GDPR HANDBOOK FOR EMPLOYEES

How can I, as an employee, process personal data?

solar

TABLE OF CONTENTS

HISTORY

Version	Content	Approved by	Date
1.0	Document created	Mette Brix	01 May 2023

INTRODUCTION

Solar A/S (the "Company") collects information about natural persons ("personal data") as part of the Company's daily operations.

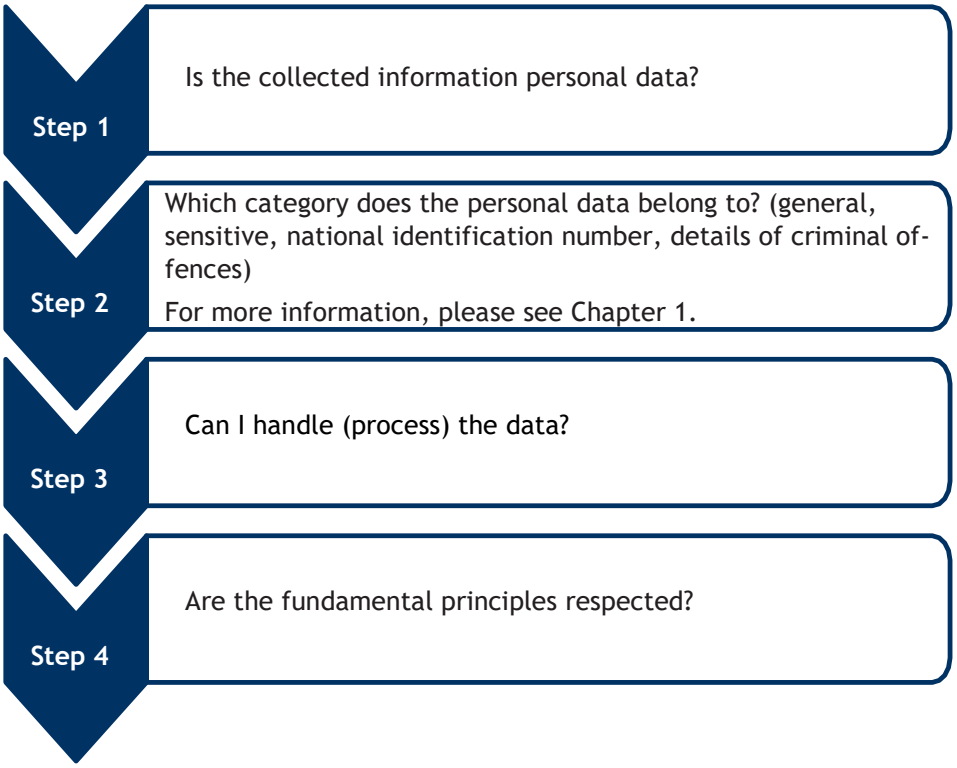
This GDPR employee handbook is based on the data processing in the Company's day-to-day operations. This may include personal data about customers, colleagues, business partners or suppliers, etc.

This GDPR employee handbook has been prepared in accordance with the Company's General GDPR Policy, which governs all processing of personal data carried out by the Company.

All employees who process personal data as part of their work must be familiar with these guidelines and the principles that apply to the processing of personal data. Therefore, employees must review these guidelines and participate in the activities (e.g., training and education) regarding protection of personal data established by the Company.

This GDPR employee handbook is designed to give you the necessary knowledge of data protection rules. It has been designed as a reference book where you quickly can find answers, advice, and guidance to questions regarding data protection you may encounter as part of your work.

When deciding as to whether you can lawfully process personal data, follow up this step-by-step guide:



In the GDPR employee handbook you will find the information you need to answer these questions.

PURPOSE

The data protection law applies regardless of whether the personal data is processed electronically or on paper.

All personal data processed by the Company must be collected and used in a lawful, fair and transparent manner and stored securely.

The company and you as an employee must work together to ensure that personal data is not disclosed to unauthorised persons.

You can only process personal data if there is a work-related need to do so. This means, for example, that employee data may only be processed by the immediate manager, HR and the payroll office. Similarly, customer, course participant and supplier data may only be processed by the departments that have a work-related need to do so.

If you are in doubt as to whether a collection or processing of personal data can be carried out, you must contact the GDPR Responsible for guidance and assistance prior to the collection or processing.

Contact details can be found here for your local GDPR Responsible:
https://solargroup.sharepoint.com/sites/sggdpr

CHAPTER 1

WHAT IS PERSONAL DATA?

1 WHAT IS PERSONAL DATA?

Personal data is any information that can be attributed to specific individuals.

This also includes information such as employee number, picture, etc. when it is possible to attribute the information to a specific natural person.

The rules of data protection law apply regardless of whether the personal data is processed electronically or on paper.

Personal data is any information that can be directly or indirectly attributed to a natural person. Personal data is categorised into four categories:

- General personal data
- Information on national identification number
- Information on criminal convictions and offences
- Sensitive personal data

Below are examples of personal data categorised into the four main categories (the list is not exhaustive).

GENERAL PERSONAL DATA	▪ Identification information
	  ▪ For example, name, address, telephone number, date of birth, e-mail address and pictures
	▪ marital status
	▪ Internal family relations
	▪ Economic conditions
	▪ Work, education and employment conditions
	  ▪ For example, education/training, position, work area and tasks, working hours, salary, tax information, sick leave, etc.

INFORMATION ON NATIONAL IDENTIFICATION NUMBER	▪ National ID number of an employee ▪ Date of birth is defined general personal data
INFORMATION ON CRIMINAL CONVICTIONS AND OFFENCES	▪ Information that an employee has committed (or has been reported to the police for) a criminal offence ▪ Information about a breach of the legislation, without triggering (or potentially triggering) actual criminal liability, but possibly other sanctions, e.g., disqualification ▪ Information on criminal record or child record ▪ Information on a clean criminal record is common information ▪ Information that a person has an address in a prison ▪ Information on offences and criminal convictions is confidential
SENSITIVE DATA	▪ Racial or ethnic origin ▪ Political, religious or philosophical beliefs ▪ Health information ▪ Trade union membership ▪ Sexual relations or sexual orientation ▪ Genetic and biometric data

CHAPTER 2

WHEN DOES THE PROCESSING OF PERSONAL DATA TAKE PLACE?

2 WHEN DOES THE PROCESSING OF PERSONAL DATA TAKE PLACE?

Processing of personal data includes any form of handling of personal data.

Processing can be, for example:

- Collection
- Registration
- Systematisation
- Storage
- Use
- Sharing
- Disclosure
- Archiving
- Deletion

The processing of personal data covers the entire life cycle. That is, all processing operations of personal data from the time they are collected until they are deleted by the Company.

The rules apply regardless of whether the personal data is processed electronically or on paper.

Personal data may only be processed if there is a legal basis for processing. You can read more about the different legal bases below in Chapter 3.

CHAPTER 3

LEGAL BASIS FOR PROCESSING

3 LEGAL BASIS FOR PROCESSING

Personal data may only be processed if there is a legal basis for processing. A legal basis is the basis on which the processing of personal data itself is authorised and lawful.

For example, if an employer wants to use photos of employees on the employer's website, the employer must have a legal basis to use the photos of the employees. In this case, the employer must obtain the employees' consent. The employer's legal basis for processing the employee's photo is therefore the employee's consent.

The type of personal data to which a piece of personal data belongs determines which processing bases you can use when deciding whether the processing of the personal data is authorised.

Attached to this handbook is a table in **Annex A** (Legal basis for processing) which summarises when it is lawful to process personal data according to the different categories.

For further information on the basis for processing see Annex A:

CHAPTER 4

BASIC PRINCIPLES FOR PROCESSING

4 BASIC PRINCIPLES FOR PROCESSING

Data protection law sets out eight basic processing principles that the Company must *always* comply with:

A	LEGALITY, FAIRNESS AND TRANSPARENCY	All personal data must be processed lawfully, fairly and in a transparent manner.
B	PURPOSE LIMITATION	When personal data is collected, it must be collected for specified, explicit and legitimate purposes. Personal data must not be further processed in a way incompatible with the original purpose.
C	DATA MINIMISATION	Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which the personal data are processed.
D	ACCURACY	Personal data must be accurate and, where necessary, kept up to date. Personal data must, as a general rule, be rectified or, where appropriate, erased if inaccurate.
E	STORAGE LIMITATION	Personal data must be kept for no longer than is necessary for the purposes for which they were collected. When the retention of personal data is no longer necessary for the fulfilment of the purpose, they must be erased or made anonymous.
F	INTEGRITY AND CONFIDENTIALITY	Personal data must be processed in a manner that protects personal data against unauthorised or unlawful processing, including access by persons other than those who have a work-related need to access personal data.
RESPONSIBILITY		In addition, data protection law is based on a principle of "accountability". This principle states that we as a company must be able to demonstrate that we comply with the processing principles and the data protection rules in general. We do this, among other things, by documenting that all employees follow and complete training in personal data protection, that we update our records, etc.
NO THIRD COUNTRY TRANSFERS		Personal data may not be transferred to countries outside the EU/EEA unless there is an instruction to do so, a legal basis for transfer and any additional measures to ensure that the country to which personal data is transferred also ensures an adequate level of personal data security.

CHAPTER 5

GENERAL GUIDELINES

5 GENERAL GUIDELINES

The company has established the following general guidelines for all employees:

- Information, including personal data, may only be accessed if it is necessary for the fulfilment of assigned and assigned tasks.
- Personal data may not be shared informally and with persons who do not have a work-related need to process the data.
- Data protection training must be followed and prioritised.
- Care must be taken in all situations to ensure the confidentiality of personal data - both in relation to colleagues and to external parties who are not authorised to receive the information.
- The local GDPR Responsible must be consulted in case of any doubt in relation to the processing of personal data.

Find the contact details of your local GDPR Responsible here: https://solargroup.sharepoint.com/sites/sggdpr

If your work requires IT systems/software other than those available, you must always obtain authorisation from **Contract Management** and **Information Security**. This is how we ensure data security in the Company. As a company, we are obliged to keep a record of processing of our systems and the related processing operations involving personal data.

CHAPTER 6

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

6 COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

COLLECTION OF PERSONAL DATA

You may only collect personal data when there is a defined purpose for the collection and the intended use. The purpose can be broadly formulated in relation to the performance of a task, but it must still be specific enough to be non-exhaustive.

It must always be assessed whether it is **relevant and necessary to** collect the individual personal data before it is collected. For example, when collecting customer data, if a new customer contacts you, etc. you may only collect the personal data necessary to establish the customer relationship. This means, for example, that as a seller you may collect the personal data on a customer that is necessary and relevant for the contract to be concluded. This could be the name, address, telephone number, bank details, etc. of the customer. This also means that you may not collect personal data on the customer that is not relevant for the conclusion of the contract. This could be sensitive information or information about criminal offences.

Before collecting personal data, the existence of a **legal basis for processing** must also be determined. Where consent is required, it must be obtained in writing and using the Company's consent forms.

For example, consent must be obtained before taking photos of employees or customers. At Solar, we have both internal and external consent forms to be used in these situations. Find our consent forms here: https://solargroup.sharepoint.com/sites/sgGDPR/SitePages/Documents.aspx.

When collecting personal data, the data subjects must be informed of how the Company processes their personal data. See further details in chapter 7.

If you have any doubts, please contact your local GDPR Responsible. Find the contact details of your local GDPR Responsible here: **https://solargroup.sharepoint.com/sites/sggdpr**.

USE OF PERSONAL DATA

The personal data collected and stored may only be used for the fulfilment of the purposes for which it was collected in the performance of your work.

This means, for example, that you cannot pass on the name and email address of a customer to another company unless you have the customer's consent.

In other words, personal data may not be used for **other purposes** than those for which the personal data was collected in the first place.

SHARING AND DISCLOSURE OF PERSONAL DATA

Sharing and disclosure of personal data is considered as a **separate processing operation**. This means that if you wish to share or disclose personal data to others, a separate and concrete assessment of the sharing/disclosure of personal data must be made. Before a sharing/disclosure takes place, it must therefore be ensured that it falls within the purposes for which the personal data has been collected and that there is a legal basis for the sharing or disclosure of personal data.

In certain situations, legislation requires the Company to disclose personal data to authorities. For example, when paying salaries, the Company is subject to legislation on reporting to tax authorities. In the case of typical disclosures of personal data to authorities as part of a regular and authorised routine by the immediate manager, you as an employee can disclose this personal data to the authority without further approval.

In case of disclosure of personal data to authorities in special or exceptional situations for which you have not received a request before or are in doubt, this must be authorised by your local GDPR Responsible before disclosure to the authority. In such cases, the Company must ensure that the request or requirement to disclose personal data is genuine and that the obligation for the Company is legitimised.

In case of doubt, always contact **your local GDPR Responsible** or the **GDPR Group Team** via gdpr@solar.dk before disclosing personal data.

CHAPTER 7

THE RIGHTS OF DATA SUBJECTS

7 THE RIGHTS OF DATA SUBJECTS

The GDPR gives data subjects a number of rights. Data subjects are the persons to whom the personal data processed relates.

As a data subject, you generally have the right to, among other things:

- To receive information that we are processing personal data of the data subject
- To know whether we process personal data about them and, if so, what data we process
- To obtain the rectification of inaccurate personal data, including the completion of the data so that it appears complete
- To have the personal data we process erased in certain situations
- To require us to restrict our processing activities
- To withdraw consent

If you as an employee receive a request from a data subject to exercise their rights, you must follow the Company's local workflows. Find the local workflows here: https://solargroup.sharepoint.com/sites/sgGDPR/SitePages/Documents.aspx.

If you are in doubt about the handling of the data subject's rights request, you must always contact your local GDPR Responsible. Find your local GDPR Responsible here: https://solargroup.sharepoint.com/sites/sggdpr.

In the privacy policy on the websites, the Company has informed the data subject about how the Company processes the data subject's personal data when visiting our websites.

For example, information on the processing of personal data by the Company is also provided in the following cases:

- In recruitment processes when we have received an application through our recruitment system
- In employment relationships, when the data subject is an employee, the privacy policy is provided together with the employment contract
- In the context of the data subject's enrolment as a course participant
- When the data subject visits our website
- Registration for newsletters and participation in competitions
- In connection with orders placed by customers via our website
- In connection with the start-up of cooperation with partners

CHAPTER 8

TRANSFER TO A THIRD COUNTRY

8 TRANSFER TO A THIRD COUNTRY

Specific rules in the data protection law apply to the transfer of personal data to a country outside the European Union (EU)/European Economic Area (EEA) (a "third country").

A transfer to a third country includes both the situation where personal data is physically moved, but also the situation where it is simply accessed from a location outside the EU (remote access).

Similarly, if there is a transfer of a data subject's personal data to a third country through the use of a processor, **Contract Management** and **Information Security** must be contacted to ensure that the third country transfer can be lawfully carried out.

Before initiating a transfer to a country outside the EU/EEA, you must **always** contact **Contract Management** and **Information Security to** determine whether there is a legal basis for the transfer and whether additional measures need to be taken.

CHAPTER 9

USE OF DATA PROCESSORS

9 USE OF DATA PROCESSORS

In some situations, the Company entrusts suppliers with the processing of personal data on behalf of the Company. In these situations, the supplier becomes the Company's data processor. This is primarily relevant for our IT use, as well as for individual business partners, including for use for HR/payroll processing, marketing, CRM system, sales, etc.

Data protection law requires us to use only processors who can provide the necessary guarantees that they will implement appropriate technical and organisational measures in such a way as to comply with data protection law.

The General Data Protection Regulation also stipulates that the Company must always have a written agreement with the data processor. The Company has a template for data processing agreements, which must be used when the Company enters into data processing agreements. This template contains a number of points that the Company must consider each time data processing agreements are entered into.

The Company continuously monitors the data processors, where the Company ensures that the data processors continue to fulfil the requirements that the Company imposes on them.

All data processors and their associated data processing agreements and controls must be registered in our contact system.

- The individual employee may not enter into agreements with anyone to perform tasks relating to the processing of personal data for the Company or enter into data processing agreements.
- All decisions to use data processors and enter into data processing agreements must be authorised by the Company's **Contract Management & Information Security** and in cooperation with **your local GDPR Responsible.**
- You must also not use IT solutions that are not authorised by **Contract Management & Information Security**. Failure to do so is a serious breach of the *General GDPR Policy*

CHAPTER 10

STORAGE AND ERASURE

10 STORAGE AND ERASURE

As a general rule, the Company may only keep personal data for as long as necessary to fulfil the purpose for which it was collected. This means that personal data must be erased again when it is no longer necessary to keep it in relation to your work-related purpose for collecting the personal data.

Please note that it **is only legal to** collect and store personal data that is necessary for the fulfilment of your work task.

If personal data is found to be inaccurate or unnecessary for the purpose, you must delete or rectify the personal data.

Personal data must be stored securely. This means that documents and other material containing personal data may only be stored in the processing systems designated by the Company, e.g., CRM system, ERP system and HRM system, but not on USB sticks, etc.

EMPLOYEE DATA

Personal data about you as an employee are collected for personnel administration purposes and are kept throughout your period of employment. After your resignation, employee data is retained after the end of the employment relationship in accordance with the locally applicable rules.

CUSTOMER INFORMATION

Customer information is collected for the purpose of processing orders etc. from customers and the information is stored as long as there is an active customer relationship. Information about invoicing is stored in accordance with the locally applicable rules.

STUDENT INFORMATION

The company collects and stores personal data on learners. The personal data is kept until after the end of the programme. After that, personal data is deleted in accordance with local applicable accounting rules.

INFORMATION ON PARTNERS AND SUPPLIERS

Information on business partners and suppliers can be categorised into two sub-categories:

1) Company information such as name of the company, finances, address, etc.
2) Personal data of the employees working in the organisation such as name, email, phone number, etc.

As a general rule, business data can be collected and stored for as long as desired and necessary for the Company. Company data is not covered by the rules of data protection law. It only applies to natural persons.

However, information about natural persons from the company/business partner, such as a contact person at a company, is personal data and subject to the rules of data protection law. This means that personal data (about the contact person in question) must be deleted when it is no longer necessary to keep it in order to fulfil the purpose for which it was collected.

For example, if the person is no longer employed by the co-operation partner/supplier, or when it is no longer necessary for the Company to store the personal data due to the end of the co-operation.

PHYSICAL DOCUMENTS

At the Company, all employees are encouraged to avoid receiving physical documents and to receive them digitally.

If you receive the documents physically, such as CVs, applications, etc., the documents must be scanned and stored in the relevant system, unless there is no need to store the documents. The physical documents must then be shredded. If there is no need to store the documents, the documents must also be shredded and not scanned.

If, exceptionally, you have physical documents that are not scanned, these must be kept in a physical archive with an indication of the content and year. In addition, personal data must be stored in a secure place, i.e., in such a way that persons - internal or external - who are not authorised to see the personal data cannot have immediate access to them, for example in a locked cabinet or drawer. When the documents no longer need to be stored, they must be shredded.

PROCESSING MAILS IN OUTLOOK

The company uses Outlook to process e-mails.

Outlook is intended to support correspondence and the Outlook inbox must not be used for storage.

All employees must create sub-folders in Outlook to file emails containing personal data relating to customers, trainees, suppliers and private matters. These subfolders must be

named to ensure that only necessary personal data is stored.

All emails that are not logged in a subfolder (including inbox, trash, attachments, sent mail and archived files) containing personal data must be deleted every 6 months after receipt/sending.

Personal data defined as sensitive or confidential must not be stored in the Outlook inbox and must therefore be deleted or logged immediately upon receipt.

Private mails must be transferred to a sub-folder named "Private Folder" when it concerns matters of a private nature that are not relevant to the Company. No personal data of a confidential or sensitive nature may be stored in the "Private Folder".

What is contained in the Private Folder is of no concern to the Company and the employee is responsible for ensuring that the personal data can be stored lawfully.

Note: The employee must not use the Private Folder for confidential or sensitive content of a private nature, as the Company retains the right to monitor that the Private Folder is not used for purposes other than those specified.

Note: The employee may be selected for internal control, where the Company will have access to the contents of the file.

Note: Content from the Private folder may become known to the Company when the Company performs cross-searches across all Outlook accounts.

CHAPTER 11

PERSONAL DATA BREACH

11 PERSONAL DATA BREACH

A personal data breach occurs when a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

You must **immediately** contact the **Group Service Desk "GSD"** if you become aware of or suspect a personal data breach.

A personal data breach may, for example, technically occur when the Company's IT systems containing personal data are not sufficiently secured so that outsiders gain access to the personal data (e.g., hacking). It may also be the Company's own handling of the personal data that can cause a breach, for example if an employee discloses or changes personal data without authorisation or sends an email to the wrong person.

In the event of a personal data breach requiring notification to the competent supervisory authority, such notification must be made within 72 hours of the breach becoming known. Notification is not required if it is unlikely that the breach has resulted in a risk to the rights of a natural person. This assessment is made by **the local GDPR Responsible** and the **GDPR Group TEAM,** therefore an email must be sent to GDPR@solar.dk in English.

You must **immediately** contact the **Group Service Desk "GSD"** if you become aware of or suspect a personal data breach.

Please call the telephone number: +45 79300155

Afterwards, you must then contact your local GDPR Responsible and send an email to the **GDPR Group TEAM** via GDPR@solar.dk in English.

You can read more about what to do as an employee in the event of a *personal* data *breach* in the Company's *GDPR Guidelines for personal data breach* and *Contingency plan for personal data breach*

CHAPTER 12

INFRINGEMENT, SANCTIONS AND DEVIATIONS

12 INFRINGEMENT, SANCTIONS AND DEVIATIONS

VIOLATION

As an employee of the Company, you are obliged to comply with the *General GDPR Policy* as amended from time to time, with related guidelines and procedure descriptions including this GDPR handbook for employees.

Find the *General GDPR Policy*, with related guidelines and procedure descriptions here: **https://solargroup.sharepoint.com/sites/sggdpr**.

SANCTIONING

The local GDPR Responsible ensures compliance with the guidelines and procedures. If you as an employee breach the applicable guidelines and procedures for the processing of personal data, you may be subject to employment law consequences.

DEVIATIONS, EXCEPTIONS AND IRREGULARITIES

The local GDPR Responsible must be contacted to request a derogation from the rules if situations arise where the requirements of the guidelines and procedures cannot be met.

No deviation may be made until written authorisation has been obtained from the local GDPR Responsible.

All questions about the processing of personal data must be addressed to **your local GDPR Responsible**.

If it is suspected that the Company or one or more employees are not complying with the procedures and guidelines, the **GDPR Group Team** must be contacted immediately.

ANNEX A – LEGAL BASIS FOR PROCESSING

TABLE 3.1 – LEGAL BASES FOR PROCESSING GENERAL PERSONAL DATA

TABLE 3.2 – LEGAL BASES FOR PROCESSING SENSITIVE PERSONAL DATA

TABLE 3.3 – LEGAL BASES FOR PROCESSING FOR NATIONAL IDENTIFICATION NUMBER

TABLE 3.4 - LEGAL BASES FOR PROCESSING CRIMINAL CONVICTIONS AND OFFENCES

The following tables provide an overview of when it is lawful to process personal data.

The tables show the legal bases for processing for the four main categories of personal data.

3.1 LEGAL BASIS FOR PROCESSING NON-SENSITIVE PERSONAL DATA	
Legal basis for processing	Scope (non-exhaustive)
Consent. Article 6(1)(a) of the GDPR.	Personal data must only be processed on the basis of consent if the other legal bases cannot be used. Consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes" by which the data subject confirms that personal data relating to him or her are processed.
Performance of a contract to which the data subject is a party. Article 6(1)(b) of the GDPR.	For example, processing personal data about the Company's customers. Can only be used when the data subject is a party to the contract.
Measures taken at the request of the data subject prior to the conclusion of a contract. Article 6(1)(b) of the GDPR.	For example, the processing of personal data by the employer during the recruitment process.
Compliance with a legal obligation incumbent on the controller. Article 6(1)(c) of the GDPR.	Processing necessary to comply with legislation, e.g., reporting of employees' salaries to tax authorities, reporting work injuries to National Board of Industrial Injuries etc.
Protect the vital interests of the data subject or other natural person. Article 6(1)(d) of the GDPR.	The processing must relate to interests which are of fundamental importance for the data subject. For example, if the person is incapable, due to illness, of consenting to the processing of personal data which would ensure the person against suffering substantial economic loss or damage.
Performing a task in the public interest. Article 6(1)(e) of the GDPR.	Includes tasks of general interest, i.e., tasks that are of importance to a wider range of people.
The exercise of official authority vested in the controller. Article 6(1)(e) of the GDPR.	This rule is primarily aimed at the processing of personal data by public authorities in the exercise of official authority.
Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests of the data subject. Article 6(1)(f) of the GDPR.	Processing may take place when the interests of the data controller - after a specific balancing exercise - override the interest of the data subject in the non-processing. The balancing exercise must be made on the basis of the specific circumstances of each case.

3.2 LEGAL BASIS FOR PROCESSING SENSITIVE PERSONAL DATA	
Legal basis for processing	Scope (non-exhaustive)
Consent. Article 9(2)(a) of the GDPR	If the person has given his or her consent to the processing of sensitive personal data relating to him or her. The consent must fulfil the same requirements as consent to process general personal data.
Processing is necessary for compliance with the controller's or data subject's obligations under employment, social security and social protection law. Article 9(2)(b) of the GDPR	For example, legislation or collective agreements may lay down specific rules on the processing of workers' personal data in employment relationships.
Protect the vital interests of the data subject or other natural person. Article 9(2)(c) of the GDPR	The processing must relate to interests which are of fundamental importance for the data subject. Can only be used in cases where the data subject is physically or legally incapable of giving consent.
Processing by a body with a political, philosophical, religious or trade union aim. Article 9(2)(d) of the GDPR	For example, a trade union may, in the course of its activities, process personal data of its members and former members and employees under the scope of the collective agreement, where the processing is carried out in the course of the trade union's work as a trade union organisation.
Personal data which are manifestly made public by the data subject. Article 9(2)(e) of the GDPR	If the personal data has been made known to a wider circle of people, for example on social media such as Facebook, Twitter and YouTube. The personal data must have been made public on the person's own initiative. Personal data published about the person by others on their own initiative is not covered.
Processing is necessary for the establishment, exercise or defence of legal claims. Article 9(2)(f) of the GDPR	The provision covers processing in the interest of the controller, the data subject and third parties. The provision covers processing in the context of judicial, administrative and extra-judicial procedures.
Processing is necessary for reasons of substantial public interest. Article 9(2)(g) of the GDPR	The processing must be carried out for reasons of substantial public interest and must be authorised by law.
Processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of social and health care or processing or the management of social and health care and services on the basis of law or a contract with a health professional subject to professional secrecy. Article 9(2)(h) of the GDPR	Usually used by public authorities, medical professionals, etc. The processing must be authorised by law, or a contract must be concluded with a professional subject to professional secrecy.
Processing is necessary for reasons of public interest in the area of public health. Article 9(2)(i) of the GDPR	The provision includes, inter alia, protecting against serious cross-border health risks or ensuring high quality standards for healthcare and medicines or medical devices. The processing must be authorised by law.
Processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes. Article 9(2)(j) of the GDPR	Includes only research or statistical purposes. The processing must be authorised by law.

3.3 LEGAL BASIS FOR PROCESSING NATIONAL IDENTIFICATION NUMBER	
Legal basis for processing	Scope of application (non-exhaustive)
Legal basis. Under national law.	Where it follows from the law that the controller has the right to process information on national identification numbers. For example, when reporting various income-related information to tax authorities.
Consent. Under national law.	If the person has given his or her consent to the processing of data relating to his or her national identification number. The consent must fulfil the same requirements as a consent to processing general personal data.
For statistical or scientific purposes. In accordance with national law.	Processing of national identification numbers for the purpose of statistical or scientific studies.
Disclosure of information on national identification number. According to national law.	Information on national identification numbers may be disclosed when the disclosure: - is a natural part of the normal operation of undertakings, etc. of the nature in question, and - when the disclosure is essential to ensure the unique identification of the data subject, or - the disclosure is required by a public authority. If name and date of birth are sufficient identification, the national identification number may not be disclosed.

3.4 LEGAL BASIS FOR PROCESSING CRIMINAL CONVICTIONS AND OFFENCES	
Legal basis for processing	Scope of application (non-exhaustive)
Legal basis. Article 10 of the General Data Protection Regulation.	If it follows from the law that the controller has the right to process personal data relating to criminal convictions and offences. For example, in the context of obtaining statutory child certificates.