Privacy Policy and Personal Data Security

Revision history

Version	Date	Responsable	Overview of changes
1.0	27.01.2020	Mathieu Pouletty	First version

Approval

Name: _____

Date: _____

Signature: _____

Privacy Policy and Personal Data Security

1 Introduction

2 Privacy and Personal Data Security Policy 2

2.1 Purpose 2

2.2 Defination of the GDPR 2

2.3 Principles for the management of personal datas 3

2.4 The rights of the individual 4

2.5 Legak management 5

2.5.1 Consent 5

2.5.3 Legal Obligation 6

2.5.4 Vital interests of the data subject 6

2.5.5 Task in the public interest 6

2.5.6 Legitime interest 6

2.6 Data security through design 7

2.7 Contracts relating to the processing of personal data 7

2.8 International transfers of personal data 7

2.9 Dataprotection 8

2.10 Security breach 8

2.11 Measures to comply with the GDPR 8

1. Introduction

In its day-to-day operations, MINDstrain makes use of a variety of information about identifiable individuals, including data on:

- Current, former and potential employees
- Customers
- Users of its website
- Collaborators
- Independent coaches

Through the collection and use of this data (called processing), MINDstrain is subject to a number of different laws that govern how such activities can be carried out, as well as the security measures that must be in place.

GDPR is a significant law that affects the way MINDstrain performs its data processing activities. Substantial fines can be imposed if the company violates the law, which is designed to protect the personal data of EU citizens.

1 Privacy and Personal Data Security Policy

1.1 Purpose

The purpose of this policy is to define the relevant legislation and to describe the decisions taken by MINDstrain to ensure compliance.

It is thus MINDstrain's policy to ensure compliance with the GDPR and other relevant legislation and that this can be documented at any time.

The policy applies to all systems, people and processes that make up the company, including board members, directors, employees, partners, suppliers and other third parties who have access to systems at MINDstrain

1.2 Basic definitions in the GDPR

The most basic definitions in relation to this policy are as follows: Personal data is defined as: any information concerning an identified or identifiable natural person ('the data subject'); identifiable natural person means a natural person who can be directly or indirectly identified, in particular by an identifier such as a name, identification number, location data, online identifier or one or more elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; Treatment is defined as: any activity or series of activities - with or without the use of automatic processing - to which personal data or a collection of personal data is made subject, e.g. collection, registration, organization, systematization, storage, adaptation or modification, retrieval, search, use, disclosure by transmission, dissemination or any other form of transfer, assembly or interconnection, restriction, deletion or destruction; Data controller is defined as: a natural or legal person, a public authority, an institution or another body which, alone or together with others, decides for what purposes and by what means the processing of personal data may be carried out; if the purposes and means of such processing are laid down in Union or national law of the Member States, the controller or the specific criteria for its designation may be laid down in Union or national law of the Member States;

There are a number of basic principles on which the GDPR is based.

These are as follows:

1. Personal data must:

(a) is treated lawfully, fairly and in a transparent manner in relation to the data subject ('legality, fairness and transparency');

(b) be collected for express and legitimate purposes and must not be further processed in a manner incompatible with those purposes; further processing for archival purposes in the public interest, for scientific or historical research purposes

or for statistical purposes in accordance with Article 89 (2); Shall not be considered incompatible with the original purpose ('purpose limitation')

(c) be adequate, relevant and limited to what is necessary for the purposes for which they are processed ('data minimization');

(d) be accurate and, where necessary, updated; every reasonable step must be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are immediately deleted or rectified ('accuracy');

(e) stored in such a way that it is not possible to identify the data subjects for a longer period than is necessary for the purposes for which the personal data in question are processed; personal data may be stored for a longer period if the personal data are processed solely for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 (1). Provided that appropriate technical and organizational measures required by this Regulation are implemented in order to safeguard the data subject's rights and freedoms ('storage restriction');

(f) processed in a manner that ensures adequate security of the personal data concerned, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

2. The Data Controller is responsible for complying with, and must be able to demonstrate compliance with, point 1 ('responsibility').

MINDstrain will ensure that it adheres to all these principles both in the processing currently carried out and as part of the introduction of new methods of processing, such as new IT systems.

1.2 The rights of the individual

The data subject also has rights under the GDPR. These consist of:

- *Right to be informed*
- *Right of access to documents*
- *Right to rectification*
- *Right to delete*
- *Right to limitation of treatment*
- *Right to data portability / have data moved to another provider*
- *Right to object to treatment*
- *Rights in relation to automated decision-making and profiling*

Each of these rights is supported by appropriate procedures of MINDstrain, which set out the necessary measures and deadlines to be complied with under the GDPR.

Request	*Time horizon*
Right to be informed	*When data is collected (if provided by the data subject) or within a month (if not provided by the data subject)*
Right of access to documents	*One month*
Ret til berigtigelse	*One month*
Right to delete	*No delay necessary*
Right to limit treatment	Without unnecessary delay
Right to data portability	*One month*
Right to object to treatment	*Upon receipt of objection*
Rights in relation to automated decision-making and profiling.	*Rights in relation to automated decision-making and profiling.*

Table 1 - deadlines for requests

1.2 Legal treatment / Legal authority

Under the GDPR, it is possible to obtain legal authority for data processing in six alternative ways. It is MINDstrain's policy to identify the legal basis for the individual data processing as well as to document it. The possibilities are briefly described in the following sections.

1.1.1 Consent

Unless legal authority can be found otherwise, MINDstrain will always seek the express consent of the data subject to collect and process their data. For children under the age of 16, parental consent must be obtained.

Consent must be based on transparent information about our use of personal data. In addition, we provide information about the data subjects' rights, such as the right to withdraw consent. This information will be provided in an accessible format, written in clear language, at the time consent is obtained.

If no personal data is obtained directly from the data subject and the processing must be based on consent, the information must be given to the data subject within a reasonable period of time after receipt of data, preferably within one month.

1.1.1 Fulfillment of an agreement / contract

If processing is necessary for the performance of a contract to which the data subject is a party or if processing is necessary for the implementation of measures

If taken at the request of the data subject before concluding a contract, express consent is not required.

This option will often be used as a legal basis when the contract / agreement cannot be carried out without the personal data in question, - e.g. it is clear that a delivery cannot be completed without an address to deliver to.

These deadlines are shown in Table 1

1.1.1 Legal obligation

If personal data is collected and processed for the purpose of complying with the law, express consent is not required. This may be the case where data relates to employment and taxation, and for many areas within the public sector.

1.1.1 Vital interests of the data subject

In cases where the processing of personal data is required to protect the vital interests of the data subject or other natural person, express consent is not required. By vital interests is meant first and foremost the consideration of life and health. MINDstrain prepares reasonable and documented evidence that this is the case when used as a legal basis for processing. As an example, this can be used in the context of social care, especially in the public sector.

1.1.1 Task in the public interest

If MINDstrain needs to perform a task that it believes is in the public interest or as part of an official duty, no consent must be requested. MINDstrain prepares reasonable and documented evidence that this is the case.

1.1.1 Legitimate interests / balancing of interests

If the processing of personal data is considered a legitimate interest in the "Name of the Company", and if the processing is not considered to significantly affect the data subject's rights and freedoms, express consent is not required.
MINDstrain prepares reasonable and documented evidence that this is the case.

Along with consent, legitimate interest is the most widely used legal basis for private companies' personal data processing

1.2 Data security through design

MINDstrain has introduced the principle of built-in personal data security and privacy protection in all new and significantly changed systems or processes.

This may involve conducting one or more impact assessments.

An impact assessment includes:

- Consideration of how personal data is processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose
- Assessment of risks for the data subject in the processing of his personal data
- What control measures are needed to address the identified risks and demonstrate compliance with the law

The use of techniques such as data minimization and pseudonymisation is considered where appropriate and appropriate.

1.2 Contracts relating to the processing of personal data

MINDstrain will ensure that all relationships entered into involving the processing of personal data are subject to a documented contract containing the specific information and terms required by the GDPR.

1.3. International transfers of personal data

Transmission of personal data outside the EU will be carefully reviewed prior to the transfer to ensure that it falls within the limits of the GDPR. This depends in part on the European Commission's assessment of the extent to which there are adequate guarantees for personal data in the recipient country, which may change over time.

Intra-group international data transfers to third countries require legally binding agreements, known as binding corporate rules (BCR).

1.2 Data Protection Adviser

A defined role as data protection adviser (DPO) is required in an organization is a public authority if surveillance is carried out on a large scale or if particularly sensitive types of data are processed on a large scale. The data protection consultant must have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

MINDstrain does not need to appoint a data protection adviser, based on the above criteria

1.2 Security breach

A securitybreach is an incident that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.
It is MINDstrain's policy to make a reasonable and appropriate balance when considering measures to inform stakeholders of breaches of personal data security. The balance should include whether there is a risk of the data subject suffering physical, material or moral damage, the amount of data, as well as the size of the risk.

If a breach is discovered to have taken place, which is likely to result in a risk to the data subjects, the Danish Data Protection Agency (or other relevant supervisory authority) must be notified within 72 hours.

This will be handled in accordance with the Procedure for handling breaches of Personal Data Security, which establishes the overall process for handling incidents regarding. data security.

4.1 Measures to comply with the GDPR

The following measures have been taken to ensure that MINDstrain complies with the principle of accountability under the GDPR at all times:

- The legal basis for the processing of personal data is clear and unambiguous
- A data protection adviser is appointed with special responsibility for data protection in the organization

● All personnel involved in the handling of personal data understand their responsibility in practicing good data protection practices

● Data protection information has been provided to all employees

● Rules for consent are followed

● Guides are available to data subjects who wish to exercise their rights regarding requests for access to personal data and such requests are processed effectively

● Reassessment of procedures involving personal data is performed regularly

● Data protection through design has been adopted for all new or changed systems and processes

● Documentation of treatment activities and data flows has been completed, with regard to:

o Company name and relevant details

o The purpose of the data processing

o Categories of individuals and personal data processed

o Categories of recipients of personal data

o Agreements and control mechanisms have been put in place for the transfer of personal data to non-EU countries

o A plan for deleting and storing data has been adopted

o Relevant technical and organizational control bodies are in place

These measures are regularly reassessed as part of the ongoing work on data protection.