Data Protection Policy of Tamro companies in Sweden

1 General Provisions

1.1 Introduction

Tamro in Sweden enjoys an excellent reputation which is the result of the hard work and positive behaviour of our employees. The protection of the personal data of customers, patients, suppliers, business partners and employees is an important issue for Tamro. The breach of data protection laws can have serious consequences, such as fines and official investigations. However, the most serious consequence would be the damage caused to our reputation. This Policy outlines what actions Tamro employees should follow in order to maintain the integrity and security of personal data processed throughout the organisation which is fully supported by the Management Board of Tamro.

1.2 Objective

This Policy lays down the rules concerning the processing of personal data within Tamro companies within Sweden relating to the protection of data subjects. The aim of this Policy is to protect the fundamental rights and freedoms of data subjects in line with data protection laws (including but not limited to the European General Data Protection Regulation, GDPR, if applicable).

1.3 Material scope[1]

This Policy applies to the processing of personal and special personal data which relates to living individuals who can be identified from that data. It applies to data processed either electronically or that which is paper based and stored in a relevant filing system.

This Policy is designed to be used alongside existing Tamro policies.

1.4 Territorial scope[2]

This Policy applies to all organisations and businesses within Tamro in Sweden.

[1] Art. 2 GDPR.
[2] Art. 3 GDPR.

1.5 Legislation

This Policy is based on the provisions of the European data protection law (specifically GDPR) which sets high standards of data protection which applies throughout the Member States of the EU.

In some areas the law provisions of national laws and regulations of the Member States may be stricter than EU law. All PHOENIX group organisations and their employees must comply with the relevant local legislation.

1.6 Change of Policy

The Local Management of Tamro reserves the right to change or amend this Policy in consultation with the responsible data protection officer. The employees of Tamro have to comply with the regulations within this Policy.

1.7 Definitions[3]

For the purposes of this Policy (and in accordance with the GDPR):

I. '*consent*' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

II. '*controller*' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

III. '*data concerning health*' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

[3] Art. 4 GDPR.

IV. '*employee*' means person employed by Tamro or another PHOENIX group organisation;

V. '*filing system*' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

VI. '*personal data*' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

VII. '*personal data breach*' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

VIII. '*sensitive personal data*' means special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

IX. '*PHOENIX group*' includes any company in which the majority of shares are owned by a PHOENIX group organisation;

X. '*processing*' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

XI. '*processor*' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

XII. '*responsible data protection officer*' means the data protection officer of your organisation, the Local Data Protection Officer (LDPO) of your country, the Local Data Protection Coordinator (LDPC) of your country or the Head of Group Data Protection;

XIII. '*restriction of processing*' means the marking of stored personal data with the aim of limiting their processing in the future.

2 Principles

2.1 Principles relating to processing of personal data[4]

Lawfulness, fairness and transparency[5]

Processing shall be lawful, fair and transparent. Processing shall be lawful only, if:

a. the data subject has given consent (see paragraph 2.2 of this Policy);
b. processing is necessary for the performance of a contract;
c. processing is necessary for compliance with a legal obligation;
d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the public interest and/or;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

Purpose limitation[6]

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Please contact your

[4] Art. 5 GDPR.
[5] Art. 6 GDPR.
[6] Art. 5 GDPR.

responsible data protection officer in advance (before plans are put in place) if you change the purposes of processing.

Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed. It shall be deleted if it is no longer required. The local management board ensures that the local requirements for retention and deletion are fulfilled.

All employees review their records regularly (at least once per year) and delete them where appropriate to ensure compliance with their local requirements. The heads of departments are responsible for such a review.

All employees have to inform the responsible data protection officer about irregularities with deletion measures and data assets with no clear or even wrong deletion rules.

For details please see the "Guidance on retention of records" (as **Annex1**).

Accuracy

Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data which is identified as being inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation[7]

Personal data shall be kept in a format which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Integrity and confidentiality[8]

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

Tamro, as data controller, is responsible for ensuring it is to demonstrate compliance with the GDPR principles listed above. All employees are required to complete the PHOENIX group Data Protection training.

---

[7] Art. 5 GDPR.

[8] Art. 5 GDPR.

The controller has to maintain a complete record of processing activities[9]. All employees (especially heads of departments) are required to inform their responsible data protection officer in advance (before plans are put in place) about new or changed processing of personal data so that they can adapt the records and check the requirements for the processing.

2.2 Conditions for consent[10]

Where processing is based on consent, the consent can only be considered to be lawful if it is given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her.[11] In addition the following conditions must be met:

a) the consent shall be kept in a format which can be used to demonstrate that the data subject has consented to the processing of his or her personal data;
b) the request for consent which is given in the context of a written declaration which also concerns other matters, shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible format, using clear and plain language;
c) the data subject shall have the right to easily withdraw his or her consent at any time. Prior to giving consent, the data subject shall be informed about the way which the consent can be revoked;
d) the consent of a child below the age of 13 for information society services[12] (e.g. online services) shall only considered to be lawful if the consent is given or authorised by the holder of parental responsibility over the child.[13]

Please contact your responsible data protection officer for templates for such consent forms.

2.3 Processing of special categories of personal data[14]

Processing of special personal data is prohibited unless:

---

[9] Art. 30 GDPR.

[10] Art. 7 GDPR.

[11] Recital 32.

[12] Information society services means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

[13] Art. 8 GDPR.

[14] Art. 9 GDPR.

a. the data subject has given explicit consent;
b. processing is necessary in the field of employment and social security;
c. processing is necessary to protect the vital interests of the data subject;
d. processing is necessary for the establishment, exercise or defence of legal claims;
e. processing relates to personal data which are manifestly made public by the data subject;
f. processing is necessary for the purposes of medical diagnosis, the provision of health or social care or treatment;
g. processing is necessary for reasons of public interest in the area of public health; in these cases those data have to be processed by or under the responsibility of a professional subject to the obligation of professional secrecy or by another person also subject to an obligation of secrecy.

Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by national law.[15]

3 Rights of the data subject

3.1 Transparent information, communication and modalities for the exercise of the rights of the data subject

Every data subject has the following rights:

- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restriction of processing;
- Right to data portability;
- Right to object.

Tamro, as data controller, should take necessary steps to verify the identity of the data subject prior to responding to any of the rights listed above. Any information and communication relating to data processing, for the data subject has to be in a concise, transparent, intelligible and easily accessible format, using clear and plain language. The information shall be provided in writing or by other means, including, where appropriate, electronically. The data controller shall provide information without undue delay and in any event within one month after receipt of the request.

[15] Art. 10 GDPR.

3.2 Information to be provided where personal data is collected from the data subject and where personal data has not been obtained from the data subject[16]

Whether personal data is obtained directly from the data subject or not, Tamro is required to provide the necessary information to the data subject. This needs to be done either at the time of collection or within a reasonable period after obtaining the data from someone else. However this must be done no later than one month. Please contact your head of department and/or your responsible data protection officer for examples of information templates.

3.3 Right of Access by the Data Subject[17]

A data subject has the right to obtain from Tamro, as data controller, confirmation as to whether or not personal data concerning him or her is being processed (so called Subject Access Request, SAR). If so, access to the personal data and further information, specifically the purpose(s) of the processing, the categories of personal data concerned, etc. must be made available to the data subject upon request. Please contact your head of department and/or your responsible data protection officer to check if and how to answer such a SAR.

3.4 Right to Rectification[18]

Data subjects have the right to have their personal data rectified if it is inaccurate and to have incomplete personal data completed (including a supplementary statement). Requests are to be processed without undue delay.

3.5 Right to Erasure ("Right to be forgotten")[19]

Data subjects have the right to request that their personal data be erased, e.g. in cases where the data is no longer required for the purposes Tamro originally collected it for, or the data subject withdraws their consent. If Tamro, as data controller, has made the information public, they will take reasonable steps to inform controllers who are processing the personal data that the data subject requested the erasure ("right to be forgotten"). Tamro organisations do not have to delete it in all cases, e.g. if they need it to comply with a legal

[16] Art. 13 and 14 GDPR.
[17] Art. 15 GDPR.
[18] Art. 16 GDPR.
[19] Art. 17 GDPR.

obligation. Please contact your head of department and/or your responsible data protection officer in such cases.

3.6 Right to Restriction of Processing[20]

The data subject has the right to request that processing of their data be restricted, e.g. if Tamro, as data controller, no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims. Please contact your head of department and/or your responsible data protection officer in such cases.

Tamro, as data controller, will take reasonable measures to inform all those with whom the data has been shared about the requested restrictions.

3.7 Right to Data Portability[21]

The data subject has the right to receive copies of the personal data they have provided to Tamro, as data controller, in a structured, commonly used and machine-readable format. The data subject has the right to request that the data be transmitted from the controller to another controller. This applies where the processing is based on consent, contract, and the data is processed by automated means. Please contact your head of department and/or your responsible data protection officer in such cases.

3.8 Right to object[22]

The data subject has the right to object at any time to processing of his or her personal data, especially for direct marketing, profiling and research purposes. Tamro, as data controller, shall no longer process the personal data unless they demonstrate compelling legitimate grounds for the processing. Please contact your head of department and/or your responsible data protection officer in such cases.

[20] Art. 18 GDPR.
[21] Art. 20 GDPR.
[22] Art. 21 GDPR.

4 Controller and processor

4.1 Security of processing

Tamro, as data controller, shall implement appropriate technical and organisational measures (e.g. pseudonymisation and encryption of personal data) to ensure a level of security appropriate to the risk[23]. This is to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, as detailed in the PHOENIX group Information Security Policy. The data controller shall also ensure data protection by design and by default, so that necessary safeguards to implement data-protection principles are integrated. This will help to ensure that only personal data which is necessary for each specific purpose of the processing are processed.[24] To ensure continuous improvement of the Information Security Management System and to guarantee the adaption of new technical requirements, periodic reviews and audit processes have been established.[25] Business continuity and disaster recovery plan are established to ensure the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

4.2 Joint controllers

When two or more controllers (e.g. Tamro together with an external service provider) jointly determine the means and purposes of processing of personal data, they shall be joint controllers and need a written agreement. Please contact your responsible data protection officer for further information.[26]

4.3 Processor[27]

Processing carried out on behalf of a controller (e.g. a service provider in IT or Human Resources) is only allowed if the processor provides sufficient guarantees to ensure the protection of the rights of the data subject and a contract has been agreed. The processor must be selected carefully and regularly audited. Please ask your responsible data protection officer for an agreement and the audit template.

---

[23] Art. 24 GDPR.
[24] Art. 25 GDPR.
[25] Art. 32 GDPR.
[26] Art. 26 GDPR.
[27] Art. 28 GDPR.

The same applies if Tamro is processing personal data on behalf of another organisation (e.g. PHOENIX group IT GmbH for IT services).

Additionally, steps must be taken to ensure that the processor meets the information security standards set by the PHOENIX group Information Security Policy, and processes data only as instructed.[28] The processing of EU citizens personal data is prohibited if the processing takes place outside of the EU, unless the special conditions of data transfer are met (see chapter 5 of this Policy).

4.4 Cooperation with the supervisory authority

Tamro and its employees are required to cooperate with the Swedish Data Protection Authority. If as an employee you are contacted by the Swedish Data Protection Authority, please contact your responsible data protection officer immediately.[29]

4.5 Personal data breach

Any breaches of personal data must immediately be reported to the responsible data protection officer by the employee or the head of department via the PHOENIX group portal. If the breach is likely to result in a high risk for the rights and freedoms of the data subjects, the data subject must be notified without undue delay.[30]

If the data breach is likely to result in a risk to the rights and freedoms of the data subjects, the local supervisory authority must be informed without undue delay (which will be done by your responsible data protection officer), this must be done no later than 72 hours after having become aware of the breach.[31]

For group-relevant breaches the Local Data Protection Officer or Local Data Protection Coordinator will also notify the head of Group Data Protection.

To mitigate the risks caused by a data breach and expedite the reporting process towards both, the supervisory authorities and also the concerned data subjects, the corresponding data breach process must be followed, for each data breach, which will guarantee that the data protection law requirements are fulfilled. For details please see the “Guidance on data breaches” (as **Annex 2**).

---

[28] Art. 29 GDPR.
[29] Art. 31 GDPR.
[30] Art. 34 GDPR.
[31] Art. 33 GDPR.

If you have any questions about data protection or are concerned that personal data is being compromised, you can contact your responsible data protection officer to discuss your concerns.

4.6 Data Protection Impact Assessment

Data Protection Impact Assessments (DPIA)[32] are required prior to the processing where the processing of data, particularly if new technologies are being used, is likely to result in a high risk to the rights and freedoms of data subjects.

A DPIA will be required in the following scenarios:

1) Introduction of new technologies,
2) automated processing, including profiling results in decision(s) being made which produce legal effects on individuals,
3) large scale processing of special category data is taking place,
4) processing of criminal activities,
5) systematic monitoring of a publicly accessible area on a large scale.
6) For further cases please see the local supervisory authority's lists.

In order to ensure that the DPIA is completed ahead of the commencement of new or changed processing of personal data, the appropriate employee must inform their responsible data protection officer in advance (before plans are put in place). Please contact your responsible data protection officer who can provide DPIA templates, guidance and ongoing advice.

In circumstances where a DPIA indicates that the processing would result in a high risk to the rights and freedoms of data subjects in the absence of measures taken by the data controller to mitigate the risks, the (Local) Data Protection Officer shall consult with the Swedish Data Protection Authority.

4.7 Designation of the data protection officer[33]

Tamro must decide if the designation of a data protection officer is necessary. In order to ascertain this, local law and the GDPR provisions should be reviewed and considered. The GDPR states that if the core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or the core activities consist of

[32] Art. 35 GDPR.
[33] Art. 38 GDPR.

processing on a large scale of special categories of data – in retail countries it is recommended.

If Tamro appoints more than one data protection officer, Tamro should nominate one as Local Data Protection Officer (LDPO). If they have no data protection officers, they should nominate one person as Local Data Protection Coordinator (LDPC). The LDPO and/or LDPC should report to the local management board. The data protection officers of the organisations, the LDPO and the LDPC have the responsibility to protect the rights of the data subjects in their organisation/country and to cooperate closely with each other and with the Head of Group Data Protection.

The PHOENIX group has appointed a Head of Group Data Protection who coordinates the cooperation regarding all crucial issues of data protection at PHOENIX group, together with the LDPO and LDPC of the countries of the PHOENIX group plus the Group Information Security Manager. The Head of Group Data Protection reports to the Management Board of the PHOENIX Group. The Head of Group Data Protection shall have close cooperation with the countries of the PHOENIX group. Their task is to monitor the compliance of the group-wide policies (this Policy plus detailed policies), to develop and update them.

The appointed roles shall have the necessary professional qualifications and knowledge of data protection law and practices.

The PHOENIX Group has appointed a Group Information Security Manager who counsels the PHOENIX group in all relevant security aspects. The task of the Group Information Security Manager is to develop, enhance and monitor the information security standards of the PHOENIX group.

4.8 Position of the data protection officer[34]

The data protection officers, LDPO, LDPC and Head of Group Data Protection shall be involved appropriately and in a timely manner in all issues, projects, changes or operations, which are related to the regulations of the protection of personal data.

The Group Management Board, the local management boards and all employees shall support the data protection officers, LDPO, LDPC and Head of Group Data Protection in performing their tasks.

The data protection officers, LDPO, LDPC and Head of Group Data Protection shall have the resources that reflect the nature and complexity of the business model in the organisation,

[34] Art. 38 GDPR.

including those to be carried out in the context of mutual assistance, cooperation and participation in group-wide data protection issues and projects.

They shall have an independent and protected position in the organisation and report to highest management level of the relevant PHOENIX group organisation.

They shall be the natural contact point for any data subjects with regard to the processing of their personal data and contact point for supervisory authorities.

They shall be bound by secrecy and/or confidentiality concerning the performance of their tasks.

The contact details of the responsible data protection officers, LDPO, LDPC and Head of Group Data Protection shall be published on Tamro's intranet (COIN) or similar.

4.9 Tasks of the data protection officer[35]

The data protection officers, LDPO, LDPC and Head of Group Data Protection shall be responsible for informing and advising the organisation/countries of PHOENIX group as controller and processor plus the employees in the organisation/countries.

The local management board of Tamro, as data controllers, are responsible for ensuring that the requirements regarding data protection formulated by law, regulations and group-wide policies are respected. The management board is specifically responsible for the protection of the rights of data subjects.

The data protection officers, LDPO, LDPC and Head of Group Data Protection shall be responsible for monitoring the compliance with the General Data Protection Regulation (if applicable), the local laws and provisions concerning data protection, this Policy and further detailed PHOENIX group policies, in order to protect the fundamental rights and freedoms of data subjects in relation to the processing of personal data.

The Head of Group Data Protection shall in close cooperation (e.g. via regular telephone conferences, meetings, etc.) with the LDPO and/or LDCP establish a common framework that can act as a supporting forum for informing and advising local PHOENIX group organisations (as controllers or processors) concerning data protection regulations.

The LDPO and LDCP shall monitor and report non-compliance issues and possible risks in Tamro's operations to the Head of Group Data Protection. They shall inform them about

[35] Art. 39 GDPR.

controls of supervisory authorities. The LDPO and LDCP shall ensure sufficient training and awareness activities for controllers, processors and employees in their countries. The Head of Group Data Protection provides a group-wide e-learning.

For a better overview see the responsibilities in the **RACI Matrix as Annex 1.**

5 Transfer of personal data

A transfer of personal data within the country in which data has been collected, within the European Union (EU) and European Economic Area (EEA) (including the processing in a third country after the transfer) is generally permitted if processing of the data is also permitted according to GDPR (especially to Chapter II).

The transfer of personal data from an EU/EEA country to a third country (outside EU/EEA) is permitted only if additional requirements are met. In such a case ask your responsible data protection officer. The transfer is permitted:

- where the European Commission has decided that the third country ensures an adequate level of protection ("adequacy decision", e.g. Switzerland)[36]; or
- where the receiving party has provided appropriate safeguards (e.g. binding corporate rules, standard data protection clauses adopted by the Commission, approved code of conduct)[37]; or
- according to judgments of a court or tribunal or decision of an administrative authority if based on an international agreement[38]; or
- where the transfer takes place in specific situations (e.g. explicit consent of data subject, necessary for performance of a contract, necessary for establishment, exercise or defence of legal claims, necessary in order to protect vital interests of data subject)[39]; or
- where the transfer is necessary for the purposes of compelling legitimate interests of controller and the controller informs the supervisory authority[40].

6 Remedies, Liability and Penalties

There are the following remedies:

[36] Art. 45 GDPR.
[37] Art. 46 GDPR.
[38] Art. 48 GDPR.
[39] Art. 49 GDPR.
[40] Art. 49 (1) GDPR at the end.

- Right of the data subject to lodge a complaint with a supervisory authority[41],
- Right of a natural or legal person to an effective judicial remedy against a supervisory authority[42],
- Right of data subject to an effective judicial remedy against a data controller or data processor[43] and
- Right of the data subject to mandate a not-for-profit body, organisation or association[44].

Breaches of data protection can result in claims of data subjects for compensation of material or non-material damage[45]. The authorities can impose administrative fines up to 10m or 20m EUR, or in the case of a company up to 2 or 4 % of the total world-wide annual turnover of PHOENIX group of the preceding financial year[46]. According to Swedish laws infringements can lead to criminal prosecution[47]. Violations for which individual employees are responsible can lead to sanctions under Swedish disciplinary procedures in line with Swedish employment law.

7 Processing in the context of employment

Under Swedish law there might be more specific rules by law or by collective agreements for processing of employees' personal data in the employment context[48].

8 Final provisions

This Policy shall apply from 25 May 2018.

[41] Art. 77 GDPR.
[42] Art. 78 GDPR.
[43] Art. 79 GDPR.
[44] Art. 80 GDPR.
[45] Art. 82 GDPR.
[46] Art. 83 GDPR.
[47] Art. 84 GDPR.
[48] Art. 88 GDPR.

9 Authorisation by Local Management

Lars Schenatz	Peter Blomqvist	Mats Johnsson
Eva Backlund Strid	Johan Mossberg	Mikael Brammesjö
Magnus Peterson	Henrik Schylander	

Annexes:

1. Guidance on retention of records
2. Guidance on data breaches
3. RACI Matrix