AARSLEFF

Personal data policy

Table of contents

1. Introduction

This present personal data policy applies to Per Aarsleff A/S and its subsidiaries such as Aarsleff Ground Engineering Ltd. The policy describes how we intend to comply with the principles of the data protection act on the processing of personal data, how we comply with the rights of the data subjects as well as a number of other important conditions relating to the processing of personal data. The personal data policy applies to all employees of Per Aarsleff A/S and Aarsleff Ground Engineering Ltd.
The personal data policy must be read by employees of Aarsleff Ground Engineering Ltd who process personal data in connection with the execution of their work. The policy is embedded in the IT security committee.

The personal data policy is updated regularly, e.g. by implementing special IT systems or by changing procedures for processing of personal data.

1.1. Purpose

Motivated and dedicated employees are important to Aarsleff Ground Engineering Ltd. We wish to treat our employees with respect and this also comprises the protection of their personal data.
It is important to Aarsleff Ground Engineering Ltd to offer sufficient protection of personal data.

1.1.1. Target group

This personal data policy applies to all departments and employees of Aarsleff Ground Engineering Ltd. Employees who process personal data as a significant part of their jobs at Aarsleff Ground Engineering Ltd have a special responsibility that the policy is complied with.

1.1.2. Background

Processing of personal data about Aarsleff Ground Engineering Ltd employees must be carried out in accordance with the data protection act with a special focus on complying with the data protection act's principles on processing of personal data and the rights of the data subjects. The purpose of this policy is to regulate under what circumstances personal data can be processed and how the processing should take place. This applies e.g. when we process personal data that are based on a contract, a legitimate interest or a consent.

It is particularly important that we comply with the principles for processing personal data as stated in section 3 and that we comply the rights of the data subject as stated in section 4.

2. PERSON DATA RESPONSIBLE

The person data responsible of Aarsleff Ground Engineering Ltd has been appointed by the senior management and is a member of the company's senior management. The person responsible is responsible for overseeing that the rules for data protection are complied with.
The person responsible does not have the same function as a data protection officer (DPO) who is mentioned in the data protection act. Aarsleff Ground Engineering Ltd has assessed that it is not required to appoint a DPO under the law.

The person responsible is responsible for updating the personal data policy and for ensuring that it is complied with, e.g. through internal audits.

The person responsible of Aarsleff Ground Engineering Ltd – Richard Hoe, Financial Controller.

Managers of Aarsleff Ground Engineering Ltd must involve the person responsible in relevant matters, and the senior management must support the solving of tasks.

All employees of Aarsleff Ground Engineering Ltd can seek advice from the personal responsible or complain about processing activities. Your requests will always be treated confidentially.

3. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

According to the data protection act, there are 6 basic principles for processing of personal data. Personal data shall be:

1. processed lawfully, fairly and in a transparent manner *(lawful, fairness and transparency)*
2. collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes *(purpose limitation)*
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed *(data minimisation)*
4. accurate and, where necessary, kept up to date *(accuracy)*
5. kept in a form which permits identification of data subjects for no longer than is necessary *(storage limitation)*
6. processed in a manner that ensures appropriate security *(integrity and confidentiality).*

The below is a description of how Aarsleff Ground Engineering Ltd complies

with the principles. **3.1. Lawful, fairness and transparency**

Personal data shall be processed lawfully, fairly and in a transparent manner.

General personal data are processed on the following lawful basis:

- Article 6 point (a) – consent
- Article 6 point (b) – contract
- Article 6 point (c) – legal obligation
- Article 6 point (f) – legitimate interests.

Sensitive personal data are processed on the following lawful basis:

- Article 9 (subsection 2) point a – explicit consent
- Article 9 (subsection 2) point b – special obligations.

In the records of processing activities, the individual data processing activities are documented with the relevant lawful bases.

3.2. Transparency and obligation to inform

The processing of personal data must be transparent. Therefore, we provide information on how personal data is processed. As a principle we only collect personal data directly from the relevant person. During the processing of personal data we will provide information about:

- Contact details of the personal data responsible
- The purpose of the processing and the legal basis for the processing
- The recipients or categories of recipients of the personal data
- Data transfers to a third country (if relevant)
- How long the processing lasts
- The rights of the data subject
- The right to withdraw consent
- The right to complain to the Information Commissioners Office
- Automated profiling, if this is used.

The requirement to inform about the processing of personal data is provided on the intranet in so far as concerns our own staff and on our website in so far as concerns external parties.

New employees will get an appendix to the employment contract with information about the processing of personal data at Aarsleff Ground Engineering Ltd during their employment.

3.3. Purpose limitation

During the collection and processing of personal data, information about the purpose of the processing should be provided. Personal data must not be processed for other purposes than those described in this personal data policy.

Aarsleff Ground Engineering Ltd purpose of processing personal data can be summarised in the following categories:

- Recruitment
- Staff administration
- Documentation requirements towards customers and authorities
- Occupational health and safety matters
- Insurance matters
- Documentation towards customers
- Planning
- Security
- Sales and marketing
- Compliance with relevant legislation.

Aarsleff Ground Engineering Ltd employees must not process personal data in a way that deviates from the above purposes. If a purpose changes, in exceptional cases, the data subjects will be informed of the change.

3.4. Data minimisation

Before collection of personal data it must be examined whether the processing hereof is limited for what is necessary. We do not collect more data than necessary, and data are only collected for specific purposes. In a number of processes, it is not unambiguous where the processing of personal data is to take place. These

processes and assignments are mentioned below with an indication of which system that *must* be used. The reason is that if storage and processing of personal data do not follow explicit requirements, the data minimisation principle cannot be complied with.

Data minimisation is carried out e.g. by processing personal data in IT systems that are suited for the purpose:

- Recruitment with written applications (HR-Manager)
- Personality tests before and during employment (Thomas Profiling)
- Job interviews (archive as appropriate on company servers)
- Registration of employee skills (CITB)
- Occupational health and safety matters (Screen4)
- Expense management system (Exchequer)
- HR documents (on company servers)

Within the above-mentioned areas, personal data must not be processed in other IT systems. In case of doubt, the personal data responsible must be contacted.

To the extent that paper records are used, the data must be locked away and only accessible to authorised employees.

3.5. Accuracy

Personal data must be updated so that they are accurate. Data subjects may contact the HR Department themselves to have their personal data updated.

3.6. Storage limitation

Personal data must be deleted, when they are no longer relevant for the purposes for which they were collected.

- Data about applicants that are not employed will be deleted at the latest 6 months after the rejection has been sent unless the applicant has consented to the application being stored for another 6 months.
- All personality test results will be anonymised at the latest after 6 months.
- Data about permanently employed staff will be deleted (or anonymised) at the latest 40years after their resignation from the company. (legal UK required time Employees Liability insurance)
- Emails combining a name and a National Insurance Number will be deleted at the latest after 6 years.
- Photos from video surveillance must be deleted at the latest after six months
- Occupational health and safety matters will be deleted after 40years, unless otherwise prescribed by legislation (legal UK required time Employees Liability insurance)

Aarsleff Ground Engineering Ltd records of processing is the source for assessment of time limits for erasure.

Erasure of personal data may also take place if a data subject has withdrawn consent or if there is a request for erasure provided this request complies with obligations under UK law.

Erasure of personal data applies to data which is stored electronically as well as to data stored in paper form. When data are erased irrevocably, it can no longer be restored. Paper records must be shredded, and electronically stored data must be erased irrevocably.

3.7. Integrity and confidentiality

Aarsleff Ground Engineering Ltd employees must not collect, process or use personal data without authorisation. Any processing of personal data undertaken by an employee that he/she has not been authorised to carry out as part of his/her duties is unauthorised.

The confidentiality requirement during processing of personal data always applies to Aarsleff Ground Engineering Ltd employees who are assigned with this task during their daily work.

It is forbidden to use personal data for private or commercial purposes, to disclose personal data to unauthorised persons or to make it available in any other way.

According to the terms of this personal data policy, unauthorised persons also include colleagues, unless access to these data is authorised as a part of their responsibilities.

The confidentiality requirement also applies in case of termination of employment.

Emails with sensitive personal data and the combination of name and National Insurance Numbers must not be sent to external email addresses without encryption. Until the solution has been implemented, the attached documents with confidential or sensitive personal data must be protected with a password when they are sent to external email addresses. An email comprising the password to the document must be sent separately. Also, emails with sensitive or confidential personal data must be deleted at the latest after 30 days in inbox, outbox and deleted emails.

Sensitive or confidential personal data must not be stored locally on portable devices unless data is encrypted.

3.7.1. Personal data requiring special protection

Aarsleff Ground Engineering Ltd processes sensitive data to a limited extent. These are processed in the occupational health and safety system SafetyNet. Access to these data must be authorised by the occupational health and safety manager.

Insurance matters about travelling employees and their family members may contain sensitive personal data. Such data must be stored, so that third parties cannot get access. Access to the data must be authorised by the insurance coordinator.

Data which are not sensitive under the law but which must still be treated confidentially are:

- National Insurance Numbers
- Information about salary
- Summaries of job satisfaction and development interviews
- Summaries of manager-employee conversations
- Summaries of exit interviews
- Personality test results

3.7.2. “Need to know” principle

To secure a high security of processing, access to personal data is provided on a “need to know” principle. Employees may have access to personal data only if this is appropriate for the type and scope of the task in question.

4. THE RIGHTS OF THE DATA SUBJECTS

Data subjects of Aarsleff Ground Engineering Ltd have several rights which must be observed to the widest

extent possible. The rights are:

- Access to own data upon request
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to object to processing
- Right to data portability
- Right to human involvement in case of automated decision-making.

In general, data subjects of Aarsleff Ground Engineering Ltd may exercise their rights by contacting the personal data responsible who will take the required measures to comply with the wishes of the request, if possible.

4.1. Right to access to own data

If a data subject wants to have access to their own personal data, a copy of the data must be supplied. The requested data must be supplied to the data subject no later than one month after the request. However, it is vital that persons wanting to have access to their own personal data can identify themselves.

When making the request, we must provide the following information:

- The purpose of our processing of the relevant data
- Categories of processed data
- From where the data has been received
- Categories of data recipients
- The data processing period (if we cannot provide precise information about this, we must inform of the purpose for storing the data)

When answering the request, the data subject must be informed of the right to have own data erased (if this is possible), to have data updated, the right to restriction of processing (if the accuracy of the information is contested, the right to protest against the processing and the right to complain to the Data Protection Agency.

The records of processing activities are the source for meeting these requirements.

Data subjects may contact the personal data responsible in case of subject access requests. The personal data responsible will coordinate the collection of information.

4.2. Right to rectification

Data subjects registered with Aarsleff Ground Engineering Ltd have the right to have his or her data updated within one month if they are inaccurate or incomplete. If these data have been transferred to a third party, he or she must be informed of the update.

If the data are master data, the employee in question must send an e-mail to the HR Department which will update the data.

In case of rectification of other personal data, the personal data responsible should be contacted for subsequent coordination of tasks.

4.3. Right to erasure (right to be forgotten)

The right to erasure is not an absolute right. The following three grounds must always be considered:

- Are the personal data still relevant in relation to the purposes for which they were collected or otherwise processed?
- Did the data subject withdraw consent?
- Has the data subject objected to the processing and is there no other ground for continuing the processing according to the balancing of interest rule?

Data which are no longer relevant for the purpose for which they were originally processed, must in particular cases be deleted on request. The same applies when *consent* is the basis of the processing. Here the data must be deleted when the consent is withdrawn *unless* there is another legal ground for continued processing.

To ensure a correct processing of requests for erasure, the personal data responsible *must* – without exemption – be involved when there is a request for erasure.

4.4. Right to restriction of processing

This right may come into force if the accuracy of the personal data is contested by the data subject. In such cases, the person receiving the request must contact the personal data responsible who will handle the further processing.

4.5. Right to object

Aarsleff Ground Engineering Ltd employees have the right to object to processing of personal data if it is lawfully based on the balancing of interest rules.

If an objection to processing of personal data is received, the personal data responsible must be contacted. The personal data responsible will take the necessary steps to stop the processing.

In case of an objection, the person making the objection must be informed of the right to complain to the Information Commissioners Office

4.6. Right to data portability

Data subjects registered with Aarsleff Ground Engineering Ltd have the right to receive the personal data concerning him or her in a readable format. This right applies to:

- Personal data which the data subjects themselves have provided to Aarsleff Ground Engineering Ltd
- When the processing is based on a consent or on a contract.

In case of such requests, the personal data responsible and the IT manager will look into the possibilities.

4.7. Automated decision-making

Automated decision-making is defined as data processing with the intention to evaluate certain personal aspects:

- Performance at work
- Economic situation
- Health
- Personal preferences
- Reliability
- Behaviour
- Location
- Movements

Where automated processing of personal data is used (technical skills or psychological profiling) it requires special attention. The data subject shall have the right not to be subject to a decision based solely on automated processing if it may have negative effects. This involves human intervention from our side where a relevant employee verifies that the results are correct. Information about *automated profiling* is provided through the obligation to inform.

5. TRANSFER OF PERSONAL DATA TO THIRD PARTIES

If personal data is transferred to third parties, it must be ensured that the required lawful basis exists. If it is assessed that that a third party will become an independent data controller in connection with the transfer, this should be informed in connection with the transfer.

6. DATA PROCESSORS

When external data processors are used, a data processor agreement must be entered into. The definition of a data processor is that he or she processes data according to guidelines from Aarsleff Ground Engineering Ltd and that he or she is not allowed to use data for his or her own purposes. The below measures must always be taken before entering into a contract with data processors:

- When choosing a data processor, it must be ensured that the company has implemented adequate technical and organisational security measures.
- There must always be a written agreement stating the terms of the data protection. It must always be stated that the data processor only acts in accordance with instructions from Aarsleff Ground Engineering Ltd

The data processor agreement must comprise:

- Categories of data subjects
- Categories of personal data
- The purpose of the processing
- The duration of the processing
- The type of processing
- Information that personal data are only processed according to guidelines from Aarsleff Ground Engineering Ltd

- Information that only specially authorised staff have access to personal data (this also applies to sub data processors)
- Information that risk assessments are made available to Aarsleff Ground Engineering Ltd
- Information that assistance is offered if there are requests from data subjects as to enforcement of their rights
- Documentation that the data processor can investigate a data leakage
- Information that all personal data are deleted or transferred to Aarsleff Ground Engineering Ltd when the agreement has expired
- Documentation for compliance with the GDPR
- Information that the data processors will inform Aarsleff Ground Engineering Ltd if they think that the processing is against the law
- Information that the data processors will only use sub data processors according to agreement with Aarsleff Ground Engineering Ltd

The data processor must also be able to document:

- Name of the data controller
- Categories of processing activities taking place in relation to the data controller
- Implementation of sufficient policies and procedures
- Data transfers to a third country (if relevant)
- That they have sufficient control measures as well as technical and organisational security measures
- That they collaborate with relevant data protection agencies
- When data must be deleted
- That they comply with the rules of the general data protection regulation.

It is *very important* to follow up on the security of the data processors. This can be done by asking for an audit report or by submitting relevant questions about information security of the data processors in question.

In case of doubt, the personal data responsible must be contacted.

6.1. Transfer to third countries

If personal data are transferred to third countries (countries outside EU), it may require the *necessary guarantees*, binding company rules or that the data recipient (e.g. a data processer) e.g. has a Privacy Shield certification. Prior to the transfer of personal data to third countries, the personal data responsible must always be consulted.

7. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

A data protection impact assessment is a risk analysis of planned processing activities assessing the risk of the data subject.

The analysis must describe the nature of the personal data processing, assess necessity, proportionality and identify measures to mitigate risks for the data subject.

A DPIA must be prepared in case of introduction of new technologies (e.g. solutions using biometric information), introduction of new processing involving a lot of sensitive information or in case of processing involving extensive

assessment of personal matters, including profiling. A DPIA must also be prepared if existing risk assessments indicate a high risk.

If the DPIA shows that despite security measures, the risk of the data subjects is high, the Information Commissioners Office must be consulted before starting the processing.

For further information, contact the personal data responsible.

8. SECURITY OF PROCESSING

Cf. the information security policy, organisational and technical security measures have been implemented with a view to obtaining the required security.

These measures must e.g. protect personal data in relation to unauthorised access, illegal processing, disclosure, accidental loss, change or destruction. These measures shall apply, irrespective of whether the processing takes place electronically or in paper files.

The organisational and technical security measures constitute the management's requirements to data protection and will be revised continuously as technological possibilities change or there are organisational changes.

8.1. Security breach

In case of a security breach where personal data are disclosed by mistake or deleted by mistake, the Information Commissioners Office must be contacted within 72 hours. In such cases, the person data responsible must handle the dialogue with the Information Commissioners Office.

For more information, see the contingency plan with further instructions. If employees become aware of a security breach, the IT department must be contacted immediately.

9. SANCTIONS AND RESPONSIBILITIES

The senior management of Aarsleff Ground Engineering Ltd is responsible for personal data processing and is required to ensure that relevant legal requirements for data protection are met, just as they are responsible that the requirements of the personal data policy are met.

The senior management is responsible for ensuring that the adequate technical and organisational security measures are in place and that all departments comply with the protective measures.

Compliance with information security, personal data protection and the data protection act is controlled by means of regular audits. Audits are handled either by Aarsleff Ground Engineering Ltd IT Department or by an external collaboration partner.

Gross negligence of the data protection measures can result in fines or police inquiries. Violations of this policy for which an employee is responsible can lead to disciplinary proceedings or employment relationship sanctions.

10. COMPLAINTS TO THE DATA PROTECTION AGENCY

Data subjects of Aarsleff Ground Engineering Ltd can complain about the processing to the Information Commissioners Office.

Wycliffe House Water Lane
Wilmslow Cheshire SK9 5AF

Tel. 0303 123 113

11. DEFINITIONS

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 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.

Sensitive personal data: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, data concerning health and sexual orientation as well as genetic and biometric data.

Genetic data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which gives unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

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.

General personal data (non-exhaustive list): Name, address, telephone, e-mail, bank account etc.

National Insurance Number**:** Processing of National Insurance Numbers are regulated in accordance with paragraph 11, subsection 2 of the Data Protection Act which has the following content: Private individuals may process data concerning National Insurance Numbers where:

1) this follows from the law
2) the data subject has given consent in accordance with article 7 of the General Data Protection Regulation
3) the processing is carried out solely for scientific or statistical purposes or if it is a matter of disclosing a National Insurance Numbers where such disclosure is a natural element of the ordinary operation of enterprises etc. of the type in question and the disclosure is of decisive importance for unique identification of the data subject, or the disclosure is demanded by a public authority.

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.

Restriction of processing: Marking of stored personal data with the aim of limiting their processing in the future.

Profiling: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

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.

Filing system: Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.

Data controller: Any 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; where the purposes and means of such processing are determined by Union or Member State law, the data controller or the specific criteria for its nomination may be provided for by the Union or Member State law.

Data processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Recipient: A natural or legal person, public authority, agency or other body to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State low shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party: A natural or legal person, public authority, agency or body other than the data subject, the data controller, the data processor and persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

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 personal data relating to him or her.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

Supervisory authority: An independent public authority which is established by a Member State pursuant to Article 51. In England, the supervisory authority is the Information Commissioners Office.

Records of processing activities: Records of the IT systems where processing of personal data is involved. These records are found in the IT department.

Ebbe Malte Iversen
General Manager

Lars M. Carlsen
Deputy General Manager

Mogens Vedel Hestbæk
Group Chief Financial Officer

Jesper Kristian Jacobsen
Deputy General Manager

Revision Status	Date	Reason for change	Owner
2		Draft UK/ versions adopted in UK	H Jones
2a	May-22	Change of Responsible person page 4	R Hoe