Data Protection Policy

Internal guide for data protection compliance

1. Introduction

1. When JYSK collects and uses personal data about its employees, customers, vendors, business contacts or other third parties, JYSK is responsible for ensuring that the personal data is processed in a secure and orderly manner and that such processing complies with applicable data protection laws

2. As an employee of JYSK you must read and comply with this policy. Any breach of this policy may have severe consequences for JYSK, both economically and with respect to how JYSK is perceived publicly.

3. This policy is structured as follows:

    - An explanation as to what is personal data (section 2)
    - The overall principles which you must know and follow when processing personal data (section 3); and
    - Contact information for whom in JYSK you may contact if you have any questions in relation to processing of personal data (section 4).

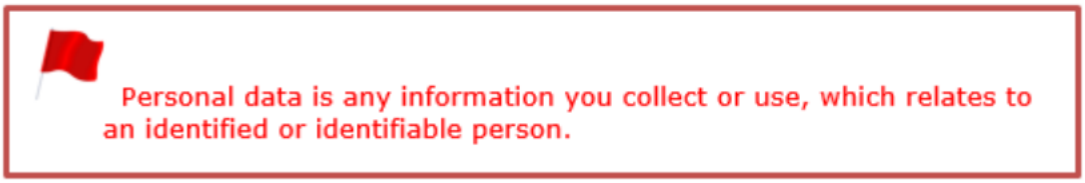
Red flags are used to highlight situations where you must be careful or aware of specific obligations when processing personal data.

---

2. What is Personal Data?

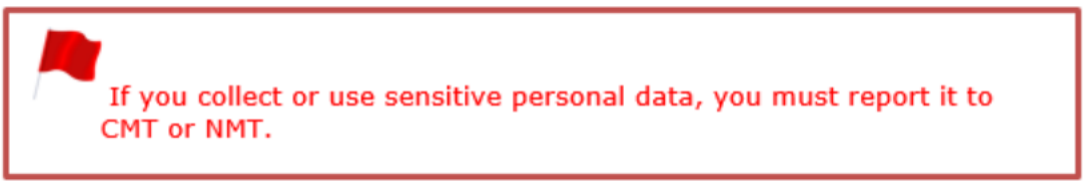
1. Personal data is *any information relating to an identified or identifiable natural person* (i.e. the 'data subject').

2. Personal data is as an example the. name, address, phone number, e-mail, employee id, criminal records, health information (e.g. allergies), food preferences, personality tests, religious believes, bank account details, IP address etc. Basically any data you collect or use which in any way relates to a physical person is personal data.



3. Sensitive Personal Data:
   Even though all types of personal data must be processed in accordance with the principles below, some categories of personal data demand extra attention. This is called *Sensitive Personal Data.* Sensitive Personal Data concerns personal data regarding: *racial or ethnic origin*, *political opinions*, *religious or philosophical beliefs*, *trade union membership*, *genetic data*, *biometric data*, *health data*, *a person's sex life or sexual orientation*, and *criminal convictions and offences*.

   JYSK will to the extent possible not be processing any sensitive personal data. However, if sensitive personal data need to be processed, any collection or use hereof must be reported to CMT or NMT and any instructions given by the data protection manager must be followed.



---

3. Principles for processing any personal data

1. Good practices for the processing of data

   When you collect or use any personal data you must ensure that this happens in a secure and orderly manner. The integrity and individual rights of the data subjects must be protected. In relation to the general principle of fairness, you are not allowed to process data in a wider scope than what the purpose dictates.

2. Documentation of the processing of personal data

JYSK is responsible for and shall be able to demonstrate compliance with data protection legislation.
It is therefore necessary that you keep documentation of the use of personal data processed in JYSK and ensure such is up to date at all times. When you process personal data as part of a new process, new project or with a new purpose, you must report this to the data protection manager using the relevant templates.

When you collect personal data for a new purpose or making new deletion routines, you must inform the data protection manager

3. Only process for a specific purpose

Personal data may only be collected for specified, explicit and legitimate purposes.
Any further processing of personal data must not be incompatible with the purposes for which the data was originally collected. If you need to use data for other purposes than the data was collected, you must provide information as mentioned under section 3.5 to the data subjects.

You must not use personal data for other purposes than the data was originally collected for.

4. Any processing requires a legal basis

You may only use personal data if the reason you are using the data is covered by one or more of the legal grounds set out in the applicable data protection laws. Processing of personal data (which are not sensitive) will within the EU/EEA be legal if:

- the data subject has given explicit consent; or
- processing is necessary for the performance of a contract to which the data subject is party; or
- processing is necessary for the purposes of the legitimate interests pursued by JYSK and these interests are not

overridden by the interests of the data subject.

When using personal data, you must ensure that the use is covered by a legal ground.

5. Information of the data subject

   When you collect personal data from a data subject (e.g. contact information of a customer) or you receive personal data from a third party, you must provide specific information to the data subject. Such information must fulfil the requirements under the EU GDPR. To ensure this, you must consult the data protection manager who will provide you with an overview of which information you must provide the data subject.

When you collect personal data, you must consult the data protection manager to ensure you provide the data subject with the required information.

6. Contract if data processing by a third party

   If a vendor or other third party is processing personal data on behalf of JYSK (e.g. cloud service providers or recruitment agencies), such processing must be governed by a written data processing agreement.

   Before you enter into a contract with a new vendor, you must always assess if the vendor will be processing personal data under the contract. If this is the case you must consult the data protection responsible to ensure a written data processing agreement is in place. JYSK is using a specific template that shall be agreed with all third party data processors unless otherwise is approved by data protection manager

If a vendor is processing personal data on behalf of JYSK, a written data processing agreement must be in place between JYSK and the vendor.

7. Transfer of data

   Personal data may only be shared between group entities and with any third party if it has been assessed that such disclosure of personal data is in accordance with applicable law.

   Any transfer of personal data between an entity established within the EU/EEA and an entity or a third party established outside the EU/EEA, e.g. UA, may not take place without the approval of data protection manager.

Personal data processed within the EU/EEA may not be transferred to a country outside the EU/EEA without the approval of the data protection manager

8. Deletion
   Personal data may only be stored and used for as long as it is necessary for the purposes for which the personal data are collected.

   When you collect personal data, it must be assessed for how long the individual must be identified for the data to fulfil the defined purpose. After this period the data must be deleted or anonymized.

   It is important that you at least annually check if you are storing any personal data which are no longer necessary for the purpose for which the data was collected. Such data must be deleted immediately.

You must delete personal data when its use is no longer necessary.

9. Accurate and updated

   If you discover or are informed that the personal data you are using is not correct or up to date, you have an obligation to correct this. JYSK may not process inaccurate information.

10. Confidentiality and security Any personal data that you process is regarded as confidential information. This means:
    - You may only use the data for the purpose for which it was collected;
    - You may not share or otherwise disclose the data to another employee, vendor or other third party unless such person has a need to know; and
    - You must ensure that all reasonable precautions are taken to ensure that the data is treated as confidential and not disclosed or used unintentionally.

Personal data is confidential information and must be treated as such.

11. Breach of security

    In the event you identify that the security of the processing of personal data has been compromised or is likely to be compromised, or there in any other way has been an unauthorised or accidental disclosure of or access to personal data, you must immediately notify the data protection manager.

    You must never take independent actions, but shall instead await instructions from the data protection manager, who lead the investigation.

    For more information about how JYSK handles security breaches, see JYSK's Data Protection Breach Policy

In the event of a security breach, you must immediately notify JYSK's data protection manager.

4. Contact persons

Risk & Fraud Controller, Data Protection Manager. Finance Nordic.