the general provisions on professional secrecy.

The data may be communicated to the registered person himself or herself.

Retention periods of data

The personal data shall not be kept longer than necessary as provided for in the legislation.

The medical file shall be kept for at least 15 years after the departure of the employee. The register of employees exposed to asbestos shall be kept for 40 years following the end of exposure.

The individual file on psychosocial intervention shall be kept by the prevention advisor on psychosocial aspects for 20 years from the date of submission of the request for psychosocial intervention.

Security

Personal data shall be processed in a way that ensures adequate security and confidentiality of such data and prevents the possibility of unauthorised access or use of personal data. To this end, the processor shall take the appropriate technical and organisational measures as defined below.

In particular, **Cohezio** shall protect personal data against unauthorised access or use of transmitted, stored or processed data, the alteration, loss or destruction of data, whether accidental or unlawful.



External Service for Prevention and Protection at Work

Cohezio asbl/vzw · Registered office: Bisschoffsheimlaan 1-8 -1000 Brussels
T. +32 (0)2 533 74 11 · F. +32 (0)2 538 79 32 · info@Cohezio.be · www.Cohezio.be
RPM/RPR Brussels · IBAN BE54 8777 94 38 02 97 · BIC BNAG BE BB · 0410.623.764

Confidentiality of data

All personal data communicated to **Cohezio** must be treated in strict confidence.

All parties undertake to keep all personal data confidential and not to distribute them internally or externally in any way unless this is necessary in order to comply with a legal obligation.

Data processing outside a Member State of the European Union

The personal data shall only be processed in Belgium and shall under no circumstances be processed outside a Member State of the European Union.

Security arrangements and protective measures

Cohezio shall take appropriate technical and organisational measures to ensure the confidentiality of the processing of personal data and to prevent unauthorised access or use of personal data.

1. Information security policy

Cohezio has an information security policy approved by the person responsible for day-to-day management. The policy imposes a number of general guidelines on information security, such as compliance with safety measures, carrying out conformity audits, implementation of measures, etc.

The policy is communicated to and also complied with by all staff members of **Cohezio**.

2. Risk assessment

Cohezio shall carry out, communicate and maintain an information security and privacy risk assessment for each process and project. This risk assessment shall consider the measures and safeguards put in place to protect personal data, mitigate risks and demonstrate compliance with the requirements of the GDPR.

3. Internal organisation of information security

Cohezio has an information security policy that sets out all responsibilities of the employee and the organisation with regard to information security and privacy. Where necessary, all employees, all hired employees or external users of **Cohezio** must sign the policy. The processor shall ensure that, insofar as this is necessary for the performance of their tasks, employees (internal and external) receive the necessary information and appropriate training with regard to information security.

4. Access management

Cohezio has designated an access manager responsible for managing the access rights to IT systems. The administrator shall determine the individual access rights of the user on the basis of a procedure validated by the management. Access shall be restricted to the applications that are necessary for the performance of the user's tasks.



External Service for Prevention and Protection at Work

Cohezio asbl/vzw · Registered office: Bisschoffsheimlaan 1-8 -1000 Brussels

T. +32 (0)2 533 74 11 · F. +32 (0)2 538 79 32 · info@Cohezio.be · www.Cohezio.be
RPM/RPR Brussels · IBAN BE54 8777 94 38 02 97 · BIC BNAG BE BB · 0410.623.764

1. Log management

The processing of personal data shall be recorded in log files. In this way, **Cohezio** can check at any time who has changed, supplemented or deleted data. Periodic checks shall be carried out on the log files for unlawful use or access to personal data.

2. Safe physical environment

Cohezio shall take the necessary measures to restrict access to buildings and premises containing sensitive or critical information to authorised persons only. **Cohezio** shall also lay down the procedures for carrying out access controls.

Cohezio shall take measures to prevent the loss, damage or theft of company assets.

3. Secure transfer of data

The storage, processing and transmission of personal data, externally or via the internet, shall always be encrypted. Encryption shall be used for the transmission of data that cannot be read by other persons. Only the sender and the recipient shall have the necessary keys to restore the data to its original form. These additional data shall be kept separately by **Cohezio**. **Cohezio** shall also take the necessary technical and organisational measures to that end.

4. Continuity management

Physical or technical incidents such as equipment failure may prevent the availability of or access to personal data or may lead to the loss of personal data. **Cohezio** shall ensure that the necessary measures are taken to enable the organisation to respond appropriately to serious incidents or disasters and to achieve timely recovery.

5. Incident management

Cohezio shall ensure that the necessary procedures are in place for recording and managing information security incidents. These procedures shall be familiar to all employees of **Cohezio**.

Every employee is required to report any unauthorised access, use, disclosure, loss or destruction of personal information. Incidents must be reported to the security advisor or data protection officer. All evidence of the incident shall be collected and stored correctly.

Any information security incident must be evaluated so that procedures can be updated and improved.

6. Data leaks

All data leaks, i.e. any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to transmitted, stored or processed data, shall be reported to the Data Protection Authority within 72 hours of discovery of the data leak.

Cohezio has developed the necessary procedures to detect all data leaks at the earliest possible stage. **Cohezio** also keeps a record of all facts relating to data leaks, their consequences and any corrective measures taken.



External Service for Prevention and Protection at Work

Cohezio asbl/vzw · Registered office: Bisschoffsheimlaan 1-8 -1000 Brussels

T. +32 (0)2 533 74 11 · F. +32 (0)2 538 79 32 · info@Cohezio.be · www.Cohezio.be
RPM/RPR Brussels · IBAN BE54 8777 94 38 02 97 · BIC BNAG BE BB · 0410.623.764

Rights of the persons whose personal data are being processed

1. Right of access and rectification

The data subject shall have the right to access and rectify his or her personal data at any time and free of charge.

The data subject may correct or complete his or her data by means of a letter containing a copy of his or her identity card addressed to the managing director of **Cohezio**, Ms Evelyne Kerger, Bischoffsheimlaan 1-8, 1000 Brussels.

2. Right to data erasure (right to be forgotten)

The personal data necessary for the exercise of its statutory responsibilities by **Cohezio** cannot be deleted.

Medical files can be deleted only in accordance with the legal provisions of the Welfare at Work Code.

3. Right to restriction of processing

Cohezio shall process the personal data insofar as this is necessary for the execution of its legal assignments under the Welfare Act and the Welfare at Work Code.

4. Right to data portability

The right to data portability means the right of the data subject to obtain his or her personal data in a structured, commonly used and machine-readable form and the right to directly or indirectly transfer them to another controller (or employer).

The health file of a data subject shall include all relevant information concerning the employee, enabling the prevention advisor-occupational health physician to carry out health surveillance. The transfer of the health file shall be carried out under the responsibility of the physician in charge of the department or section responsible for medical surveillance.

The transfer of an individual file on psychosocial intervention in the event of a change of external service is regulated as follows: the prevention advisor on psychosocial aspects shall inform the employee and the other person directly involved in the file of the fact that **Cohezio** is no longer competent to deal with his or her request. The prevention advisor on psychosocial aspects to whom the request has been submitted shall forward the individual file to the prevention advisor on psychosocial aspects of the new external service. The prevention advisor on psychosocial aspects of the new external service shall inform the employee that he or she shall take over the examination of the request.

If the examination of the request for formal psychosocial intervention is completed at the time of the change of external service for prevention and protection at work, the prevention advisor on psychosocial aspects of the new external service may, if this is necessary for the performance of his or her task, obtain a copy of the individual file kept by the prevention advisor on psychosocial aspects to whom the request was submitted.



External Service for Prevention and Protection at Work

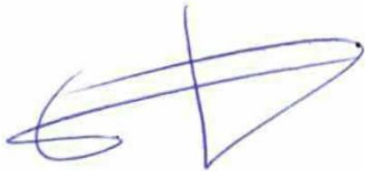
Cohezio asbl/vzw · Registered office: Bischoffsheimlaan 1-8 -1000 Brussels
T. +32 (0)2 533 74 11 · F. +32 (0)2 538 79 32 · info@Cohezio.be · www.Cohezio.be
RPM/RPR Brussels · IBAN BE54 8777 94 38 02 97 · BIC BNAG BE BB · 0410.623.764

Complaints

Any data subject has the right to lodge a complaint with the Data Protection Authority if he or she considers that his or her rights under the General Data Protection Regulation have been infringed.

If you need more information

If you need more information, please contact the data protection officer: Johan Van Middel (infosecurity@Cohezio.be).



Olivier LEGRAND
Managing director

15/05/2018



External Service for Prevention and Protection at Work

Cohezio asbl/vzw · Registered office: Bisschoffsheimlaan 1-8 -1000 Brussels
T. +32 (0)2 533 74 11 · F. +32 (0)2 538 79 32 · info@Cohezio.be · www.Cohezio.be
RPM/RPR Brussels · IBAN BE54 8777 94 38 02 97 · BIC BNAG BE BB · 0410.623.764