Dilafor AB

Privacy Policy

Datum: 2024-11-05 Version: 1,2

Contents

Purpose

The Privacy policy applies to Dilafor AB (556642-1045) or other businesses within the same corporation group as previous named (henceforth **"Dilafor"**, **"we"**, **"our"**, **"us"**).

The policy is approved by the management and is updated at a needs basis. The policy constitutes general information about how the company processes internal and external personal data.

Personal data controller is responsible for the annual update of the policy according to decision by the management.

Personal data is handled within the company and its operations. The data is processed, among other things, in order for the company to be able to fulfill agreements entered into with customers, suppliers and employees and due to obligations under law. As a starting point, Dilafor's customers are the data controller for all processing of personal data made under agreements between us and our customers. For such processing, the company enters into personal data processing agreements with its customers and processes the data under instruction from and on behalf of the customer.

This general privacy policy (the "Privacy Policy") applies when we process data on our own account, i.e. when Dilafor is the data controller. The Privacy policy applies to all employees and hired personnel of our company including management, employees and persons acting on behalf of the company (such as third party consultants).

The overall purpose of this Privacy policy is to establish roles and responsibilities within our organization, as well as to establish the standards and principles that will ensure that the collection and processing of personal data within the company is carried out in accordance with applicable Data Protection Legislation (as defined below).

Definitions

Processing (personal data) is any measure of series of measures taken in respect of personal data, whether automatic or not, such as collection, registration, organization, storage, processing, alteration, restriction, adjustment, erasure or destruction, disclosure by transmission, dissemination or other provision of data, compilation or interconnection.

Processing register refers to the register that Dilafor is obliged to transfer personal data processing in accordance with Article 30 of the GDPR. We use the service "GDPR Hero" to keep our processing register.

Data protection legislation refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April on the protection of physical persons with regard to the processing of person data and on the free movement of such data ("GDPR") and any other national or European law, regulation or directive applicable from time to time to the company's processing of personal data.

Personal data is any information relating to an identified or identifiable physical person who is alive. Identifiable physical person means a person who can be identified directly or indirectly by reference to an identifier as a name, identification number, location data or online identifiers or one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of the physical person.

The personal data controller is the legal person who alone or together with others determines the purposes and means of the processing of personal data.

The personal data processor is a legal entity that processes personal data on behalf of the controller, e.g. Dilafor's IT-providers.

The Privacy Protection Agency (IMY) conducts checks in response to complaints from individuals, information in the media or on its own initiative. Measures include field inspections and inspections by questionnaires or other verification by e-mail, telephone or letter.

1. Basic principles of Dilafor's personal data processing

We shall comply with applicable Data Protection Legislation when processing personal data at any time.

We shall only process personal data in a lawful, correct and transparent manner in relation to the data subject and the controller. This means, among other things, that our personal data processing must follow these basic principles:

- **Documented personal data liability:** For each processing of personal data, where we determine the purpose and means, there shall be one or more companies within the company that have been deemed to be the data controller. Responsibility for processing where companies within the company are data controllers must be documented in the Processing Register.
- **Legal basis:** Any processing of personal data shall be carried out on the basis of a documented legal basis.
- **Purpose limitation:** The data shall be collected for specified, expressly stated purposes and shall not subsequently be processed in an incompatible manner.
- **Purpose limitation:** Only personal data that is adequate, relevant and not too comprehensive in relation to the purpose shall be collected.
- **Accuracy:** The data shall be accurate and up-to-date and it shall be possible to trace changes.
- **Storage minimization:** The data may not be kept for longer than is necessary in relation to the purpose, see further paragraph 5.
- **Confidentiality:** Personal data shall be protected by appropriate technical and organizational security measures to prevent unauthorized processing and loss, destruction or corruption of the data. See further, paragraph 6.

2. When the processing of personal data is legal

2.1 General legal basis

The processing of personal data is only legal if at least one of the following conditions is met:

- The data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes.
- The processing is necessary for the performance of a contract in which the data subject is a party or to take action at the request of the data subject before such contract is concluded.
- The processing is necessary in order to fulfil a legal obligation where the responsibility lies with the controller.

- The processing is necessary to protect interests of fundamental importance to the data subject or to another physical person.
- The processing is necessary for the performance of a task of general interest or as a part of the controller's exercise of authority.
- The processing is necessary for the purposes relating to the legitimate interests of the controller or a third party unless the interests or fundamental rights and freedoms of the data subject outweigh and require the protection of personal data.

The legal basis for our processing of personal data shall be determined and documented in the controller's Processing Register. In case of uncertainty, consultation shall take place with Dilafor's Group Privacy Manager (GPM).

2.2 Legal basis for personal data processing in recruitment

Processing is necessary in order to be able to handle the application from the person applying to work with us and is based on the consent given in connection with the application. We have no interest knowing trade union, religious beliefs, sexual orientation, political opinions, any illnesses or other information that is irrelevant to the recruitment process.

For certain specific processing operations in connection with recruitment, Dilafor may need additional supplementary or deviant information about individual processing of your data.

3. Rights of the data subject

A fundamental aspect of the GDPR is that it contains certain statutory and mandatory rights for data subjects whose personal data are processed. As a data controller, Dilafor has an obligation to facilitate those who wish to exercise their rights under the GDPR.

If a person wishes to know what information is registered about him or her, or if the person wants to exercise any other of their rights under the GDPR, you are referred to Dilafor's GPM.

The data subject also has the right to withdraw any consent given. The withdrawal of consent shall not affect the legality of processing based on consent before it is revoked.

- Data subjects have the following rights, among others: Right to access your personal data, which means that you have the right to receive confirmation of whether personal data relating to you is being processed and if so, also access the personal data and certain additional information about the processing.
- Right to data portability, which means that the data subject has the right to access personal data under certain circumstances, in order to transfer the personal data to another controller. Right to rectification, erasure or restriction of their personal data and the right to object to the processing.
- Right to complain to the national data protection agency (in Sweden IMY) if the processing of their personal data does not meet the requirements of EU/EEA data protection legislation.
- Right to withdraw their consent if and to the extent that specific consent was given to certain processing.
- Right to object to the balancing of interests when processing is based on the so-called balancing of interests according to nature 6.1 (f) of GDPR.

- Right to object to direct marketing when processing their personal data. In that case, the personal data shall no longer be processed for such purposes.

4. Storage and deletion of personal data

According to data protection law, personal data may not be stored for longer than permitted by law, or otherwise necessary for the purposes for which the data is processed. Data that may no longer be stored shall be permanently deleted and destroyed (thinning). Under special conditions thinning can be carried out by anonymizing personal data instead of being destroyed. Anonymization means that any information that makes it possible to trace the data to a data subject is irrevocably deleted.

If there are certain laws or regulations that require the storage of personal data for a certain period of time, such as in tax-, accounting- or money laundering legislation, such provisions apply before the GDPR. For example, the Accounting Act states that accounting information must be kept for seven years from the year in which the financial year ended.

The main rule within the company is that personal data that is not subject to certain laws or regulations (in addition to data protection legislation) should be deleted when we no longer need the data to fulfil the purposes of the processing.

5. Security in the processing of personal data

5.1 General

Dilafor shall take appropriate technical and organizational measures to prevent the destruction, altering or distortion of personal data. This means that a security assessment needs to be made on a case-by-case basis and that different processing/systems require different levels of security measures depending on the sensitivity of the information, the risk of intrusion (and other risks) and vulnerability.

5.2 Risk analysis

Before we start processing personal data, an initial risk analysis must be carried out to take a position on:

- The technical and organizational security measures appropriate for the processing in question, based on an assessment of information sensitivity, relevant risks and vulnerabilities.
- If the processing is adapted from the outside and meets our requirements regarding privacy by design and information security.
- Where the processing is likely to pose a high risk to the rights and freedoms of the data subject, for example through the use of new technologies or by the fact that data subjects cannot be expected to know that they are subjects to the processing. If such high risk is identified Dilafor's Group Privacy Manager (GPM) shall be informed and determine whether further analysis in the form of a Data Protection Impact Assessment is necessary.

6. Transfer of personal data

Personal data may be transferred to external parties with or without a personal data assistant agreement, depending on whether the recipient processes the data on Dilafor's behalf or on his own

account. In all cases, there must be a legal basis for the transfer and only the data that needs to be transferred. The transfer shall be documented in an appropriate manner.

6.1 Transfer to data processors

Dilafor may transfer personal data to external parties that processes personal data on our behalf and according to our instructions. Such external parties is a data processor assistant to us and shall always sign a personal data assistant agreement with Dilafor. Our Personal data controller is responsible to keep such templates updated and accordingly to applicable Data Protection Legislation from time to time.

6.2 Transfer to parties with their own personal data liability

Dilafor may transfers personal data to other external party which have their own personal data liability, provided that we have legal basis for such transferring. Such legal basis may be, for example, that the transfer constitutes a legal obligation for us, or a customer agreement that gives us the right to transfer the data.

6.3 Transfer of personal data to a third country

If and to the extent our personal data processing involves the transfer, storage or otherwise processing of personal data outside the EU/EEA, further measures are required for the processing to be lawful. It is sufficient that the personal data is accessible from the outside the EU/EEA, or that certain infrastructure or resource is outside the EU/EEA, that further action is necessary. When transferring personal data outside the EU/EEA, the data subject shall be informed of the purpose and scope of the transfer.

The measures we take to ensure that personal data processing outside the EU/EEA is legal must always be documented and approved by Dilafor's Group Privacy Manager (GPM).

6.4 Request by the authority for information

Dilafor and its employees are obliged to provide information about our personal data processing and related circumstances if requested by the Privacy Protection Authority. Other authorities may also have the right to receive information that contains personal data from us, such as the Enforcement Authority, The Swedish Tax Agency or the Swedish Economic Crime Authority. There may also be an obligation to disclose information to the police or prosecutors in the event of a criminal investigation, information being disclosed only at the written request of the lead investigator och prosecutor.

In addition to regular and mandatory transfers of personal data to authorities that we have a legal obligation to report (e.g. salary data to the Swedish Tax Agency and information about sick leave to the Swedish social insurance), personal data shall be disclosed to the authority only after consultation with Dilafor's Group Privacy Manager (GPM).

Dilafor's Group Privacy Manager (GPM) is responsible for contact with the Privacy Protection Authority. All contacts with the Privacy Protection Authority, or other authorities regarding personal data processing issues, on behalf of Dilafor shall be referred to Dilafor's Group Privacy Manager (GPM).

7. Reporting

Dilafor's Group Privacy Manager (GPM) shall report annually or if necessary to management about our processing of personal data and, in addition, immediately report to management if serious flaws, privacy risks or problems arise.

The report shall contain the results of the follow-up and verification of personal data carried out in accordance with this Privacy Policy, including:

- If the processing as adapted from the outside and meets our privacy by design and information security requirements.
- Number of personal data breaches
- Our compliance of the applicable Data Protection Legislation and this Privacy Policy.
- Any contact with the Privacy Protection Authority; and
- Changes in applicable Data Protection Legislation and supervisory practices regarding the processing of personal data.

8. Contact information

If you have any questions about the processing of your personal data or about cookies, or if you want to exercise your rights specified above you are welcome to contact us according to below.

Dilafor AB (reg. nr. 556642-1045),
Fogdevreten 2A, 171 65 Solna
Phone nr: +46 8-524 847 02
E-mail: dpo@dilafor.com