Data Privacy Policy Model

COPENHAGEN COMPLIANCE

The Data Privacy Policy Model is an example document that should be adapted to suit your circumstances and not used as a one-size-fits-all policy.

Introduction
The organisation is committed to all aspects of data protection and takes its duties, and the duties of its employees, under the General Data Protection Regulation seriously. This policy sets out how the organisation deals with personal data, including personnel files and data subject access requests, and employees' obligations about personal data.

Data protection officer
[Name of individual] is the organisation's data protection officer and is responsible for the implementation of this policy. If employees have any questions about data protection in general, this policy or their obligations under it, they should direct them to [name of individual], contactable on [contact details].]

Data protection principles
The General Data Protection Regulation requires that specific data protection principles be followed in the handling of personal data. These principles require that personal data must:

- be accurate;
- be secure;
- not be kept longer than is necessary;
- be adequate, relevant and not excessive;
- be fair, lawfully and transparently processed;
- be treated with individuals' rights;
- be processed for limited purposes and not in any manner incompatible with those purposes;
- and not be transferred to countries without adequate protection.

"Personal data."
The General Data Protection Regulation applies only to information that constitutes "personal data". Information is "personal data" if it:

- identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and
- is a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as it's focus or is otherwise biographical.

Consequently, automated and computerised personal information about employees held by employers is covered by the Regulation. Personal information stored physically (for example, on paper) and contained in any "relevant filing system" is also included. Also, information recorded

with the intention that it will be stored in an appropriate filing system or held on the computer is covered.

A "relevant filing system" means a well-structured manual system that amounts to more than a bundle of documents about each employee filed in date order, i.e. a system to guide a searcher to where specific information about a named employee can be located quickly.

The use of personal information
The General Data Protection Regulation applies to personal information that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it.

"Sensitive personal data."
"Sensitive personal data" is information about an individual's:

- racial or ethnic origin;
- political opinions;
- sex life;
- physical or mental health or condition;
- religious beliefs or other beliefs of a similar nature;
- commission or alleged commission of any criminal offence; and
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.
- biometric;
- generic;
- trade union membership;

The organisation will not retain sensitive personal data without the express consent of the employee in question.

The organisation will process sensitive personal data, including sickness and injury records and references, by the eight data protection principles. If the corporation enters into discussions about a merger or acquisition with a third party, the agency will seek to protect employees' data by the data protection principles.

Personnel files
An employee's personnel file is likely to contain information about his/her work history with the organisation and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance data and personal information about the employee including address details and national insurance number.
There may also be other information about the employee located within the organisation, for example in his/her line manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.

The organisation may collect relevant sensitive personal information from employees for equal opportunities monitoring purposes. Where such information is collected, the organisation will anonymise it unless the purpose to which the information is put requires the full use of the

individual's personal information. If the information is to be used, the organization will inform employees on any monitoring questionnaire of the use to which the data will be put, the individuals

or posts within the organization who will have access to that information and the security measures that the organization will put in place to ensure that there is no unauthorized access to it.

The organisation will ensure that personal information about an employee, including information in personnel files, is securely retained. The organisation will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls, and passwords and encryption software will be used where necessary.

The organisation provides [compulsory] training on data protection issues to all employees who handle personal information in the course of their duties at work. The organisation will continue to provide such employees with refresher training on a regular basis. Such employees are also required to have confidentiality clauses in their contracts of employment.

Where laptops are taken off site, employees must follow the organisation's relevant policies relating to the security of information and the use of computers for working at home/bringing your device to work.

Employees' obligations regarding personal information

If an employee acquires any personal information in the course of his/her duties, he/she must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so;
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.

In particular, an employee should ensure that he/she:

- uses password-protected & encrypted software for the transmission and receipt of emails;
- sends fax transmissions to a direct fax where possible and with a secure cover sheet; and
- locks files in a secure cabinet.

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an employee acquires any personal information in error by whatever means, he/she shall inform [name of individual/the data protection officer] immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within the organisation.

Where an employee is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact [name of individual/line manager/the data protection officer].

An employee must not take any personal information away from the organisation's premises [save in circumstances where he/she has obtained the prior consent of [the data protection officer/senior management] to do so].

If an employee is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from [name of individual/line manager/the data protection officer]. If he/she cannot get in touch with [name of individual/line manager/the data protection officer], he/she should not disclose the information concerned.

Data subject access requests

The organisation will inform each employee of:

- the types of information that it keeps about him/her;
- the purpose for which it is used; and
- the types of organisation that it may be passed to unless this is self-evident (for example, it may be self-evident that an employee's national insurance number is given to ……).

An employee has the right to access information kept about him/her by the organisation, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee.

[Name of individual/The data protection officer] is responsible for dealing with data subject access requests.

The organization [will charge [amount up to DKK X00]/will, not charge] for allowing employees access to information about them. The organisation will respond to any data subject access request within 30 calendar days.

The organisation will allow the employee access to hard copies of any personal information. However, if this involves a disproportionate effort on the part of the organisation, the employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by the organisation.

The organisation may reserve its right to withhold the employee's right to access data where any statutory exemptions apply.

Correction, updating and deletion of data
The organisation has a system in place that enables employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an employee becomes aware that the organisation holds any inaccurate, irrelevant or out-of-date information about him/her, he/she must notify [name of individual/the data protection officer/the HR department] immediately and provide any necessary corrections and/or updates to the information.

Data that is likely to cause substantial damage or distress
If an employee believes that the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person, he/she may notify the organization in writing to [name of individual/the data protection officer] to request the organization to put a stop to the processing of that information.

Within 21 days of receiving the employee's notice, the organisation will reply to the employee stating either:

- that it has complied with or intends to comply with the request; or
- the reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

Monitoring
The organisation may monitor employees by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, the organisation will inform the employee that monitoring/surveillance is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about him/her. The organisation will not retain such data for any longer than is necessary.

In exceptional circumstances, the organization may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the organisation by the activity being monitored and where the information cannot be obtained efficiently by any non-intrusive means (for example, where an employee is suspected of stealing property belonging to the organisation). Covert monitoring will take place only with the approval of [name of individual/senior management/the data protection officer].

[**Taking employment records off site**]
An employee must not take employment records off site (whether in electronic or paper format) without prior authorisation from [name of individual/the data protection officer/senior management].

An employee may take only certain employment records off site. These are documents relating to [disciplinary or grievance meetings that cannot be held on site/meetings with occupational health/discussions surrounding the sale of the business or specific monitoring purposes/seeking

professional advice]. An employee may also take employment records off site for any other valid reason given by [name of individual/the data protection officer/senior management].

Any employee taking records off site must ensure that he/she does not leave his/her laptop, other device or any hard copies of employment records on the train, in the car or any other public place.

He/she must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.]

Review of procedures and training

The organisation will provide training to all employees on data protection matters on induction and a regular basis after that. If an employee considers that he/she would benefit from refresher training, he/she should contact [name of individual].

The organisation will review and ensure compliance with this policy at regular intervals.

Consequences of non-compliance

All employees are under an obligation to ensure that they have regard to the eight data protection principles (see above) when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the organization will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.