Policy

DKSH Group Data Protection Policy

Version:	1.1
Effective date:	June 22, 2018
Approved by:	CEO
Issued by:	Corporate Legal
Distribution:	DKSH Group

Supersedes and replaces all prior versions as from the effective date.

DKSH Holding Ltd.
Wiesenstrasse 8, P.O. Box 888, 8034 Zurich, Switzerland
Phone +41 44 386 7272, Fax +41 44 386 7282, www.dksh.com

Table of contents

1. General

DKSH purports to comply with all applicable data protection rules when processing personal data (e.g. data related to customers, suppliers and employees). As such, DKSH is committed to respect the personality rights and privacy of each data subject.

As a Group that operates around the globe, DKSH uses various systems to process data and to exchange data between DKSH companies and with third parties. The mutual provision of data-processing services also entails the exchange of personal data. Therefore, it is necessary that personal data are carefully processed.

2. Purpose

The purpose of this DKSH Group Data Protection Policy ("DPP") is to establish common data protection principles for the protection of personal data within DKSH in line with the General Data Protection Regulation of the European Union ("GDPR"). Where local law is stricter than the principles set out in this DPP, these laws shall take precedence over the principles set out in this DPP and must be complied with.

3. Scope

This DPP covers all personal data that DKSH collects, shares or uses in any way. It applies to all DKSH Group (as defined from time to time in the DKSH Annual Report) companies (collectively, DKSH, individually, DKSH company) and their employees.

Where personal data are processed on DKSH's behalf by third parties (see Clause 5.5), appropriate measures shall be taken to ensure compliance by said third parties with the principles set forth in this DPP.

4. Definitions

For the purpose of this DPP, the following definitions apply:

Data subject means the identified or identifiable natural person (in certain jurisdictions, such as Switzerland, also legal persons) to whom personal data relates; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity (including a passport number, a social security number, a code in combination with other information). Data subjects can be (among others) employees, customers or third parties, contractors, sole proprietors or vendors.

Personal data shall mean any information that relates to an identified or identifiable natural person whether the person can be identified directly, for example through a name, an e-mail address or a photograph, or indirectly, for example through a passport number, a social security number, the business function, or a code in combination with other information, including all such data kept on file in systems such as CRM, ERP, etc. In certain jurisdictions, personal data may include IP addresses or data relating to legal persons.

Processing shall mean any operation or set of operations performed on personal data, including but not limited to collection, recording, storage, alteration, analysis, use, transmission, combination, blocking, erasure and destruction.

5. Principles

All personal data must be processed lawfully and in a fair manner. In particular, the following principles apply:

5.1 Lawfulness

5.1.1 Justifications

Personal data may only be collected and processed if at least one of the following applies:

- The data subject has given consent. Note that:
  - where processing is based on the consent of the data subject, data subjects must have been given a genuine opportunity to exercise a choice about such processing. This means that their consent must be freely given, specific and that each data subject has been fully informed about the use of her/his personal data
  - in certain cases, processing without the consent of the data subject is prohibited by applicable law
- Processing is necessary for the performance of a contract to which the data subject is a party
- Processing is necessary for compliance with a legal obligation, or
- DKSH is pursuing a legitimate interest, except where such interest is overridden by the interest of the data subject concerned

For further guidance on the requirements i) on legal justifications that can be relied on and ii) on obtaining consent, please refer to the "Guideline on Legal Justifications for Collecting and Processing Personal Data" and the "Guideline on Notice and Consent".

5.1.2 Transparency

Persons whose personal data are being collected must be informed of and provide their consent to, at a minimum, the following:

- The fact that their data are being collected and processed
- The purposes for which the data are being processed
- The category (type) of data being collected and processed, and
- The persons that might have access to the data and why

The information provided to the data subject must be:

- Concise, complete, transparent, and easily accessible
- Written in clear and plain language; and
- Free of charge

For further guidance on how to provide a privacy notice, please refer to the "Guideline on Notice and Consent".

5.1.3 Proportionality

The amount of personal data collected must be limited to what is necessary to fulfill the identified purpose. Necessity may be assessed by asking the following questions: "Do I really need this data to fulfill the purpose?" "Can I fulfill the purpose without the data?" Whenever possible, data should be pseudonymized or anonymized. For further guidance and advice on anonymization techniques, consult the FAQ to this DPP and ask your Data Protection Officer ("DPO")[1] or Privacy Coordinator.

The principle of proportionality requires, inter alia, that:

- Processing more personal data than **necessary** to attain the legitimate purpose of processing such personal data is forbidden.

[1] In countries that have a DPO (i.e., at the date of first issue of this policy: Germany, Korea, New Zealand, Singapore).

- Disclosure, transfer, access granting or publication of personal data within DKSH or vis-à-vis third parties is only permissible if there is **a sufficient justification** to do so and only on a strict "need-to-know basis" to accomplish the purpose for which the personal data was collected.
- According to the principle of data minimization, personal data must be processed only to the extent compatible with the purpose for which they were collected (as indicated to the data subject at the time of collection). **Subsequent changes of purpose** are acceptable only:
  - If reasonably expected by the person concerned, or
  - If the person concerned has given her/his consent to the change of purpose, or
  - If otherwise permitted by law

  Reasons for changing the purpose must be documented and checked for legal admissibility by the DPO, Privacy Coordinator or Global Privacy Lead

- Subject to legal provisions that require a longer retention period, personal data are to **be stored no longer than is necessary** to accomplish the purposes for which they were collected or processed unless they are anonymized

5.2 Accurateness
Personal data must be accurate and up-to-date at all times. Personal data that are no longer accurate or complete must be corrected or deleted

5.3 Data Security
Personal data must be protected against accidental loss or destruction, unauthorized copying, modifications, access, disclosure or processing, through adequate technical and organizational measures as defined in the "DKSH Group IT Security Policy" and applicable laws

Please reach out to Country IT to put appropriate safeguards in place which ensure compliance of all data processing systems employed by you with the requirements of accuracy, up-to-datedness and security.

5.4 Documentation of Data Processing Activities
DKSH is responsible and accountable for providing evidence of compliance of all data processing with data protection laws. This presupposes:
- Knowledge/complete listing of all personal data held by DKSH
- Clear understanding of where, how and why such data is used
- Documentation of all processing activities and systems which is up-to-date at all times

Please consult the "Guideline for Documenting Processing Activities" and ask your DPO or Privacy Coordinator for further guidance.

5.5 Outsourcing
The engagement of a service provider outside the DKSH Group, who processes data on behalf of DKSH (such as e.g. payroll providers) is subject to the following requirements:
1. Understanding of what personal data such service provider may need to access and process in order to provide the services
2. Verification that the service provider is able to adequately protect the data and to comply with all applicable privacy laws
3. Written agreement with the service provider, stipulating all relevant data protection and security obligations

For further guidance, consult the “Guideline on Outsourcing”.

5.6 Cross-border transfer
The GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an “adequate” level of personal data protection. In the absence of an adequacy decision, personal data may in principle only be transferred to third countries (i) if the controller or processor exporting the data has himself provided for “appropriate safeguards” (such as by inclusion of EU Standard Contractual Clauses for the Transfer of Personal Data in contracts or use of binding corporate rules), and (ii) on the condition that enforceable data subject rights and effective legal remedies are available in the given country.

Please refer to the “Guideline on Cross-border Data Transfers” or ask your DPO, Privacy Coordinator or Legal for further guidance.

5.7 Rights of data subjects
DKSH must be aware of the privacy rights of individuals. In particular, DKSH must meet access requests of individuals within one month by (a) confirming if it processes an individual’s personal data, and if so, (b) providing access to the personal data and (c) other supplementary information. Where appropriate, data subjects also have a right to require that data be corrected, blocked or deleted, as set out in the “Guideline on Privacy Rights”.

6. Implementation, monitoring and enforcement by DKSH companies and DKSH employees
6.1 DKSH companies
Each DKSH company shall explicitly adopt, implement, monitor and enforce this DPP and other pertinent internal guidelines and procedures (including the agreements allowing a lawful cross-border transfer of data, see 5.6 hereabove) in compliance with local laws and regulations by providing its employees with appropriate information as well as guidance and training.

In particular, each DKSH company is to implement the **technical and organizational measures necessary to ensure the security of personal data**. In particular, personal data are to be protected against unauthorized disclosure and any form of unlawful processing. The measures implemented must ensure a level of security appropriate to the nature of the data to be protected and the risks arising from processing the data.

Each DKSH company shall conduct periodic reviews and audits, where appropriate, to ensure and demonstrate compliance with this DPP, other pertinent internal guidelines and procedures as well as applicable privacy laws.

6.2 DKSH employees
DKSH employees whose activities and responsibilities involve the processing of personal data are accountable and responsible for processing such personal data in strict adherence to the applicable laws, the data protection principles set forth in this DPP and other pertinent internal guidelines and procedures.

Important: Each employee must immediately **report any suspected data security breach** (e.g. the loss or deletion, unauthorized access to or disclosure of personal data) of which they become aware by contacting Country IT, as set forth in the DKSH Group IT Security Policy respectively the corporate IT Security Incidents Management Process.

6.3 Third-party processing of personal data

The relevant DKSH company shall satisfy itself that the contracted third party (see Clause 5.5) is processing the data properly and that it is complying with the principles set forth in this DPP and other pertinent internal guidelines and procedures as well as applicable laws. If, at any time, a third party is determined to be unable to ensure the adequate security of personal data, the collaboration shall be terminated immediately.

6.4 DKSH Group Data Protection Organization

The Group Data Protection Organization consisting of the Global Privacy Lead, Global Business and Functional Privacy Coordinator, DPOs, as well as Country Privacy Coordinators shall be responsible for implementing and operationalizing this DPP, other pertinent internal guidelines and procedures and applicable laws, as well as for providing subject matter expertise, guidance and training to the business functions, management and employees.

7. Violations

All directors, managers, employees and associated persons shall strictly comply with this DPP and other pertinent internal guidelines and procedures, as well as applicable laws. Any violation of such standards will lead to an investigation and appropriate disciplinary measures up to and including termination for cause, and, in warranted cases, legal action.

8. Roles and responsibilities

This Policy is owned by Corporate Legal. It will be reviewed and amended from time to time to reflect changes in applicable privacy laws and DKSH's business requirements

References

- FAQ about the Group Data Protection Policy
- Guideline on Legal Justifications for Collecting and Processing Personal Data
- Guideline on Notice and Consent
- Guideline on Privacy Rights
- Instructions for Documenting Processing Activities
- Guideline on Outsourcing
- Guideline on Cross-border Data Transfers
- DKSH Group IT Security Policy