MANGOLD

POLICY
PERSONAL DATA MANAGEMENT
15-06-2021

1. GENERAL BASIS

Mangold is subject to the EU General Data Protection Regulation, GDPR, which regulates how personal data may be processed. Mangold therefore has a policy that shall ensure the secure handling of personal data and compliance with the GDPR.

2. RESPONSIBILITY

In his capacity as representative of Mangold, the CEO is ultimately responsible for ensuring that the requirements incumbent on Mangold as the Personal Data Controller are complied with.

Within Mangold, there is also an appointed Data Protection Officer (DPO) who is responsible for monitoring that Mangold fulfils obligations and requirements stipulated in the GDPR and in other legal obligations.

All managers in the business are responsible for ensuring that their department follows the procedures and guidelines established by the Board of Directors and the CEO, and that all new or changed processing of personal data is notified to the DPO.

3. DEFINITIONS

3.1. Personal data

Personal data is all information that can be linked to and identify a living natural person. Personal data can be, for example, a name, photo, telephone number or custodian account number.

3.1.1. Sensitive personal data

Certain personal data is by nature particularly sensitive and therefore has stronger protection according to the GDPR. Such personal data may reveal a person's ethnic origin, political opinions, religious or philosophical beliefs, or information on health and sexual life, but also personal data relating to criminal offenses and social security numbers. The basis is that it is forbidden to process such personal data. However, there are a number exceptions to the ban.

3.2. Processing of personal data

Processing of personal data involves a measure or a combination of measures concerning personal data. A measure may be the gathering, storage, use, reading or deletion of personal data, or anything else that involves the handling of personal data. At Mangold, several types of personal data are processed in many different ways by different functions. Advisors process personal data on customers. HR processes personal data on the employees. The Compliance department processes personal data on both customers and employees.

3.3. Personal Data Controller and Data Protection Officer

A Personal Data Controller is the natural or legal person who, alone or together with someone else, is/are responsible for and determine(s) the purposes and means of the processing of personal data.

Those who process personal data (as in Mangold's case) must, in certain cases, appoint a Data Protection Officer. The role of the Officer is to check that the General Data Protection Regulation is complied with within the organisation. Mangold has made the assessment that, for the business which Mangold operates, a Data Protection Officer is not required by law. Mangold shall, however, comply with all laws and regulations and, in a continuous and risk-based manner, work with data protection issues in accordance with this policy. To ensure that this work is carried out efficiently, Mangold has decided that a Data Protection Officer should be appointed nonetheless.

MANGOLD

POLICY
PERSONAL DATA MANAGEMENT
15-06-2021

3.4. Principles for the processing of personal data

When personal data is processed, the data must be processed in a *legal*, *correct* and *transparent* manner. It is also important that personal data is protected from unauthorised processing or alteration, and that integrity and confidentiality are ensured. The three principles for the processing of personal data entail the following;

- *Legality*. Personal data shall not be processed in a manner contrary to the regulation. For example, personal data shall not be used for any purpose other than that for which it was gathered.
- *Correctness*. The personal data gathered shall be correct and up-to-date and thereby not incorrect.
- *Transparency*. The processing of personal data shall be open and transparent, which means that it shall be clear which personal data is processed, how it is processed, and why it is processed. Information about the processing must be provided to the data subject in a clear and unambiguous manner.

3.5. Purpose limitation

Personal data may only be gathered for specific, explicitly stated and justified purposes. Those who gather and process personal data must therefore decide in advance why the data is gathered before it takes place. The personal data may not later be used for any purpose other than that for which it was originally gathered.

3.6. Storage of personal data

The Personal Data Controller may not store personal data in a form that allows the data subjects to be identified for a longer period than is necessary for the purpose for which the personal data is processed. Personal data that is no longer needed for the purpose for which it was gathered shall therefore be deleted or de-identified.

To ensure that personal data is not stored longer than necessary, those processing personal data should introduce time limits and procedures for deletion or de-identification.

4. PERSONAL DATA MANAGEMENT

4.1. When personal data may be processed

To be allowed to process personal data, a *legal basis* for the processing is required. That which constitutes a legal basis is determined in Article 6 of the General Data Protection Regulation. One or more of the justified conditions must therefore be fulfilled in order for personal data to be processed.

Legal basis can be consent, agreement, balancing of interests, legal obligation, exercise of authority, and information of general interest or fundamental interest.

4.2. The data subject's right to receive information about processed personal data

The data subject has the right to receive a confirmation from the Personal Data Controller that their personal data is being processed. The data subject has the right to access the personal data and information about, among other things, the purposes of the processing, which categories of personal data it relates to, and how long the personal data is to be stored. The data subject therefore has the right to access the personal data concerning them, but not the document or e-mail itself where their personal data is processed.

4.3. Correction and deletion

In accordance with the General Data Protection Regulation, the Personal Data Controller shall *correct* inaccurate personal data if the data subject so requests. The Personal Data Controller shall also *delete* personal data if the data subject so requests, provided that certain conditions are met. If personal data is corrected or deleted, the Personal Data Controller must inform all recipients of the personal data that the data has been changed or deleted.
There are, however, exceptions in other laws that make a longer storage than that which is permitted under the General Data Protection Regulation acceptable. For example, according to the Swedish Securities Market Act, securities companies must store certain information for at least five years, the same applies according to the

Swedish Money Laundering Act, while the Swedish Accounting Act stipulates a storage period of seven years. In addition, there is the general limitation period of ten years, which may justify storage during that time. Such storage is permitted under the General Data Protection Regulation as there are exceptions in other laws.

4.4. Personal data from or to someone other than the data subject

If personal data is obtained from someone other than the data subject, the data subject must be informed that their personal data will be processed. Information about the handling must be sent within one month of receiving the data. If the Personal Data Controller believes that they will pass on the personal data to a third party, the data subject must be informed of this at the latest when the personal data is disclosed for the first time.

If personal data is intended to be transferred to a third country, the data subject must give their consent to this. If, before entering into a business relationship, the Personal Data Controller knows that the data subject's data will be transferred to a third country, the Personal Data Controller must tell the customer.

4.5. List of personal data processing

The Personal Data Controller is obliged to keep a record of all personal data processing within the company. These records shall be drawn up in writing, be available in electronic format, and be kept up to date. Upon request, the records shall be made available to the Swedish Authority for Privacy Protection.

5. PERSONAL DATA PROCESSOR

The Personal Data Processor is the party who processes personal data on behalf of the Personal Data Controller. A Personal Data Processor is always located outside of the Personal Data Controller’s organisation. A personal data assistant can be a natural or legal person, public authority, institution, or other body.

The Processor engaged by the Personal Data Controller shall be able to provide sufficient guarantees that the processing fulfils the requirements of the General Data Protection Regulation and ensure that the data subject's rights are protected.

A Personal Data Processor and their personnel may only process personal data in accordance with instructions from the Personal Data Controller. The Processor may not engage another Processor without obtaining written permission from the Personal Data Controller in advance.

The Personal Data Processor can also be subject to supervision or administrative penalty fees and be liable for damages. The Personal Data Controller and the Personal Data Processor must draw up a so-called Data Processor Agreement. The General Data Protection Regulation lists what such a Data Processor Agreement shall contain.

6. DATA PROTECTION OFFICER

Mangold has chosen to appoint a Data Protection Officer (DPO). Mangold shall ensure that the DPO does not have information that could lead to conflicts of interest. This means in particular that the DPO cannot hold a position within the organisation that means the DPO determines the purposes and means for processing personal data. The DPO shall have an independent position when they carry out their duties.

Mangold shall ensure the following:

1) That the DPO is regularly invited to participate in meetings at the highest and intermediate administrative level;
2) That the DPO participates when decisions with consequences for data protection are made.

3) That the DPO's opinion on relevant issues is given due weight. If Mangold chooses not to follow the DPO's advice, this shall be documented.
4) That the DPO shall be informed and consulted immediately when a personal data incident has or may have occurred.
5) That the DPO has resources in the form of information, time and training to be able to carry out their duties.

6.1. The DPO's tasks

The DPO shall inform and advise Mangold on personal data processing. The DPO shall also monitor compliance with the GDPR. This may mean that the DPO:

1) Gathers information on how personal data is processed within Mangold.
2) Analyses and verifies whether personnel comply with the provisions laid down in this policy and the GDPR.
3) Issues recommendations to Mangold on the processing of personal data.

Employees, customers and other data subjects should be able to easily get in touch with the DPO. For customers and other external data subjects, contact is made by post to the address:

Mangold Fondkommission AB
F.A.O.: GDPR
P. O. BOX 55691
102 15 STOCKHOLM

The DPO shall act as a contact person with the Swedish Authority for Privacy Protection.

If the business wants to propose changes to this policy or any other policy that affects Mangold's processing of personal data, the DPO shall be consulted before the change is submitted for decision, to ensure that proposed changes do not adversely affect Mangold's work to comply with GDPR requirements.

6.2. Personal data incidents

Incident investigation is handled by the COO and Compliance departments in accordance with provisions in the policy for incident management and significant events. These departments are responsible for keeping the DPO informed of personal data incidents and the measures taken.

The DPO shall provide assistance in the form of advice and support if a personal data incident occurs or may have occurred. The DPO shall document the potential personal data incident and the assessment made thereof, and submit this assessment to the Compliance and COO departments.