Title	Version	Replaces	Org. location	Page # (of #)
Guidelines for Data Protection	1.2	1.1	N/A	1(7)

Owner	Changed by	Latest changed	Document type
General Counsel	Amelia Wallace	2024-03-12	Guidelines

Adopted by	Adopted on (Date)	Status	Replaced by
CEO	2024-04-10	Adopted	N/A

Guidelines for Protection of Personal Data

Background

What does this guideline include?

This Guideline complements Hemnet's *Policy for Information and Data*, which expresses the intentions and rules that apply to the use and protection of information, information systems and data (including personal data) on Hemnet. The Policy states that we shall conduct our business in a manner that ensures that we protect and handle our data including personal data in accordance with applicable data protection legislation (referring to the GDPR and Swedish legislation that complements the GDPR) and the reasonable expectations of our stakeholders. This document constitutes Hemnet's guidelines for protection of personal data and describes what Hemnet must do to achieve this.

Detailed instructions and procedures may supplement these Guidelines where appropriate.

Publication on hemnet.se and related personal data processing falls under the scope of Hemnet's publication license (*Sw*. “utgivningsbevis”) and is not subject to these guidelines in its entirety (see below under “Publication License”).

Who is affected by this guideline?

All employees and consultants at Hemnet.

Why did we create this guideline?

To clarify what we at Hemnet need to do to achieve the goals set with regard to protection of personal data in the *Policy for Information and Data*.

Information

Overall structure for governance

Hemnet shall have a structured working method for compliance with regulations, whereby Hemnet's Legal has the overall responsibility and shall ensure that Hemnet can show reasonable proof of compliance in accordance with the principles of accountability in the GDPR. The operational elements of the work with protection of personal data are handled in accordance with the Target Operating Model for data protection as updated from time to time, in which particularly Legal, Infosec Officer, system owners and managers have important roles. Legal is the owner of the Target Operating Model, which is continuously updated to ensure that measures and resources at all times are adequate.

Hemnet shall strive for protection of personal data to be an integral part of the business and a natural part of our business culture.

Some key concepts in protection of personal data

What is personal data?
All information that directly or indirectly (together with other information) can identify a living person is considered personal data. The definition is wide and much of what at first glance may not appear to be personal data can actually per definition be personal data, and is then covered by data protection legislation.

What is meant by the processing of personal data?
Any form of handling of personal data is referred to in data protection legislation as "processing": collection, transfer, sharing, analysis, storage, back-ups, processing etc. A processing activity can be that you collect information via a Google form and then save a Google Sheet with a list of names with e-mail addresses, or that you at a later stage use the list as a basis for sending out emails. Even completely passive storage of personal data is "personal data processing".

Who is the Data Controller?
When we collect and process personal data on our own behalf and for our own purposes, Hemnet as a company is the "Data Controller". With that role comes a large number of obligations under the data protection legislation that aim to protect the persons whose personal data we process from having their personal privacy violated.

What is a Data Processor?
Anyone who processes personal data without having their own purpose with the processing, but only follows the instructions of the data controller, is referred to in data protection legislation as a "data processor". In Hemnet's context most of our suppliers are data processors.

What is meant by accountability?
Under the data protection legislation, we are obliged to be able to show that we meet all legal requirements. This in turn requires that we not only do the right thing, but also that we need to be able to show through documentation, agreements and system logic, that we comply with the law.

Lawfulness and basic principles

Ensuring lawfulness
The principles listed below are the backbone of all work with data protection. All processing of personal data must be assessed against the basic principles listed below. The business should receive relevant support to make such assessments, and can always turn to Legal for advice.

Basic principles for lawful processing
At Hemnet, we shall observe the following principles for personal data processing:

- Purpose limitation - *Personal data may only be processed for specific, explicit and legitimate purposes.*
- Lawfulness, Accuracy and Transparency - All *processing must have a legal basis (see below) and be fair and transparent in relation to the individuals concerned. Personal data that we process must be correct and, where necessary, kept up to date. To the extent personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

- Storage limitation - *Personal data must not be stored longer than necessary for the purpose.*
- Data minimisation - *Personal data must be adequate, relevant and limited to what is necessary with regard to the purpose.*
- Integrity and Confidentiality - *Personal data shall be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.*

Legal basis

In order for the processing of personal data to be compliant with data protection legislation, all processing must have a legal basis. There are several different legal bases. These are set forth in the data protection legislation. For Hemnet, there are mainly the following four legal bases that we can rely on:

Legitimate interest

This is the most common legal basis for our processing of personal data: our legitimate interest in processing the relevant personal data outweighs the risks that it may entail from an integrity perspective, for the individuals it affects. Relying on legitimate interest as a legal basis also assumes that we feel confident that the processing in question is within the reasonable expectations of the individuals concerned. In this case, we do not ask for approval before, but allow a person to say no ("opt-out") in cases where the individual has the right under applicable data protection legislation to object to such processing.
It can, for example, be the case when we are saving information about customers in a CRM system or sending out a user survey to those who have chosen to use a certain function on hemnet.se.

Legal obligation

If we need to process personal data in order to be able to meet obligations in other legislation, we can do so with reference to the fact that it is necessary for the fulfillment of a legal obligation.
An example is the Accounting Act, which requires that certain documents need to be archived and saved for a period of seven years.

Fulfillment of contracts

The processing of data which is necessary to be able to fulfill obligations under a contract can normally rely on this legal basis ("fulfillment of contracts"). An employment contract is an example of such a contract. Hemnet will process a number of personal data about its employees in order to fulfill its part of the contract, such as to pay salary.

Consent

Consent as a legal basis shall be used to a limited extent and only to the extent that we do not see that legitimate interest can be used as legal basis. Also, consent shall not be relied upon when there is a position of dependency between the data subject and the controller, which is common for example in relation to employees. A consent must be based on correct, clear and complete information; such as what personal data is collected and for what purposes. A consent can be revoked at any time, and then we must stop the processing activity.

Transparency

Hemnet must ensure that personal data processing is transparent to the various groups of individuals affected by it: employees and candidates, visitors to Hemnet's channels, brokers and consumers. For each such group of individuals, there must be relevant and easily accessible information about

Hemnet's processing. Such information can be presented in the form of personal data policies or similar documents and must meet the requirements of data protection legislation.

Sensitive personal data

Sensitive personal data (as defined in the applicable data protection legislation) shall only be processed after particularly careful consideration and with the assurance that explicit consent or other applicable legal ground exists for such processing.

Exceptions from the data protection legislation in the context of publication at hemnet.se

Hemnet has a publication license which means that published information in Hemnet's channels is subject to the same constitutional protection for freedom of expression as radio, TV and newspapers have. This means, among other things, that the data protection legislation, to a large extent, is not applicable to personal data processing in connection with publication in Hemnet's channels where the freedom of expression is instead applicable. However, the requirements relating to relevant security measures and reporting in certain cases of personal data incidents also apply to these parts of the business. Personal data processing that follows the collection of data through cookies and similar technologies in Hemnet's channels is generally not covered by the exception.

Processing register (List of personal data processing)

Hemnet must have an up to date processing register of the personal data processing that takes place in the business and which falls under the data protection legislation. The register must also contain principles for retention and information on legal basis. There must be relevant routines to ensure that the processing register is kept up to date.

Rights of the data subjects

Anyone who is subject to the processing of personal data (referred to in the data protection legislation as the "data subject") has a number of rights that we are obliged to respect. There must be relevant routines to ensure that issues relating to the exercise of rights are handled correctly by employees with relevant knowledge and that our support has clear routines for who they contact when questions of this nature come in. The rights that are primarily relevant to Hemnet's operations are the following:

- Right to information and access
- Right to rectification
- Right to deletion (to be forgotten)

The right to information and access is about receiving information of the processing in accordance with the data protection legislation and being able to turn to us at Hemnet and find out what information we process about the person in question. This applies to both users of our service and you as an employee with Hemnet as an employer. The right to information also applies in that sense that the data subject must be informed about what data is collected when collecting the data, the purpose of the processing and how long we will save them. (See above under "*Transparency*")

The right to rectification means that you as an individual can request that a personal data controller adjust any errors in your personal data.

Under certain limited circumstances, there is also a right to be "forgotten". This is not an absolute right, but an assessment is to be made on a case-by-case basis. Issues concerning the right to be forgotten should normally be escalated to Legal.

Privacy by design

Every time we build a new function, purchase or develop a service or system of any kind, we must always ensure that we can meet our obligations in the data protection legislation as presented in these guidelines. We must remember to protect personal data from being spread, corrupted or lost, but we must also ensure that we can meet our other obligations and that we respect the basic principles (see above under "*Basic principles for lawful processing*").

This may involve ensuring that data is stored encrypted, that data is anonymised or pseudonymised, or other technical solutions to guarantee the privacy of personal data. The protection of personal data must therefore always be a part of our requirements, specification and design and not become something that we try to solve afterwards. In short - we must think beforehand.

Suppliers' processing of personal data

Evaluation before entering into a new supplier agreement
Prior to entering into a new agreement with a supplier, it must be ensured that:

- the new suppliers are analysed from an integrity perspective - i.e. that it is identified whether the supplier processes personal data on behalf of Hemnet and - if so - that the supplier's ability to comply with the data protection legislation is evaluated, and that
- formal requirements set out in the GDPR are complied with, with regards to the content of Data Processing Agreements (see below under *Data Processing Agreements and transfers to third countries*).

Legal shall ensure that the business receives relevant support. Prior to the extension of supplier agreements and otherwise where justified, suppliers' compliance with existing DPA and the ability to comply with data protection legislation must be followed up in an appropriate manner. In the event of personal data incidents that occur with suppliers, the supplier's ability for relevant security measures must be re-evaluated.

Data Processing Agreements and transfers to third countries

As soon as we ask someone to process personal data which we are the controller for, we must ensure that the processing takes place with the requirements and restrictions we set and in accordance with the data protection legislation's requirements for agreements between the data controller and the data processor. This is to be regulated by a Data Processing Agreement, or as they are often called "DPA".

We shall, through active choices, strive for personal data to be processed within the EU/EEA. However, in some cases we need to use systems or buy services where the supplier processes personal data outside the EU/EEA for our purposes, as a personal data processor. We also need to, regardless of where the personal data are localised but where the supplier itself is a US-based company (or where companies within the supplier's company group have actual or legal right to get access to the personal data that the supplier is processing on our behalf), deal with the possibilities that exist in American law for various authorities to request the personal data. Corresponding assessment may also need to be done for other non-European suppliers. Before the transfer of personal data to the supplier takes place we shall assess the lawfulness of the transfer, in each respective case, with the starting point in the data protection guidance applicable from time to time. The assessment shall include what special measures has to be taken to ensure that the personal data is adequately

protected. Examples of special measures is to make sure that the EU Commission has decided that the relevant country ensures an adequate level of protection of personal data, if the supplier is certified under a framework that the EU Commission has decided has an adequate level of protection (e.g. EU-US Data Privacy Framework) or that we enter so-called standard contractual clauses (“SCC”), adopted by the EU Commission, with the supplier. The issue with third country transfers must be regulated in the DPA and Legal must always be involved in the assessment.

Personal data incidents

No matter how well we have worked with "privacy by design" and risk mitigation in our processing of personal data, we may be affected by personal data incidents, i.e. an incident that affects the confidentiality, integrity or availability of personal data. Such an incident means that;

- Personal data has become accessible to others than those who are authorised (*confidentiality*)
- Personal data has been corrupted or altered in a way that it is no longer correct (*integrity*)
- Access to personal data is temporarily or permanently affected. We can e.g. have deleted it before it was time for deletion, lost the cryptographic key to encrypted data, etc. (*availability*)

Depending on the probability that a personal data incident involves risks for the individuals affected by it, and the severity of such risks, there may be an obligation to report the incident to Integritetsskyddsmyndigheten (“**IMY**”), the Swedish Authority for Privacy Protection, and/or to inform the individuals concerned.
All personal data incidents must be documented, and the risk to the individuals affected by it must be assessed by Legal according to the *Routine for handling and reporting personal data breaches.* Legal also assesses whether a personal data incident is subject to notification requirements or not.

Risk based approach - relevant security measures

Personal data shall be protected with relevant security measures, in relation to the risk that a personal data incident would entail for the individuals affected by it. Hemnet’s management of information security is described in the *Policy for Information and Data* as well as the underlying governing documents within information security.

Data Protection Impact Assessment (DPIA)

Prior to any new processing activity that may involve a high risk from an integrity perspective, a so-called impact assessment (DPIA or Data Protection Impact Assessment) is to be performed. An assessment of the risk must therefore always be made before a new personal data processing is initiated to ensure that the risks are adequately mitigated. Legal is responsible for carrying out data protection impact assessments in cases where potentially high risk activities have been identified.

Retention policies and Deletion

Deletion routines must be implemented in accordance with the retention periods stated in Hemnet’s processing register to ensure that the principle of storage limitation is maintained. Legal is responsible for implementing and maintaining deletion routines, with support from system owners in respective systems or managers.

Data Protection Officer (DPO)

The data protection legislation stipulates that if certain criteria are met, a business must appoint a so-called “Data Protection Officer" to monitor and support compliance with the GDPR. The DPO-role is regulated by law and requires registration with IMY. Hemnet has made the assessment that Hemnet’s

business does not meet these criteria, and has therefore not appointed a Data Protection Officer. Legal is responsible for making an annual reassessment.

Reporting channels for compliance issues

Hemnet's Code of Conduct indicates which reporting channels are to be used by employees who detect violations in compliance with Hemnet's steering documents. Each employee is asked to raise compliance issues with the person concerned in the matter in the first place where possible. If it is not suitable or possible, the employee should contact the immediate supervisor. If that is also not suitable or possible, employees are asked to contact their supervisor's supervisor, Hemnet's Chief People & Culture Officer or Hemnet's General Counsel. Also, severe misconduct can be reported anonymously via the Company's whistleblower function available via https://report.whistleb.com/en/hemnet.

Violations of these guidelines

Violations of these guidelines will always be taken very seriously and may lead to disciplinary action, including dismissal. In addition, violation of relevant laws may mean that you (and/or the Company) are subject to legal sanctions.

Related documents

- Hemnet's policy for Information & data
- Code of Conduct
- Routine for handling and reporting personal data breaches
- Routine for handling data subjects' rights (in Swedish only)