Handling of personal data

When I work with personal data

- The work with personal data must take place in the relevant systems.
- I may not make local copies of personal data.
- I may only process the personal data I need for my task.

If I handle personal data

- When I send personal data to a colleague, the only requirement is that it must be work-relevant.
- If I send sensitive or confidential personal data out externally, it must be encrypted.
- If I send ordinary personal data out externally, it does not need to be encrypted.
- I should never send more information than absolutely necessary.

If I receive personal data

- If I receive more information than necessary, I must delete it.
- I must store all personal data in the relevant systems.
- I must remember to delete the CPR number and any other personal data if I need to respond or forward the inquiry.
- I must delete emails with personal data when I no longer have a work-related need for them.

Tips

- Always lock your computer (Windows key + L) when you leave your desk.
- Never store personal data on the local drive of your computer.
- Always make sure you have a valid purpose for processing personal data.
- Delete emails with personal data when you no longer have a purpose for keeping them.

Data breach

A data breach is a situation where unauthorised persons gain access to personal data or where personal data is lost.

Data breaches can happen as a result of accidents, human error, or malicious actions.

Among other things, data breaches can consist of personal data being disclosed knowingly or unknowingly to unauthorised persons, personal data being deleted or changed accidentally, unauthorised persons unlawfully gaining access to the data through e.g. hacking or your computer or phone being stolen.

However, the majority of data breaches happen as a result of everyday errors. Typically, an e-mail sent to the wrong recipient.

In certain situations, Solar is obliged to report the data breach to the Danish Data Protection Agency within 72 hours. It is, therefore, important that you as an employee, inform the GDPR team as soon as you have become aware of a possible data breach.

If you have any questions regarding data breaches or personal data, or if you are contacted regarding data subject rights, please send an email to GDPR@solar.dk.

You can report data breaches to the GDPR team via the QR code below.

solar

GDPR in Solar

General guidance

Solar A/S collects personal data as part of its daily operations.

This GDPR guide has been prepared in accordance with Solar Group's general GDPR policy, which governs all processing of personal data by Solar Group.

As an employee, you must know these guidelines and participate in relevant activities such as training and education.

This guide provides you with basic knowledge of the data protection rules within your field of work.

What is personal data?

There are three types of personal data:

There is general personal information, which is all general information about people such as name, address, telephone number, email and similar.

Then there is sensitive personal data, which is race, ethnic origin, political, religious or philosophical beliefs, trade union, genetic data, biometric data, health information or sexual orientation.

In Denmark, we also have a special category called confidential personal data. In this category is CPR number and other information that you generally do not want unauthorised persons to know. Confidential information must be treated in the same way as sensitive information.

Processing

Processing of personal data is everything you do with personal data. Be it collection, registration, sharing, deletion and storage.

You may only process personal data if there is a work-related need for it. This means, for example, that employee information may only be processed by the immediate manager, HR and the payroll office. In the same way, customer, course participant and supplier information may only be processed by those departments that have a work-related need for this.

Please note that the data protection rules apply to the processing of both electronic and physical documents containing personal data.

Rules

Principles and objectives
When processing personal data, the legislation imposes some general requirements.

- Information collection may only be for legitimate purposes
- The data may only be processed to the extent necessary for the purpose
- The information must be accurate and up to date
- The information may only be stored for as long as there is a legitimate purpose

Basis for processing (legal basis)
The General Data Protection Regulation sets out six possible legal bases for the processing of personal data. At least one of the six grounds must be present, for the processing of personal data to be legal.

- Consent
- Contract or agreement
- Legal obligation
- Vital interest
- Society's interest
- Legitimate interest

Data processors

In some situations, Solar entrusts others to process personal data on our behalf. These are referred to as data processors and include suppliers of IT services, course providers, external alarm companies, consultants or recruitment agencies.

In order for the data processors to process information on Solar's behalf, the two parties must enter into a data processing agreement. It is typically an independent document or part of a main contract with the supplier. A data processing agreement may not be signed without prior approval from the Group GDPR team.

The rights of the data subject

As a data subject, you have a number of rights under GDPR, which basically give the data subject insight into and control over how their own personal data is used by Solar.

If you as an employee receive an enquiry from a data subject, you must as a rule contact the Group GDPR team. If you are the 1st point of contact for a registered person , you are, however, allowed to make changes to the data subject's master data.