Policy Document

DATA PRIVACY

Policy Identification	Tausi - Data Privacy	Date Compiled	01 July 2024
Policy Owner	Group Human Resources	Policy Location	IMS HR Manual HR Departments
Version	1		

1. INTRODUCTION

Tausi respects the privacy of individuals and is committed to managing personal data in a professional, lawful and ethical manner. Personal data means any information, whether in a physical document or in electronic form, relating to an identified or identifiable individual; if the information allows someone, somewhere (even outside Tausi) to identify an individual then the data is personal data.

Examples of personal data include an individual's name, contact information, online identifiers such as IP addresses, cookie strings or mobile device IDs, that can be used to identify an individual, personal preferences or opinions, employment information, financial information, photographs, CCTV images, or location data.

Sensitive personal data are special categories of personal data and are subject to more stringent requirements and IT controls and should only be collected in specific limited circumstances. Examples of sensitive personal data include an individual's racial or ethnic origin, political opinions, membership of political parties or similar organisations, religious or philosophical beliefs, trade union membership, physical or mental health information including any opinion thereof, sexual orientation or sexual life, criminal records or proceedings regarding criminal or unlawful behaviour, or biometric data (such as fingerprints, retinal or facial recognition). In some circumstances, photographs may be considered sensitive personal data when used to identify such information as ethnicity or a health condition.

Tausi is subject to a wide range of national and international data privacy laws that protect the personal data and privacy of individuals while maintaining the ability of organisations to use personal data for legitimate business purposes.

Data privacy laws can vary greatly from country to country and, in some countries, are non-existent. Consequently, Tausi has adopted rules that govern intragroup processing of personal data, including transfers between countries, in a binding and consistent manner Personal data processes by Tausi in any location is therefore subject to the requirements of the rules. Where local law has stricter requirements then these must be met in addition to the rules in this policy.

2. IDENTIFYING SYSTEMS AND BUSINESS OPERATIONS THAT PROCESS PERSONAL DATA

All instances of processing personal data must be identified, whether in IT systems, applications, mobile applications, cloud computing, websites, campaigns or otherwise.

Where new operations/systems that process personal data are being designed or existing ones updated, Businesses and Functions ;must ensure that these mandatory requirements are followed.

3. PROCESSING PERSONAL DATA FOR A LEGITIMATE BUSINESS PURPOSE

There must always be a legitimate business purpose to process personal data and it should be carefully considered whether such legitimate business purpose covers all data processing activities.

The legitimate business purpose is the primary purpose for a specific instance of processing personal data. Any secondary purposes for data processing (such as statistical analysis) must be closely aligned to the primary legitimate business purpose.

Legitimate business purposes can be different depending on whether the personal data being processed is that of:

- Employees (including their dependents, former employees and job applicants) and other members of staff; or
- Customers, suppliers and other business partners.

3.1 Legitimate business purposes for processing employee personal data and employee sensitive personal data:

There are defined legitimate business purposes for processing employee personal data:

- Human resources and personnel management;
  Examples: preparation, performance or termination of employment contracts or any other contract or relationships; recruitment or outplacement; compensation and benefits; taxes, social security contributions, pensions and similar entitlements; career and talent development, performance evaluations and training; travel and expenses; leave and other absences; security and employees communications.

- Organisation and management of the business;
  Examples: financial management, asset management, work scheduling, time recording, employees surveys, mergers and acquisitions, implementation of controls, creating and managing employees directories, management reporting, analysis, internal audits and investigations.

- Health, safety and security; and
  Examples: protection of an individual's life, health or vital interests, occupational health and safety, protection of Shell assets and employees, authentication of individual status and access rights.

- Legal or regulatory compliance.
  Examples: compliance with legal or regulatory requirements including investigations, litigation and defence of claims.

Where processing of employee personal data or sensitive personal data is not covered by one of the legitimate purposes listed, but it is required or permitted by local law, approval of the Head of Human Resources or external legal counsel must be sought before such data is processed.

2.2 Legitimate business purposes for processing personal data of customers, suppliers or business partners:

There are defined legitimate business purposes for processing personal data of customers, suppliers or business partners:

- Business execution;
  Examples: researching, developing and improving products or services; concluding and executing agreements; recording and settling services, products and materials to and from a NFC company; managing relationships and marketing e.g. maintaining and promoting contact with existing and prospective customers, account management, customer service, and development, execution and analysis of market surveys and marketing strategies.

- Organisation and management of the business;
  Examples: financial management, asset management, mergers, acquisitions, implementation of controls, management reporting, analysis, internal audits and investigations.

- Health, safety and security; and
  Examples: protection of an individual's life or health, occupational safety and health, protection of assets and people, authentication of individual status and access rights.

- Legal or regulatory compliance.
  Examples: Compliance with legal or regulatory requirements including investigations, litigation and defence of claims.

Sensitive personal data of customers, suppliers or business partners may only be processed in specific limited circumstances or where required by law and Tausi's specific privacy guidelines and regulations.

4. COMPLETING A PRIVACY IMPACT ASSESSMENT

The Privacy Impact Assessment process must be followed when processing personal data in IT systems.

A PIA is an important tool for documenting accountability, demonstrating compliance with this policy, legal requirements

Business and Functions must:

- Initiate the PIA process and, where it has been determined that one is required, complete the PIA, before processing personal data.

  The PIA process will assist Business and Functions to meet their personal data protection responsibilities by ensuring that:

- Processing of personal data is for a legitimate business purpose;

- Personal data collected is used only for the intended purpose and is not excessive for this state purpose;

- Data private risks to individuals are identified and assessed, with agreed controls implemented;

- Privacy notices are developed and communicated;

- Consent, where relied on or required, meets legal requirements and conditions;

- Mechanisms for responding to individual requests within specific time limits have been implemented;

- Any local data privacy laws have been considered and followed where local requirements are stricter than this policy; and

- Personal data that are records are retained and disposed of in accordance with retention requirements or for personal data that is not a record that the personal data disposal plan is defined and implemented .

5. ENSURING THAT PERSONAL DATA IS ACCURATE AND RELEVANT

All personal data processed by Tausi must be relevant and limited to that which is strictly necessary to achieve the legitimate business purpose. Personal data must not be collected or kept “just in case” a use for the data can be found in the future.

Personal data must be accurate, and it must be kept up to date. All reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay. All requests from individuals to update their personal data must be promptly addressed.

Businesses and Functions must:

- Ensure that the personal data collected is not excessive for the business purpose;
- Personal data that are records are retained disposed of in accordance with company requirements.
- Build mechanisms into systems or processes that facilitate timely data updates by individuals, such as self-serve portals.

6. PROTECTING PERSONAL DATA IN TAUSI'S CUSTODY OR CONTROL

Personal data must be protected from misuse, accidental, unlawful or unauthorised access, disclosure, corruption, destruction, loss, unavailability or acquisition.

The methods of protecting personal data must include physical measures, for example, restricted access to file rooms; limiting access on a 'need-to-know' basis and privacy training for staff, and technological measures, including adding a password to attachments containing personal data which are sent by email.

Businesses and functions must:

- Ensure processes and systems where personal data is processed are identified and those systems are registered in the Tausi repository;
- Implement required access and loss prevention controls to protect personal data.
- Implement all available protection capabilities for end-user computing, and ensure that end-user computing is only used for processing personal data where there are no alternative approved applications or tools that can be utilised.
- Ensure that staff who have access to personal data only have access to the information they need to do their job.
- Ensure that all third parties engaged by Tausi to process personal data have executed the required data privacy agreements.
- Assess whether business and IT control remain adequate when there is a change to a processing operation or system; and
- Regularly assess systems and processes to ensure that the personal data has been deleted according to its disposal plan.

7. SAFEGUARDING PERSONAL DATA TRANSFERRED TO, OR PROCESSED BY, A THIRD PARTY

Personal data must be safeguarded and protected by implementing the required contract clauses to ensure that the third party meets the minimum requirement of local privacy laws.

When Businesses or functions engage third parties to process personal data. Tausi is responsible for ensuring that the personal data is safeguarded and adequately protected. This applies equally to personal data processed by a third party on behalf of Tausi or to any personal data transferred to a third party by Tausi.

Third parties can be either:

- Third party data controllers, who process personal data in an independent manner and determine the purpose and manner of the processing activity for their own needs e.g, health insurers, car lease companies etc.
- Third party data processors;

8. INFORMING INDIVIDUALS THROUGH PRIVACY NOTICES

Every individual whose personal data is processed by Tausi must be adequately informed about such processing. There must be a clear explanation in a concise, transparent and easily accessible manner, of what individuals can expect to happen with their personal data.

Being transparent and providing accessible information to individuals about how Tausi will use their personal data is a key element of data privacy laws. This information is included in a privacy notice accessible and communicated at the time of collecting personal data.

9. COUNTRY SPECIFIC DATA PRIVACY LAWS AND REGULATIONS

It is imperative that the country in which registered companies are operating within data privacy laws and regulations are enforced and adhered to at all times.

10. REPORTING BREACHES OR SUSPECTED BREACHES OF PERSONAL DATA

Tausi must report breaches of personal data to regulatory authorities within a very short period of time, in line with privacy laws.

A data privacy breach is an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

11. POLICY UPDATE

This policy will be reviewed and updated annually by Group Human Resources. The policy can be found on the Tausi IMS System, or you can request it from your Human Resources Department.

12. POLICY QUERIES

Please refer queries relating to the Data Privacy Policy to:

Stella Molenaar	Group Head of Human Resources	Stella.molenaar@newforests.earth