Privacy Policy of MENSURA

Mensura External Agency for Prevention and Protection at Work, vzw, with its registered office at Gaucheretstraat 88/90 1030 Brussels, and company number 0410.664.742, registered in the register of legal persons in Brussels, duly represented in this matter by Gretel Schrijvers in their capacity of general director,

hereinafter referred to as "the controller"; (regarding the advice of COPREV, date 26/01/2018)

Declares as follows:

The controller acknowledges the importance of the safe processing of our clients' personal data. The controller wishes to provide insight into the processing of your personal data by means of this Privacy Policy.

This Privacy Policy was drawn up in accordance with the European General Data Protection Regulation (GDPR), dated 27 April 2016. This regulation was transposed into the Framework Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data. Where the Policy speaks of "the controller"; in principle this means Mensura External Agency for Prevention and Protection at Work.

*Furthermore, as a lex specialis, the new European e-privacy guideline will govern the processing of personal data within the framework of direct marketing and cookies. (*At the time of writing this Privacy Policy, this was still a draft text)*

If the content of the above legal texts changes, the controller will amend this Privacy Policy to conform with these changes. Our clients will be informed of fundamental changes in a timely manner. Additional changes will not be informed to our clients. Our Privacy Policy can be freely consulted on our public website.

Point 1. Scope of the Privacy Policy

This Privacy Policy and its appendices serve as an appendix to the Main Contract between the controller and our clients. This Privacy Policy is applicable for the full duration of the Main Contract.

If there are deviating provisions in the Main Contract on the processing of Personal Data, this Privacy Policy will have precedence.

Deviations from this Privacy Policy are only valid if both parties have granted their permission for this in writing.

Point 2. Definitions

In accordance with the text of the GDPR, the following terms will have the following meaning for the application of this Privacy Policy:

"Data subject": *the identified or identifiable natural person*

"Data concerning health": *personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*

"Sensitive personal data": *personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs or membership of a trade union and processing of genetic information or biometric data with a view to the unique identification of a person or data related to health or someone's sexual behaviour or sexual orientation.*

"Personal data breach": *a breach of security that accidentally or unlawfully leads to the destruction, loss, change or unauthorised disclosure or unauthorised access to data that has been sent, stored or processed in any other way.*

"Personal data": *any information relating to an identified or identifiable natural person ('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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

" Pseudonymisation": *the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*

"Consent of the Data Subject": *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.*

"Processor": *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (in this case, Mensura EOHS).*

"Processing": *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": : *a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (in this case, you, the client).*

Point 3. Processing personal data

The controller guarantees that your personal data will be:

a) Processed in a lawful, fair and transparent manner
b) Collected for specified, explicit and legitimate purposes
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
d) Correct and updated when necessary
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
f) Appropriate technical and organisational measures will be taken to guarantee appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

Personal data is lawfully processed by the controller as processing is based upon legal grounds. Article 6, 1 C of the GDPR states that Personal Data is lawfully processed if "*processing is necessary for compliance with a legal obligation to which the controller (here: the client) is subject*". In this case, our clients have a legal obligation to take the necessary measures within the framework of occupational health and safety. These legal obligations are stipulated in the Code on Well-being at Work.

The aforementioned personal data includes name, address, telephone number, gender and age. An overview is available in appendix 1 to this Policy.

Point 4. Processing sensitive personal data

The controller will lawfully process sensitive personal data (more explicitly: "data concerning health") in conformity with article 9, b) and h) of the GDPR;

- *b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller (here: the client) or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;*

The controller's services are primarily determined by law, namely the Code on Well-being at Work. Our clients are legally obligated – within Belgian social law – to join an External Agency for Prevention and Protection at Work.

- h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Sensitive data that is processed by the controller is related to data concerning health; i.e. weight, BMI, working capacity as stated on the HAF (Health Assessment Form) or the RAF (Reintegration Assessment Form), medical data, psychological data, injuries after a serious accident at work, the data subject's lifestyle, etc.. An overview is available in appendix 1 to this Policy.

Point 5. Explicit agreement from the Data Subject(s)

In the context of the provision of service where the controller must request the Personal Data directly from the Data Subject(s), the controller (Mensura) will inform the Data Subject(s) prior to the processing concerning the following elements, in conformity with article 13 point 1 of the GDPR:

- the identity and contact details of the controller
- the contact details of the Data Protection Officer;
- the purpose and legal grounds for the processing;
- the recipients or the categories of the recipients of the personal data;

- the manner in which the rights of the Data Subject(s) are exercised;
- the fact that the Data Subject can revoke his or her explicit permission and the manner in which this is done;
- the fact that the Data Subject has the right to submit a complaint to the supervisory authority;
- the retention period for Personal Data;
- if applicable, the existence of automated decisions.

Where the controller provides services in the context of points 3 and 4, the client must share the aforementioned information with the Data Subject(s). The client can use this Privacy Policy to inform the Data Subject(s).

Point 6. Processing personal data for marketing purposes

With regard to processing Personal Data for Marketing Purposes, the controller can rely upon a legal basis (recital 47 of the GDPR). An opt-out for the Data Subjects will be always possible. No personal data of the customer's employees are processed by controller for Marketing purposes. Only the customer's personal details (contact details) are processed for this purpose, so that controller can keep the customer informed of changes to the mandatory services within the context of the well-being legislation.

Point 7. Anonymous group reporting

The controller guarantees that group reporting will be anonymous given that personal data is only shared as from a dataset of 10.

For example, the results of the medical examinations are part of the risk analysis. These results are reported in the form of the anonymous group results.

Point 8. The record of processing activities

The controller has drawn up a record of processing activities in which the following elements of each of their services are described in detail:

1 ° Which categories of personal data are being processed?

2° Who can receive this personal data (internal/externally)?

3 ° For how long will the personal data be kept?

4 ° For how long will the personal data be protected?

5° Will the personal data be processed outside Belgium?

6° Who has access to the personal data (internally/externally)?

7° The purposes of processing.

If you have questions within this framework that have not been made clear in this Policy, please contact the persons listed in point 20.

Point 9. Appropriate technical and organisational measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure the safe processing of personal data. Appendix II to this Policy contains a summary of these measures.

The controller guarantees that they will take the necessary measures in conformity with article 32 of the GDPR, which, among other things, pertain to the following:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The controller guarantees that the only employees who will have access to personal data are those who are actually involved in implementing the services. Furthermore, these employees will be contractually bound by a duty of confidentiality.

Point 10. Third parties

Third parties who may gain access to personal data will also be restricted to persons involved in implementing the services. Appendix III contains an overview of external parties who may be involved.

These third parties will be subject to the same obligations with regard to data protection as those arising from this Privacy Policy, in particular, including the obligation to take appropriate technical and organisational measures for processing the Personal Data. The controller binds the third parties contractually in this regard.

Point 11. Processors

If the controller engages a processor to perform specific processing activities on the behalf of the controller, this processor will be subject to the same obligations with regard to data protection as those arising from this agreement, including the obligation to take appropriate technical and organisational measures for processing personal data. To this end, the processors have signed a processing agreement in accordance with article 28 point 3.

The controller guarantees that processors may only process personal data under written instructions of the controller. If the processors engage a sub-processor to perform processing activities, the processor will, in principle, remain liable towards the sub-processor.

Point 12. Processing of data outside a Member State of the EU

The controller guarantees that the personal data will not be processed outside a Member State of the EU. The Personal Data will only be processed in Belgium.

Point 13. Minimal processing of personal data

The controller's services are primarily determined by law, namely the Code on Well-being at Work. The controller will only process the minimum amount of personal data necessary within the framework of implementing the requested services. An overview is available in appendix 1 to this Policy.

The controller guarantees that personal data will not be stored for longer than is necessary for the implementation of the requested services. The controller is obliged to observe statutory retention periods. An overview is available in appendix 1 to this Policy.

Point 14. The rights of data subjects:

14.1. General

Within the framework of the GDPR, data subjects have the following rights with regard to their personal data:

1° Right of access

2° Right to rectify incorrect personal data

3° Right to erasure (Right to be forgotten")

In most cases, the right to erasure of data will not be executed by the controller, as processing is carried out on the basis of a legal obligation to process data.

4° Right to restriction of processing

5° Right to data portability

6° Right to object

In most cases, the right to object will not be executed by the controller, as processing is carried out on the basis of a legal obligation to process data.

The controller guarantees to answer requests within one month of receiving them. This will be done in conformity with the obligations of the controller stipulated in article 12 point 3 of the GDPR. Depending on the complexity and number of requests, this period may be extended by two months if necessary. The controller will inform the data subject of this extension within one month of receiving their request.

The controller's internal procedures are set out in points 14.2 and 14.3 so that the data subjects can correctly exercise their rights against the controller. The client must inform data subjects of the controller's internal procedures in a concise, transparent, comprehensible and easily accessible form and in clear and simple language. If data subjects wish to exercise a right that does not fall under point 14.2. or 14.3. the request can be sent to privacy@mensura.be.

If the Data Subject finds that one of the processors or third parties (see Appendix III) is processing Personal Data in contradiction to the GDPR, then the Data Subject can report this to the controller via privacy@mensura.be. The controller will try, after having received such a complaint, to contact the accused processor(s) or third party/parties within three business days. The controller will contact the Data Subject again within one month after receiving the complaint.

14.2. Rights of data subjects within the framework of medical supervision

With regard to the exercise of one of the rights related to their medical files, data subjects must respect the following internal procedure of the controller:

- requests must be submitted by means of a registered letter addressed to Marie-Noelle Schmickler, directeur afdeling medisch toezicht, Italiëlei 2 at 2000 Antwerp.
- they must enclose a copy of their identity card.

Access to medical files will not be granted to employees directly but to their attending physician. This is in conformity with the recommendation issued by the Medical Association on 07/09/1996.

14.3. Rights of data subjects within the framework of psychosocial files

With regard to the exercise of one of the rights related to their psychosocial files, Data Subjects must respect the following internal procedure of the controller:

- requests must be submitted by means of a registered letter addressed to the relevant prevention advisor on psychosocial aspects;

- they must also enclose a copy of their identity card.

14.4. Right to submit a complaint to the Belgian supervisory authority (= "the Data Protection Authority")

In accordance with article 77 of the GDPR, data subjects have the right to submit a complaint directly to the Data Protection Authority if they think that the controller is failing to protect and/or process their personal data in conformity with the GDPR.

Point 15. Portability of Personal Data if the controller changes an external agency

15.1. Transfer of Personal Data in the Medical Supervision Department

The transfer of health files is set out in the provisions of Book 1, Title 3, of the Code on Well-being at Work.

Health files consist of four separate sections:

a) social-administrative information concerning the identification of the employee and their employer.

b) occupational history and objective medical personal information that can be established on the basis of compulsory actions undertaken during preventative medical researches. This personal information is related to the employee's work station or activity.

c) specific information of a personal nature established by the occupational physician during preventative medical examinations and that are restricted to the last-mentioned doctor.

d) exposure of all employees employed at a work station or in an activity that exposes them to biological, physical or chemical agents.

Health files do not contain information on cooperation with public health programmes that are not related to work.

The transfer of medical information takes place under the responsibility of the doctor who is in charge of the department tasked with medical supervision (director of medical supervision).

To transfer medical files, the director of medical supervision of the new external service must write to the Mensura's director of medical supervision to request data transfer. The requested files will not be effectively transferred until this request has been received.

15.2. Transfer of Personal Data in the Psycho Department

The transfer of this personal data is set out in the provisions of article 34 van Book I, Title 3, Prevention of Psychosocial Risks at Work, of the Code on Well-being at Work.

If the client changes the external agency for prevention and protection at work, the transfer of individual files will be arranged as follows:

1° If a request for formal psychosocial intervention is being dealt with at the time of the change:

a) the prevention advisor on psychosocial intervention will inform the applicant and the other persons directly involved as soon as possible of the fact that the external agency for which he performs tasks will no longer be authorised to deal with the request;

b) the client will give the prevention advisor for psychosocial aspects to whom the request was submitted with the coordinates of the new external agency upon request;

c) the prevention adviser for psychosocial aspects to whom the request was submitted will submit the individual file to the prevention adviser for psychosocial aspect of the new external agency;

d) the prevention advisor on psychosocial aspects will inform the applicant and the other persons directly involved of the fact that they will be taking over the handling of the request;

2° If the handling of the request for formal psychosocial intervention is concluded at the time of the change of external agency for prevention and protection at work, the prevention adviser for psychosocial aspects of the new external agency may obtain a copy of the individual file from the prevention adviser for psychosocial aspect to whom the request was submitted if this is necessary for the performance of their duties.

The transfer of individual files is subject to conditions to safeguard professional secrecy.

Point 16. Removal of the Personal Data at the end of the Main Contract

The controller guarantees that the processed Personal Data will be deleted or transferred at the request of the client within the month following the end of the Main Contract, unless there is a legal provision allowing the controller to retain the Personal Data for a longer period of time.

At the request of the client, the controller will provide the necessary proof of this.

The processors and third parties are also informed by the controller about the removal of the Personal Data received, if the Main Contract has been terminated. Processors and third parties shall delete this Personal Data unless they too can provide proof of legal provisions allowing for the retention of Personal Data for longer periods of time.

Point 17. Requests for Personal Data from public government services

The controller will inform the client within three business days in cases where:

(a) concerning the processing of Personal Data, a public body requests information from the controller, or the controller receives a summons or a research or inspection request, unless the controller is not legally authorised to provide this;

(b) the intention is to provide Personal Data to a public body;

(c) the controller receives a request to publish the client's Personal Data or to provide information relating to the processing of the client's Personal Data from a third party, an employee, a customer, or the client's contractor.

The controller gives the client 72 hours, as from the time of the report, to object to such a transfer of Personal Data.

Point 18. Measures in the event of a personal data breach

The controller is obliged to report breaches of personal data security to the authorised Belgian supervisory authority within 72 hours. This applies unless it is unlikely that the personal data breach will result in a risk to the rights and freedoms of the data subject(s).

The controller will notify the client as soon as they have become aware of a personal data breach, without unreasonable delay. It is agreed that the controller and the client will contact each other within 48 hours of the controller learning of the breach and agree together whether it must be reported to the authorised Belgian supervisory authority.

The aforementioned obligation is also applicable if the controller is actually aware of a Personal Data breach committed by a processor or a third party, e.g. if the Data Subject submits a complaint to the controller.

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the client will inform the data subject(s) of it in accordance with article 34 of the GDPR.

Both the controller and the client will work together with the authorised Belgian supervisory authority to provide the necessary information and to limit the consequences of the breach.

Point 19. Miscellaneous provisions

If one or more of the provisions in this Privacy Policy should become null and void, the remaining provisions are still in full force.

This Privacy Policy is subject to Belgian law. The parties can only present their disputes concerning this Privacy Policy before the courts of Brussels.

Point 20. If you need more information or support.

The controller guarantees that they will provide the client with the necessary additional support and information so that the controller can show that they have complied with their obligations under the GPDR. This information obligation does not apply to information that is confidential or cannot be shared with the client for legal reasons.

Furthermore, the controller will grant the necessary cooperation if an audit is conducted on their premises on the orders of the client or by an auditor authorised by the client. The client will bear the costs of the appointed auditor and audit. The audit will always be limited to the controller's systems that are used for the processing.

The controller's Data Protection Officer is Annelies Feytons, who can be contacted at the following email address: Privacy@mensura.be. The controller's Security Officer is Ronnie Van Weert, who can be contacted at the following email address: Privacy@mensura.be.

Appendix 1. The categories of processed personal data and retention period

Categories of Personal Data that the controller can process

The employee's national register number, name, first name, age, address, gender, date and place of birth, photo, company position, employer, email address, seniority in the company, seniority in the position, work station, race, marital status, nationality, seaman's book number if applicable, type of driving licence if applicable.

Extra personal information: telephone number, email address, mobile phone number + consent to use of this information for notification.

Data concerning health: physical and mental health

Retention period

Medical file = statutory retention period (= 40 years)

Psychosocial files = statutory retention period (= 20 years)

Appendix II. Technical and organisational security measures

- Internal IT policy approved by the management board (contains password policy, acceptable use of company resources, Clean Desk and Clear Screen policy, Software policy, Internet policy, email policy, social media policy, policy on data confidentiality.....)
- Data will only be stored in Belgium
- Our systems are redundant on 2 data centres with TIER III + classification. (DRP and BCP)
- The hosting provider has ISO27001 certification.
- Firewalls on several network layers.
- Network Access Control, separation of networks, etc…
- Data in transit will only be permitted if encrypted.
- Remote access of users is only via VPN with Multi Factor authentication.
- Verified backup and restore procedures.
- Data in rest (backups) will be encrypted
- "Role based access" to applications.
- User Awareness training sessions will be organised.
- Antivirus/Antispam on several layers. (Firewall, Endpoints, Servers, mail systems…)
- SIEM for security devices.
- Logging and reporting.
- Regular security testing.
- Mobile Device management
- Capacity Management
- Regular updates of all systems and reporting on this.
- Regular security meetings met our hosting provider.
- Physical access security.
- Asset Management.
- Network and system monitoring.
- DDOS and IPS measures.
- Data Loss Prevention implementation in the near future.
- Change Management
- Separate Test, Validation and Production environments.
- Regular assessments of suppliers.

Appendix III. External parties who may process the personal data of data subjects

III.I. Third parties

- Personal data within the framework of psychosocial risks:
  - in conformity with article 35 of book 1, Title 3 of the Code on Well-being at Work, individual files on psychosocial risks will be kept at the disposal of the **official tasked with supervision**.
  - signed and dated statements from persons who were interviewed by the prevention adviser for psychosocial aspects will be communicated to the **Public Prosecution Service** that requests it, if the interviewed person has consented to the transfer in their statement. This is in conformity with article 35 of Book 1, Title 3 of the Code on Well-being at Work.
  - Article 41 of Book 1, Title 3 of the Code on Well-being at Work: the prevention adviser for psychosocial aspects will communicate the recommendation to the **Centre for equal opportunities and opposition to racism** and to the **Institute for Gender Equality**, if these institutes submit a written request and insofar as the employee has given their consent to this request in writing, but without the Centre and the Institute being allowed to convey the recommendation to the employee.
  - This is in conformity with article 44 of Book 1, Title 3 of the Code on Well-being at Work: If the applicant or the accused are considering commencing legal action, the employer will give them a copy of the recommendation by the prevention adviser for psychosocial aspects upon request.
  - Individual files will only be passed on to the **occupational doctor providing treatment**, if the employee has consented to this.
  - **Youston:** archiving of psychosocial files

- Personal data within the framework of medical supervision:
  - Merak/Houston: archiving of the medical files
  - Exchange of medical files with the medical department of the Nuclear Research Centre in Mol, the nuclear power station at Doel, Belgoprocess and FEDRIS
  - Exchange of files between other external services
  - Individual files will only be passed on to the attending physician, if the employee has consented to this.
  - In conformity with the Codex on Well-being at Work, book 1, title 4, acces to the medical file is given to the doctor of the Federal Public Service Employment, Labour and Social Dialogue.
  - Vaccinnet: personal data within the framework of vaccinations
  - The advising physician for the health insurance provider within the framework of rehabilitation files

- Personal data within the framework of ergonomics:
    - storage by U&I for E-coach

III.II. Processors

- Personal data within the framework of psychosocial risks:
    - ICAS
    - Pulso
    - Checkmarket

- Personal data within the framework of medical supervision:
    - Laboratory analyses:
        - The Central Laboratory for Medical Analyses
        - Vivalia
    - Via E-Health My Box: Personal data within the framework of rehabilitation research will be exchanged between Mensura and the health insurance providers and/or the treating physicians.
    - FEDRIS: personal data within the framework of occupational illness reporting, reimbursement of medical exams for interns, reimbursement of vaccinations
    - Vaccinnet: personal data within the framework of vaccinations

- Personal data within the framework of ergonomics:
    - E-coach: anonymous processing of results of completed questionnaire
        - U&I: storage of the data