Personal data policy for TiksPac

For all employees and customers – concerning processing of personal data

Version	Date	Changed by	Established by
1.1	25 June 2018	Johan Nilsson	CEO, Stefan Arvidsson

Contents

Personal data policy for TiksPac

This document has two purposes: Firstly as a practical instrument in the company's work to protect personal data, and secondly as a written documentation of our efforts to comply with legal requirements in accordance with the General Data Protection Regulation (GDPR). Through this document, we are guaranteeing to our customers, suppliers, partners and other stakeholders that we are doing all we can to protect and process their data in accordance with the applicable legislation and practice.

TiksPac's personal data policy has been developed together with the company's overall strategy, assessments and visions, and is therefore an integrated part of how the company works. The policy has been established by the management and all employees are familiar with it and their responsibilities in connection with processing personal data. If there is any suspicion that personal data are not being handled correctly, contact your immediate supervisor immediately and inform them of what has happened.

This personal data policy is revised and updated at least once a year by the management team. All new employees are made aware of this policy when starting employment, and must confirm they have taken note of it by signing the employment contract. The signed employment contract is stored in the employee's personal file by the Human Resources Department.

Together with this personal data policy, an IT policy has been developed to deal with the more technical aspects concerning processing of personal data, including preparations for any security breaches. In addition to this, a database register has been created. This is stored and kept updated by the Controller at TiksPac.

1. Definitions

TiksPac processes personal data in connection with purchases, sales, marketing, cooperation and HR questions. Some of the key terms that arise in connection with GDPR are defined below, to make it easier to understand the personal data policy.

GDPR	The General Data Protection Regulation is the law that will govern the processing of personal data after 25 May 2018.
Personal data	All information about an identified or identifiable natural person, such as name, address, telephone number, personal ID number, photos, etc. Information about individual companies is also personal data.
Sensitive personal data	According to the regulation, sensitive personal data includes health data, trade union membership, race/ethnicity, political affiliation, philosophical beliefs, religion, genetic or biometric data.
Data subject	All people whose information is processed by TiksPac, e.g. customers, employees and suppliers.
Processing (of personal data)	Everything the company does with personal data, including storage and deletion.
Controller	The person deciding on the purpose, scope and methods of processing personal data, in this case TiksPac AB, 556856-0063
Processor	The party handling personal data on behalf of the Controller, e.g. payroll, cloud services and transport operators.

2. Organisation and responsibility

TiksPac is divided into different units. This personal data policy applies to all parts of the organisation, but in some cases it may be necessary to have specific rules for specific parts. Where specific rules are

required, these rules must be consistent with this policy, have a clear division of roles and responsibilities and a defined plan for review.

The responsibility for ensuring employees comply with this personal data policy lies primarily with the employees themselves, then with their immediate supervisors. Checks of compliance with this policy should be carried out and the results reviews documented and kept by the Controller. If checks show that there have been incidents in which this personal data policy has not been followed, it is primarily the immediate supervisor's task to remedy these incidents. Department heads/company managers must also carry out regular follow-ups and report to the Controller for the company, who has the overall responsibility for the personal data policy.

3. Instructions to employees

Below are the specific rules and guidelines that all TiksPac employees must follow in connection with the processing of personal data. These instructions and guidelines are based on the legal requirements in GDPR and, together with the IT Policy and other documents concerning personal data processing, form the basis for the company's efforts to comply with the regulation. Each part of the instructions is divided into **purpose** (why we do it) **guidelines** (how we do it) and **checks** (how we actually did it).

3.1 Legal basis

Purpose:

- There is a legal basis for all personal data processing

Guidelines:

Before starting to process personal data, the legal basis for processing must be established. This is done by the process owner in consultation with the head of department. GDPR specifies six different cases of legal basis;

- Consent
- Performance of a contract
- Legal obligation
- Vital interest
- Public interest and exercise of official authority
- Legitimate interest

As a rule, the company uses *legitimate interest* regarding customers and prospective customers, as well as consent and performance of contracts for employees, suppliers and established customers. Should any questions or uncertainties arise regarding the legal basis, contact your immediate supervisor or the Controller for the company. If a legal basis cannot be identified, processing of the personal data cannot be started.

In the event sensitive personal data is processed outside the requirements for the employment, the legal basis is always consent.

When processing personal data on children under the age of 13, consent must be given by the child's parents.

The legal basis for processing the personal data should be documented together with the relevant processes in the database register.

Signed/accepted consent documents should be kept by the Controller.

Checks:

Examples of checks:

All processing is reviewed annually, including the legal basis.

3.2 Minimisation of data and limitation of purpose

Purpose:

- The information collected is based on a clear purpose and we do not collect more information than is actually required.

Guidelines:

For each processing event, there must be clearly defined guidelines on which personal data are relevant in relation to the purpose, which also ensures that no more data is collected than is actually necessary. The purpose of the processing and the types of personal data processed should be defined in the database register.

In cases where it may be in the company's interest to collect more data than is necessarily needed, there must be a documented consent.

Checks:

Examples of checks:

All processing is reviewed annually, the collected categories of personal data are compared in order to ensure that the data are still needed to achieve the purpose.

Responsible managers must perform random checks in the CRM system once a month, in order to check whether the processing contains more data than relevant for the purpose. If the system contains more data, consent must be obtained from the data subject.

3.3 Correctness and openness

Purpose:

- To ensure transparency regarding the company's processing of personal data and to ensure that the data subjects are aware of their rights.

Guidelines:

When starting employment, employees should be informed, in an easy-to-understand manner, through their employment contract of:

- Who the Controller is, together with their contact information
- The purpose of processing personal data
- Legal basis for processing and legitimate interests used by the company
- Other recipients of the company's personal data and any transfers to third countries
- Sorting time for personal data
- The rights of the data subject in relation to personal data (right of access, correction of data, deletion of data, limitation of processing and portability)
- Right to withdraw consent
- The right to complain to the supervisory authority
- Whether they have an obligation to inform and the potential consequences of failing to inform
- How the information is collected if it does not come directly from the data subject
- Possible scope of automated decision-making and the logic behind this

If the company subsequently wishes to process personal data for a purpose other than that previously disclosed to the data subject, the data subject must be informed of this before processing is started.

A summary of the company's personal data processing and this privacy policy are posted on the company's website as information for customers and stakeholders. A link to this policy is sent electronically to the data subject with initial contact.

Checks:

Examples of checks:

It is the responsibility of the department heads to verify compliance with the requirements on which information should be shared. Sharing of most of the information is ensured as it is available on the website, but with direct contact via e-mail, a link to the information must be enclosed. This e-mail is the acknowledgement that we are complying with the information requirements and must be archived along with other customer information. Open customer cases are regularly reviewed to ensure compliance with the information requirement.

3.4 Right of access

Purpose:

- To ensure that the data subject can access the information being processed about them

Guidelines:

Upon request, the data subject must, without undue delay, be given access to the information stored about them in an easily readable manner, including:

- The purpose of the processing
- What categories of data are processed
- Any other recipients of the information, including transfers to third countries
- The retention period for the data
- The data subject's rights in relation to their personal data (access, correction, deletion, limited processing and portability)
- The right to lodge a complaint with the supervisory authority
- How the company received the data if it was not supplied directly by the data subject
- Possible scope of automated decision-making and the logic behind this

An employee who receives such a request should contact the Controller for the company as soon as possible. The information should be provided in paper format or in a user-friendly electronic format based on which format the data subject wants.

It is necessary to ensure that the person receiving the data is the right person. The information may only be shared after the person has identified themselves or it has otherwise been ensured that the person requesting access is actually the person to whom the information relates, or they have authorisation from that person.

Telephone requests

In case of telephone requests, it is necessary to ensure that information is communicated to the right person. For example, it may be necessary to ask control questions, such as asking for their address or personal ID number, or call the person back. If the employee cannot guarantee the person’s identity, the information must be sent by letter to the data subject’s registered address to reduce the risk of fraud.

Requests via letter and e-mail

If the name and address of the letter/e-mail is identical to the previously registered information in the system, the information can usually be sent to the registered address. If this is not the case, the case must be investigated before the information is shared.

Access to information on behalf of someone else (Authorisation)

The data subject may authorise someone else to access their information. This authorisation can be specific or general.

In case of any uncertainty on whether the authorisation is sufficient, senior management/legal counsel must be consulted.

Checks:

Examples of checks:

Requests for access to information are checked monthly to ensure that they are handled without unnecessary delay.

3.5 Ensuring the right to correction

Purpose:

- To ensure that data subjects can have their data corrected in the event of errors

Guidelines:

Upon request from the data subject, the company must correct any incomplete or incorrect information about the person concerned.

An employee who receives a request for correction or who discovers that incorrect information is being processed must notify the Controller, who will correct the erroneous data.

Checks:

Examples of checks:

Requests regarding corrections are checked regularly to ensure that they are handled without unnecessary delay.

3.6 Sorting and the right to be forgotten/deleted

Purpose:

- Personal data are deleted when there is no longer a purpose for processing them
- To ensure that the data subject has the right to be deleted/forgotten

Guidelines:

The sorting time for each processing is stated in the database register.

Personal data are stored in defined storage areas and systems to minimise dissemination of personal data within the organisation and to facilitate the deletion and sorting process. If employees need to temporarily store personal data locally, they should delete them as soon as the work/need is accomplished.

The Processor also needs to ensure that it sorts/deletes information.

Personal data should be deleted regularly:

Employees should regularly delete/sort e-mails containing personal data, when these are moved and stored in designated locations or when there is no longer a purpose for processing the data.

Employees destroy physical documents that contain personal data on a regular basis when they are no longer needed.

The person responsible for systems containing personal data deletes or anonymises the data in the systems when there is no longer any purpose or need for processing them.

Before any information is deleted, it is necessary to ensure that it does not need to be stored to comply with any other rule/statutory requirement.

The right to be forgotten:

Where a data subject requests to be forgotten, this request must be forwarded to the Controller, who deletes their data without undue delay after ensuring that there is no longer a purpose/need to process the information. It is necessary to ensure that the data subject has no outstanding/unfinished

business/contract with the company before the information is deleted. Employees handling requests for deletion must inform the data subject if the company cannot fully or partially comply with the requirement for deletion e.g. where it is not possible to continue providing a service without the personal data. The data subject must always be able to delete data obtained with consent as a legal basis. It is necessary to ensure the identity of the data subject before data is deleted.

Deletion of data in backups:

If it becomes necessary to read a backup, it is necessary to ensure that deleted information in the production environment is deleted again during rereading – this is done manually.

Checks:

Examples of checks:

The sorting time for personal data processing is reviewed annually.

Every year, checks are performed in the CRM system in order to delete data on customers who should not still be in the system.

Every quarter, checks are performed of whether data that should have been deleted has been deleted.

Employees carry out regular checks on whether personal data stored locally or in e-mails are moved to the designated location and deleted from the mailbox and local computer.

3.7 Limitations on processing personal data

Purpose:

- To limit the processing of personal data to consist exclusively of storage

Guidelines:

When a data subject requests limitation of the processing of their personal data, the Controller for the company must be informed immediately. The processing of personal data is then limited to storing the personal data until the reason for the request for limited processing is investigated and rectified.

Checks:

Examples of checks:

Requests for limited processing are checked regularly to ensure that the company has actually limited its processing to consist exclusively of storage and that this was done without undue delay.

3.8 Right to object

Purpose:

- To satisfy the data subject's right to object to profiling and direct marketing

Guidelines:

When a data subject notifies that they do not want personal data to be used for profiling or direct marketing purposes, contact the Controller for the company immediately to ensure that the processing of personal data for the purpose of profiling and direct marketing is stopped.

Checks:

Examples of checks:

Requests received regarding limitation are checked regularly to ensure that the company no longer uses the information for profiling

3.9. Processing agreement

Purpose:

- To ensure that a processing agreement is entered with other parties who have access to personal data or to which we send personal data.

Guidelines:

A processing agreement has been entered with all organisations that have access to the company's personal data or to which the company sends personal data.

Whenever a new contract is entered with a supplier, assessment should be made as to whether the service will involve/contain any personal data. If this is the case, a processing agreement must be drawn up.

Regular checks of the Processor's premises are carried out by obtaining audit documentation or by visiting the supplier in order to ensure compliance with the processing agreement.

Processing agreements are stored centrally by the Controller for the company.

If an employee discovers or becomes aware that the processing of personal data by the Processor fails to comply with established contracts, they must notify the Controller for the company.

Checks:

Examples of checks:

The list of current Processors is checked regularly and matched to current processing agreements to ensure the agreement is still sufficient.

Audit documentation is collected annually from IT-providers, primarily concerning processing of personal data in order to assess and ensure compliance with the processing agreement.

3.10 Safeguarding documentation

Purpose:

- To meet the requirements in GDPR for a database register and the risk analyses carried out.

Guidelines:

The company has established a database register, which is available from the Controller for the company. The database is regularly updated when new processing is carried out or changes occur within the company concerning personal data processing.

Checks:

Examples of checks:

The company's processing is reviewed annually to determine whether any high-risk processing is being carried out, the purpose of this is also to determine whether a new risk analysis and action plan need to be established to reduce potential risks. If it is not possible to reduce the risk, the supervisory authority must be consulted before processing is started. Risk analyses are updated in plans for new processing or changes in existing processing.

3.11 Data security

Purpose:

- To ensure that the necessary organisational and technical measures have been taken to prevent personal data from being unintentionally disclosed or lost.

Guidelines: Limitation of access to personal data stored electronically.

All systems/storage sites that contain personal data have limited access, so that only employees who need the data in their work are able to access them.

Checks:

Examples of checks:

Checks are performed regularly of access rights for systems and storage areas to ensure that this is consistent with the employee's duties and that they need access to the personal data.

Guidelines: E-mails containing personal data

E-mails containing personal data must be limited to the absolute minimum. Where there is still a need to send personal data via e-mail, content must be encrypted and sent via secure e-mail.

Checks:

Examples of checks:

General security settings in the IT environment are checked regularly

3.12 Physical security

Purpose:

- To ensure that measures are taken to prevent unauthorised access to places where the processing of personal data takes place.

Guidelines:

Areas where processing of personal data takes place are secured in such a way that unauthorised persons cannot gain access. This is achieved by storing personal data in locked cabinets/drawers when the room is left unattended. In addition, personal data are regularly archived in locked archives.

All employees should lock their computer using a screen lock as soon as they leave it, even if only for a short time. The company also applies a clean desk policy, which means that all employees should put away/lock up documents when leaving the workplace. The employees shall also apply the so-called Front down policy, which means that documents containing personal data should be turned over or covered when leaving the workplace.

For more information on security, please refer to the company's IT and information security policy.

Checks:

Examples of checks:

A review of documents in locked cabinets must be carried out annually.

Random checks should be carried out to ensure that cabinets and drawers are locked and that only the employees responsible for the cabinet/drawer have a key

Checks and reminders should be performed to ensure that employees actually do lock their computers when they leave the workplace.

3.13 Printouts and documents containing personal data

Purpose:

- Personal data in paper format must be handled correctly.

Guidelines:

Ensure that printers are monitored when printing documents that contain personal data and do not leave documents that contain personal data lying in the printer.

Do not leave paper documents containing personal data unattended in the workplace.

All physical documents (letters, printed e-mails, notes, etc.) containing personal data must be destroyed in designated recycling or destroyed in a shredder.

Checks:

Examples of checks:

Regular checks should be carried out to ensure that documents containing personal data are not left lying in printers and that no documents containing personal data are left unattended in the workplace.

3.14 Employee training and knowledge

Purpose:

- To ensure that all employees are aware of the requirements and rules applicable to the processing of personal data

Guidelines:

All TiksPac employees must sign a confidentiality agreement when starting employment.

All new employees must be trained in the rules and guidelines that apply to the processing of personal data when starting employment.

Checks:

Examples of checks:

When starting employment, the employee signs the confidentiality agreement and has read and understood the company's personal data policy.

Every year, all employees are required to participate in training concerning the processing of personal data.

3.15 Reporting personal data breaches

Purpose:

- To ensure that the supervisory authority is notified within 72 hours and, in special cases, the affected data subjects are also informed as soon as possible.

Guidelines:

Breaches are defined as an event which risks personal data being made available to those not authorised to access them or where personal data are lost or destroyed.

If an employee detects a data breach or a security breach, it must be reported to the Controller for the company as soon as possible. The Controller then, together with the employees concerned, collects information about the breach, the amount of personal data and the number of data subjects affected, as well as potential consequences for the data subjects, before deciding whether it must be reported to the supervisory authorities

If the breach is so serious that the data subjects must be notified, this is done via e-mail.

For information on how the company protects personal data and detects potential breaches, please refer to the company's IT and information security policy.

Checks:

Examples of checks:

Regular checks are carried out so that situations requiring notification to the supervisory authority are also reported within 72 hours.

3.16 Privacy by design and privacy by default

Purpose:

- Compliance with the requirements for privacy by design and privacy by default in GDPR

Guidelines:

When purchasing or developing new IT systems, the company must ensure that the systems are secure and that they comply with the requirements for protection of personal data, the separation of users and protection against data loss.

Employees are not allowed to use services that process personal data without this being approved by the Controller or IT manager for the company, including private e-mail clients, private cloud services that can be downloaded from the internet.

Checks:

The IT department has checklists on how new systems and services can be developed/connected to existing systems. The IT department performs regular checks on which systems are being used and also searches the network to ensure that unauthorised applications are not used.

4. Cookies

When you visit our website, information about the visitor is collected in order to ensure that they get the best experience of the website with access to all features. Therefore, in order to use our website as intended, we recommend that you allow the use of cookies on your computer. If you do not allow cookies, you risk having a poor user experience and not being able to use the full site.

There are two types of cookies. One type saves a file on your computer for a longer period. This is used, for example, for functions that provide information on what is new since the user last visited the relevant website. The second type of cookie is called a session cookie. While surfing a website, this cookie is stored temporarily in your computer's memory, for example, to keep track of the selected language. Session cookies are not stored for an extended period of time, but disappear when the browser is shut down. Cookies cannot contain malicious content, such as viruses.

If you do not want information to be collected, it is possible to delete or block cookies in your browser settings.