



**H U G O B O S S**

**Data Protection Organization Policy**

Policy

## Contents

<b>1</b>	<b>Purpose</b>	<b>4</b>
<b>2</b>	<b>Territorial Scope</b>	<b>4</b>
<b>3</b>	<b>Responsibility at the Level of Group Companies</b>	<b>4</b>
3.1	Controllers	4
3.2	Definition of Responsibilities	5
3.3	Duty of Notification and Training	5
<b>4</b>	<b>Responsibility for Data Protection within the HUGO BOSS Group</b>	<b>5</b>
4.1	Data Protection by the Management	5
4.2	Data Protection by Employees	5
4.3	Data Protection at the Departmental Level	6
4.4	Data Protection Personnel	6
4.5	Data Breach Emergency Response Team	6
<b>5</b>	<b>Data Protection Officer of HUGO BOSS AG</b>	<b>7</b>
5.1	Legal Obligation	7
5.2	Duties	7
5.3	Consultation and Access to Information	8
5.4	Qualifications and Conflicts of Interest	8
5.5	Points of Contact, Confidentiality	8
5.6	Appointment and Independence	8
5.7	Reporting	8
<b>6</b>	<b>Local Data Protection Contacts (GDPR subsidiaries)</b>	<b>9</b>
6.1	Local Data Protection Contacts	9
6.2	Responsibility	9
6.3	Enquiries from Public Authorities	9
6.4	Point of Contact	9

<b>7</b>	<b>Group Data Protection Officer</b>	<b>9</b>
<b>8</b>	<b>Reporting</b>	<b>10</b>
<b>9</b>	<b>Departmental Level</b>	<b>10</b>
9.1	Self-Audits	10
9.2	Points of Contact	11
9.3	Data Protection from the Outset	11
9.4	Documentation of Changes	11
<b>10</b>	<b>Risk Management</b>	<b>11</b>
<b>11</b>	<b>Application / Point of Contact</b>	<b>12</b>

## 1 Purpose

The purpose of this Data Protection Organization Policy (hereinafter referred to as the “Policy”) is to put in place organizational processes and structures to achieve and secure minimum standards for compliance with data protection legislation by HUGO BOSS within the territorial scope of this Policy.

## 2 Territorial Scope

This **Policy applies equally to all companies of the HUGO BOSS Group located within the territorial scope of the General Data Protection Regulation of the European Union** ([GDPR](#)). The Policy and the provisions contained therein are consistent with the HUGO BOSS Code of Conduct. They are binding upon all employees and must be strictly observed.

In the event that provisions of local law contain other requirements concerning the organization of data protection and the authority of persons responsible for implementation and monitoring, such provisions will take precedence.

The Data Protection Officer of HUGO BOSS AG and the Central Legal Department must be consulted in advance in the case of any deviations.

## 3 Responsibility at the Level of Group Companies

### 3.1 Controllers

The Management of every Group company located within the territorial scope of the GDPR is responsible for implementation of this Policy as well as for the deployment and maintenance of suitable structures to ensure compliance with the provisions of data protection legislation.

Controllers must prescribe suitable technical and organizational measures to ensure and demonstrate that personal data are processed in compliance with this Policy and legal requirements. Such instructions must be implemented by the persons instructed and chosen to do so.

Provisions of national law that are not consistent with this Policy are to be taken into account and the Data Protection Officer of HUGO BOSS AG and the Central Legal Department consulted in advance to determine the course of action to be taken.

### **3.2 Definition of Responsibilities**

The Management must clearly define the duties and responsibilities of those involved in the processing of personal data and notify relevant employees, managerial personnel and any third parties accordingly (hereinafter referred to as “employees”). Fulfillment of such duties and responsibilities must be regularly monitored and documented.

Remedial measures must be taken immediately in the case of breaches and the measures taken documented.

### **3.3 Duty of Notification and Training**

It is the responsibility of the Management to ensure that employees who process personal data are notified accordingly and aware of their duties under the law. HUGO BOSS AG may assume responsibility for the notification of employees.

The Management must provide special data protection training when necessary and document the fact that such training has been provided. The Management may assign responsibility for notification, building awareness and training of employees to the Data Protection Officer or Data Protection Contact.

## **4 Responsibility for Data Protection within the HUGO BOSS Group**

### **4.1 Data Protection by the Management**

The Managing Board of HUGO BOSS AG and the Management of each of the Group companies agree to provide an adequate level of data protection as required by applicable policies and laws in place and ensure compliance with such policies and laws.

### **4.2 Data Protection by Employees**

In the case of the Group companies of HUGO BOSS, data protection begins at the lowest level and compliance by each individual employee is mandatory. The Group’s

Code of Conduct, the Data Protection Policy and many different in-house corporate guidelines go beyond what is prescribed by law and require that employees treat personal data responsibly in connection with their activities.

### **4.3 Data Protection at the Departmental Level**

The individual departments play an important role in the context of data protection. Specific individuals are assigned responsibility for data protection at the level of the various departments to ensure dissemination of information and the exchange of information with the departments. These individuals are also the points of contact for the Data Protection Officer of HUGO BOSS AG and Data Protection Contacts.

### **4.4 Data Protection Personnel**

In addition to the members of the Management responsible for data protection, the HUGO BOSS Group has also created permanent positions that are assigned responsibility for monitoring and compliance with the provisions of data protection legislation.

These include the following:

- Data Protection Officer of HUGO BOSS AG
- Local Data Protection Contacts at the level of the subsidiaries

Additional such positions may also be created or filled by HUGO BOSS AG.

### **4.5 Data Breach Emergency Response Team**

A Data Breach Emergency Response Team is formed in accordance with the provisions contained in the Personal Data Breach Policy depending on the needs of the specific occasion. Permanent members include the Data Protection Officer of HUGO BOSS AG (or his or her alternate), the Compliance Officer (or Director of Legal & Compliance) and the Head of the Legal Department (or his or her alternate), who may appoint further members (e.g., from any of the various departments, IT) in the case of the occurrence of specific types of personal data breaches.

## **5 Data Protection Officer of HUGO BOSS AG**

### **5.1 Legal Obligation**

HUGO BOSS AG is under an obligation to appoint a Data Protection Officer. The rights, obligations and duties of the Data Protection Officer are defined in the following sections.

### **5.2 Duties**

The Data Protection Officer of HUGO BOSS AG monitors compliance with the provisions of data protection legislation for Germany and Austria. The Data Protection Officer of HUGO BOSS AG is the point of contact for all questions regarding data protection legislation for all other subsidiaries that fall within the territorial scope of the GDPR.

At the very least, the duties of the Data Protection Officer include the following:

- (1) to advise and inform the Management and employees as regards their obligations under the provisions of data protection legislation and internal data protection policies;
- (2) to monitor compliance with the provisions of data protection legislation and internal data protection policies;
- (3) to carry out risk-oriented assessments of selected processes on a sample basis against the background of data protection legislation and internal data protection policies;
- (4) to monitor the strategies of the Management for the protection of personal data (including assignment of responsibilities, building of awareness and training of employees involved in processing operations and the corresponding audits);
- (5) to provide advice in connection with the data protection impact assessment and monitoring of implementation in the case of enquiries;
- (6) to cooperate with the supervisory authority;
- (7) to function as the point of contact for the supervisory authority for all issues related to processing.

The duties of the Data Protection Officer of HUGO BOSS AG involve putting in place appropriate precautions by taking into account the nature, scope, surrounding circumstances and purposes of processing.

### **5.3 Consultation and Access to Information**

The Data Protection Officer of HUGO BOSS AG will be properly consulted on a timely basis on all issues related to the protection of personal data.

The Data Protection Officer of HUGO BOSS AG will be provided with the resources and the access to personal data and processing operations required to fulfill his or her duties. The Data Protection Officer of HUGO BOSS AG will receive suitable training to maintain the level of his or her professional qualifications.

### **5.4 Qualifications and Conflicts of Interest**

The Data Protection Officer of HUGO BOSS AG must have appropriate professional qualifications and specialized knowledge in the area of data protection legislation and practice. The Data Protection Officer of HUGO BOSS AG may assume further duties and obligations as long as such activities do not result in any conflict of interest. The Management will ensure that this is the case.

### **5.5 Points of Contact, Confidentiality**

Data subjects may consult the Data Protection Officer of HUGO BOSS AG on all issues pertaining to the processing of their personal data and the exercise of their legal rights pursuant to the applicable provisions of law.

The Data Protection Officer of HUGO BOSS AG is bound to a duty of confidentiality in connection with the fulfillment of his or her duties.

### **5.6 Appointment and Independence**

In order to achieve a certain continuity and facilitate familiarization with his or her duties, the Data Protection Officer of HUGO BOSS AG will be officially appointed for a period of at least two years by the Management. Deviations are permissible. The possibility of automatic extension of this term is excluded.

### **5.7 Reporting**

The Data Protection Officer of HUGO BOSS AG reports directly to the Director of Legal & Compliance and regularly briefs the Managing Board of HUGO BOSS AG.



## **6 Local Data Protection Contacts (GDPR subsidiaries)**

### **6.1 Local Data Protection Contacts**

Each Group company that falls under this Policy designates a local Data Protection Contact, who should have suitable qualifications and specialized knowledge in the area of data protection legislation and practice. The Data Protection Officer may not be sanctioned for the performance or his or her duties. Local Data Protection Contacts report directly to the Management.

Local Data Protection Contacts may also assume other duties and obligations as long as such activities do not result in any conflict of interests. The Management will ensure that this is the case.

### **6.2 Responsibility**

The local Data Protection Contacts are responsible for compliance with the provisions of data protection legislation pursuant to the HUGO BOSS policies and legal requirements. The Data Protection Officer of HUGO BOSS AG may be consulted for advice.

### **6.3 Enquiries from Public Authorities**

The Data Protection Officer of HUGO BOSS AG must be notified without delay in the event that public authorities (in particular the supervisory authority) should contact the company in connection with data protection and request information. Further procedures are to be coordinated with the Data Protection Officer.

### **6.4 Point of Contact**

Local Data Protection Contacts are the points of contact for the employees of the subsidiaries and the Data Protection Officer of HUGO BOSS AG.

## **7 Group Data Protection Officer**

HUGO BOSS may appoint a Group Data Protection Officer. The Data Protection Officer of HUGO BOSS AG can also serve as the Group Data Protection Officer at the same time.

The following are the key duties of the Group Data Protection Officer:

- (1) to act as point of contact (support and advice) for local Data Protection Contacts at the level of the subsidiaries as regards questions concerning data protection legislation;
- (2) to coordinate data protection issues of Group-wide importance;
- (3) to handle coordination and cooperation with the competent supervisory authority;
- (4) to notify and provide the Managing Board of HUGO BOSS AG with information in the case of serious data protection breaches;
- (5) to report to the Managing Board of HUGO BOSS AG on the status of data protection at the Group level on a semi-annual basis.

The duties contained in sections (2), (4) and (5) will be assigned to the Data Protection Officer of HUGO BOSS AG if no Group Data Protection Officer is appointed.

## **8 Reporting**

Local Data Protection Contacts report to the Data Protection Officer of HUGO BOSS AG at least twice a year. Local Data Protection Contacts submit reports to the Data Protection Officer of HUGO BOSS AG on an ad hoc basis in cases to be defined by the Data Protection Officer. The Data Protection Officer of HUGO BOSS AG will specify the content, timing and scope of such reports.

The Management may decide to involve a Group Data Protection Officer.

## **9 Departmental Level**

### **9.1 Self-Audits**

In the case of certain departments, the processing of personal data is one of the most important activities. Legal and technical requirements as regards the applicable provisions of data protection legislation are to be taken into account from the very beginning if personal data are processed and/or processes are changed in the case of such departments.

“Privacy by design” at the time of determination of deployment of new processes as well as the use of “privacy by default” at the operational level play a decisive role in

terms of fulfillment of the legal and technical requirements for compliance with the provisions of data protection legislation.

## **9.2 Points of Contact**

The departments listed here must – and other departments may – designate a point of contact and alternate who are active in the respective operational areas:

- IT
- eCommerce
- CRM
- Human Resource
- Customer Service

The designated individuals are the points of contact for the Data Protection Officer of HUGO BOSS AG.

## **9.3 Data Protection from the Outset**

The various departments must take into account legal and technical requirements for processing personal data at the level of the initial design phase and/or when processes are changed.

## **9.4 Documentation of Changes**

The various departments are responsible for preparation of the required documentation of their processes that involve the processing of personal data. Additions and changes are to be documented and submitted to the Data Protection Officer of HUGO BOSS AG in advance for the purposes of evaluation and assessment in terms of data protection.

## **10 Risk Management**

Risk management and the corresponding reports are addressed in the HUGO BOSS Risk Report. Actual and legal risks are identified and their potential implications at the level of business processes assessed twice a year by local Data Protection Contacts.

The results of risk assessment are then forwarded to the Data Protection Officer of HUGO BOSS AG without delay. If possible, local Data Protection Contacts should propose measures to reduce or eliminate risks.

The results of risk assessment are to be documented and forwarded to Central Risk Management.

## **11 Application / Point of Contact**

This Policy will enter into force and effect on as of 25 May 2018.

Any questions regarding the implementation of this Policy should be addressed to the Data Protection Officer of HUGO BOSS AG.

Valid for: HUGO BOSS (HUGO BOSS AG and Subsidiaries under the GDPR)	Version: 1.0
Valid from: 25.05.2018	Status: released, valid
Approved by: Managing Board	