Huhtamaki

GROUP DATA PRIVACY POLICY

Date issued	November 11, 2015
Approved by	Global Executive Team
Mgmt responsibility	Global Ethics and Compliance
Version	2.0
Version created	October 16, 2023

Huhtamaki

GROUP DATA PRIVACY POLICY

1 Purpose

Huhtamäki Oyj, together with its subsidiaries, associated companies, and other affiliates ("Huhtamaki" or "Group"), is committed to complying with all applicable data protection laws and regulations in safeguarding the data privacy of its employees, customers, suppliers, and other stakeholders. Compliance with applicable laws and regulations is an essential element of Huhtamaki's responsible business conduct. Further, non-compliance can have serious negative consequences for Huhtamaki, including criminal liability, significant administrative fines, and severe damage to reputation and shareholder value.

The purpose of this Group Data Privacy Policy ("Policy") is to enhance group-wide understanding of principles of data privacy, and to outline the key requirements when processing personal data.

2 Scope

This Policy is applicable to all Huhtamaki companies and employees, members of the management, officers and directors, as well as parties acting on Huhtamaki's behalf, such as agents and consultants. The Policy may be complemented by other documents and instructions containing more detailed guidance.

In some countries it may be necessary or desirable to adopt local policies or guidelines that are stricter or more detailed than this Policy, and that may be done in co-operation with Global Ethics and Compliance. These local policies and guidelines must always provide at least the same level of protection for personal data as this Policy.

Failure to comply with this Policy may result in disciplinary actions, including termination of employment. Additionally, since many aspects of this Policy are legally mandated, violations may expose individuals to criminal charges, obligation to compensate for damages, and other civil penalties.

3 Our data protection principles

At Huhtamaki, we process personal data in lawful, fair, and transparent manner.

> **Personal data** means any information that can be used to identify an individual either directly or indirectly, such as name, email address, identity number, location data or photo. Sensitive personal data is a category of personal data that, due to its sensitivity, requires specific grounds for processing. Sensitive personal data includes information such as ethnic origin, religion, and health status.
>
> **Processing** of personal data means any operation (automated or manual) performed on personal data, whether in electronic systems and files, or manually on paper documents, if such documents form a part of structured filing system.

Huhtamaki

Definition is broad and contains actions such as collecting, storing, accessing, using or sharing.

At Huhtamaki, personal data shall be processed only for specific, justified, lawful, and well-defined purposes, and the need of processing shall be reviewed at regular intervals. To meet the requirement for transparency, the procedures are to be communicated clearly to the individuals whose data is being processed (data subjects).

At Huhtamaki, we only process personal data for purposes that are necessary for our business (*purpose limitation*).

The necessary purpose shall be defined prior to the collection of the data. The purpose limitation principle means that personal data cannot be collected "just in case" or for purposes to be defined in the future.

Personal data is to be used only for the purpose it was collected for. Using personal data for any other purpose is allowed only if such use is still compatible with the purpose for which the personal data was initially collected for.

At Huhtamaki, we limit the data to what is required, and keep it only for as long as it is necessary (*data minimization and storage limitation*).

The amount and type of personal data used shall always match the pre-defined purpose for processing it. Whenever possible, aggregated and anonymous data is to be used instead of personal data. The data shall be stored only for the intended purpose or as required by applicable laws and regulations.

Huhtamaki is responsible for the personal data also when it is handled by external parties, such as tax authorities, IT service providers, or payroll processors. Personal data can be shared with external parties only for legitimate business purposes or to the extent required by law. Before sharing any data, it is necessary to ensure that disclosing is legal, assess related risks and impacts, and have appropriate contractual safeguards in place.

At Huhtamaki, we keep the personal data accurate and up to date (*data accuracy*).

Accuracy of personal data is guaranteed by taking appropriate steps, such as conducting regular checks and requesting updates. If any mistakes in personal data are discovered, they shall be corrected promptly. It is the responsibility of every employee to keep their personal data up to date.

At Huhtamaki, we protect confidentiality, integrity, and availability of personal data.

Huhtamaki

Confidentiality, integrity, and availability are safeguarded through appropriate technical and organizational measures. These measures shall cover the whole lifecycle of personal data and ensure an appropriate security level.

At Huhtamaki, we consider data protection from the beginning to the end of the processes (*privacy by design and by default*).

Data protection shall be considered when developing, designing, selecting, and using services, products, and applications that involve the processing of personal data. When planning a new project, IT-system procurement, or other processing activities with possible data privacy implications, privacy features like user consent options and data encryption shall be made part of the initial design process right from the beginning.

At Huhtamaki, we are responsible for demonstrating compliance with the data protection principles (*accountability*).

Huhtamaki is responsible for demonstrating compliance with data protection principles through appropriate policies and procedures, and by maintaining records of all processing activities. When planning or performing personal data processing, relevant documentation for demonstrating accountability shall be created and maintained.

4 Risk-based approach

Huhtamaki follows a risk-based approach to data protection. This means that the protective measures need to correspond to the risk level associated with data processing activities in question. Accordingly, the risks relating to the processing of personal data always need to be assessed prior to such processing starts e.g. by conducting a data processing impact assessment. Risk assessments must be carried out from the perspective of the data subject.

5 Data subjects' rights

Huhtamaki respects data subjects' rights with regards to their personal data, including right of access, rectification, erasure, consent withdrawal, data portability, objection, and restriction of processing. The data subjects' rights shall be taken into account when planning any personal data processing activities, and the relevant information and instructions about data subjects' rights shall be given to the data subjects in question in a clear, transparent, and easily accessible form.

6 Personal data breaches

A personal data breach refers to a security incident where personal data is unintentionally or unlawfully compromised, leading to its destruction, loss, alteration, unauthorized disclosure, or unauthorized access. Examples of personal data breaches include security breaches in computer networks or systems, the loss of devices like computers, phones, or USB drives, and the leakage of confidential documents.

Huhtamaki

Legislations in different countries include various notification requirements related to personal data breaches. For example, when it comes to personal data originating from the EU/EEA area, Huhtamaki is obligated to report specific types of personal data breaches to the relevant supervisory authority without unnecessary delay and no later than 72 hours after becoming aware of the breach.

To secure that these notification requirements can be fulfilled, all employees are expected to pay attention to possible data breach incidents and report any possible breach immediately and in any case within 12 hours, as instructed on Huhtamaki intranet (Huhtamaki Hub).

7 Roles and responsibilities

Each employee is responsible for acting in accordance with this Policy and the related instructions.

Leadership teams at global, segment, and local levels are responsible for ensuring that this Policy is fully implemented in their field of responsibility.

Global Executive Team is responsible for ensuring compliance with applicable data protection law and regulations, and implementation of this Policy through:

- allocating adequate resources and
- taking appropriate action, if breaches of applicable law and regulations, this Policy, or the related instructions are suspected and/or identified.

Global Ethics and Compliance manages this Policy and, together with Information Security and Legal, assists in its interpretation and practical application.

8 Breaches against the policy – Speak up

Any employee who suspects violations of this Policy or related instructions is expected to speak up and report the issue to their manager, over manager, local HR, Global Ethics & Compliance or through Huhtamaki Speak Up channel as described in the Huhtamaki Code of Conduct. Huhtamaki does not accept any form of retaliation against someone who speaks up or expresses concerns in good faith.

9 Further Information

Further information, documentation, and instructions are available on Huhtamaki Hub. You may also contact Global Ethics and Compliance, Legal or Information Security for further advice.