HUGO BOSS

Data Breach Complaint Policy

Table of Contents

1 Introduction

1.1 Background

"Data is the gold of the 21st century". This citation makes it clear that in the digital age each individual's data is an extremely valuable asset and, at the same time, one that is worth protecting. It is obvious that employees, customers, business partners and other third parties must deal responsibly with the data provided to them. This is also expected of them. HUGO BOSS too must meet these expectations and the new statutory data protection requirements.[1] These include processing the data provided in a professional manner, guaranteeing its security and effectively managing complaints in the case of data protection infringements.

1.2 Scope of the Policy

The overriding aim of the Data Breach Complaint Policy (hereinafter referred to as the "Policy") is to create transparency regarding the handling of complaints against data breaches (complaints) and the processing, assessment and possible notification of such complaints to the competent authority and the data subject(s) in accordance with predefined processes.

It covers all complaints against breaches of the data protection rules that are submitted by employees, customers, business partners or other third parties.

1.3 Application of the Policy

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.

[1] These include, inter alia, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) – hereinafter referred to as the GDPR.

2 Material scope

For the purposes of this Directive, the form in which the data is stored (on paper, on a data medium, in a database, in a filing system, etc.) and how the data breach occurred are irrelevant. Differences may, however, arise in connection with notification obligations and the competent supervisory authority (cf. section 7 "Determination of the existence of an obligation to notify the competent supervisory authority").

3 Definitions

For the purposes of this Directive, the following definitions apply:

- **Data subject** (Art. 4(1) of the GDPR)
  A data subject is every identified or identifiable[2] natural person whose personal data is affected by a data breach.

- **Data breach** (Art. 4(12) of the GDPR)
  A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **Personal data** (Art. 4(1) of the GDPR)
  Personal data means any information relating to an identified or identifiable natural person (see "data subject").

- **Main establishment** (Art. 4(16)(a) of the GDPR)
  Main establishment means as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in

[2] A natural person is considered **identifiable** if such person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

which case the establishment having taken such decisions is to be considered to be the main establishment.

- **Cross-border processing** (Art. 4(23) of the GDPR)
  Cross-border processing means either processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

4 Officeholders at HUGO BOSS

Data Protection Officer

The appointment, duties and function of the Data Protection Officer of HUGO BOSS AG are specified and described in the **Data Protection Organization Policy**.

Data Breach Emergency Response Team

The Data Breach Emergency Response Team must be assembled according to the kind of incident. The Data Protection Officer (or his representative), the Compliance Officer (or the Director of Legal & Compliance) and the Head of Legal Department are permanent members of the team. They may appoint additional team members (e.g. from the specialist departments, IT) for a specific data breach incident.

Controller

The controller is the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, each company is a controller and is represented by its management.

5 Complaints against data breaches

5.1 General handling of complaints against data breaches

Where complaints of data breaches are received by HUGO BOSS, they will be immediately investigated and analysed by defined persons or groups of persons and, if necessary, appropriate measures will be taken.

5.2 Ways of submitting complaints

Complaints about data breaches do not have to be made through any particular channel or be directed to a specific person.

The preferable way of submitting a complaint is for employees, customers, business partners or other third parties to either directly contact HUGO BOSS's Data Protection Officer or send an email to either datenschutz@hugoboss.de or privacy@hugoboss.com.

Any employee, customer, business partner or other third party may contact HUGO BOSS's external ombudsman, **Dr. Carsten Thiel von Herff** (ombudsman@thielvonherff.com), if they wish to report (also anonymously) a data breach or a suspected data breach.

5.3 Form of complaints

There are no formal requirements for lodging a complaint. Every complaint irrespective of whether it is submitted orally, in writing, openly, anonymously or in any other manner is of the same importance and will be followed up in the same manner.

6 General complaint-handling procedure

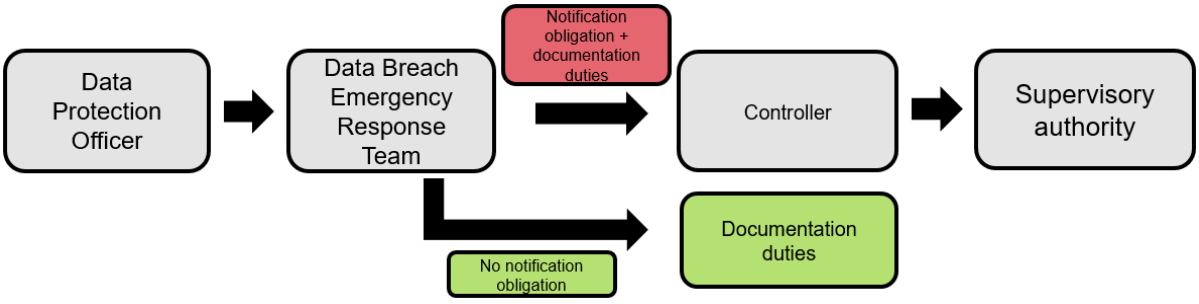
As soon as HUGO BOSS **receives or becomes aware of** a complaint about a data breach, irrespective of how and where this occurs, the following procedure must be followed:

- Top priority must be given to all complaints received about data breaches, including in particular reported breaches committed by data processors and

such complaints must be passed on, in their entirety, to HUGO BOSS's Data Protection Officer or, in his absence, his representative.

- The Officer must immediately record the complaint and inform the Data Breach Emergency Response Team. The team then takes over the further handling of the complaint and, if necessary, orders the implementation of emergency measures to minimise damage.
- If the Data Breach Emergency Response Team finds, while investigating the complaint, that
  - no obligation to notify the competent supervisory authorities regarding the data breach exists, the documentation duties contained in this Policy must be complied with. The controller will be fully informed in the next data protection report.
  - an obligation to notify the competent supervisory authorities regarding the data breach exists, the controller must be informed of this immediately. The controller makes the final decision on whether the data breach should be notified to the competent supervisory authorities and, where necessary, makes the notification. Compliance with the documentation duties contained in this Policy is mandatory.

Chart showing the course of the procedure:



Where an obligation to notify the competent supervisory authority exists, the notification and documentation must meet the requirements set forth in this Policy.

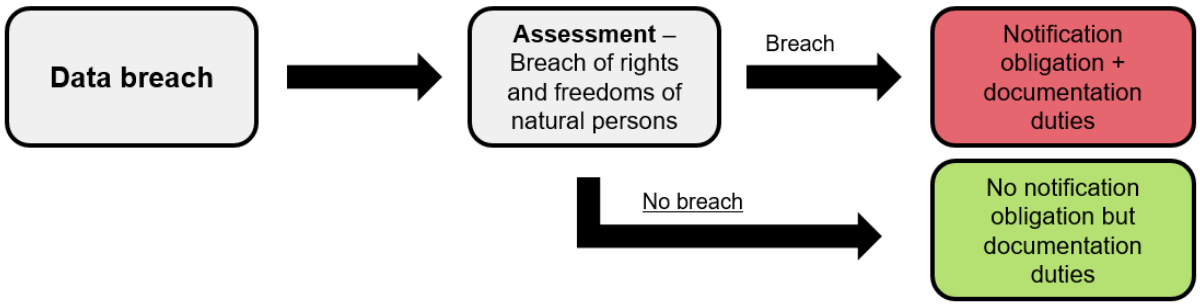
7 Determination of the existence of an obligation to notify the competent supervisory authority

In the event of a data breach – irrespective of the form in which the data is stored – HUGO BOSS may be under an obligation to notify the incident to the competent supervisory authority. The actual existence of notification obligations must be checked in each individual case of a data breach.

7.1 Existence or absence of a notification obligation

In the event of a data breach, HUGO BOSS is, **as a rule**, required to document and notify the incident to the competent supervisory authority. The information described below must be provided within the prescribed timeframe.

This does not apply in the case of incidents where the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In these cases, there are documentation duties in order to be able to provide the competent supervisory authority with evidence that the risks were properly assessed.



7.2 Assessment – risk to the rights and freedoms of natural persons

In order to decide whether not a breach notification obligation exists, the Data Breach Emergency Response Team must investigate and assess whether the data breach is likely to result in a risk to the rights and freedoms of natural persons.

No assessment is necessary in the following cases because the legislature deems a risk to the rights and freedoms of natural persons to exist in such cases.

When investigating and assessing a data breach, the Data Breach Emergency Response Team must be guided by the specific cases of breach that have been defined by law.

7.3 Documentation

In the event of a data breach, HUGO BOSS must document all facts relating to the breach, their effects and the remedial action taken. This applies in those cases where a notification obligation exists, but also in particular in those cases in which HUGO BOSS lawfully decides not to report a breach.

The documentation must contain at least:

- **Details of the nature, form and scope of the data breach**
  (insofar as possible with mention of the categories and the approximate number of data subjects concerned and the categories and the approximate number of personal data records concerned)
- **Details of the reasons for the assessment**
  (pursuant to the investigation requirements under section 7.2 "Assessment - risk to the rights and freedoms of natural persons")
- **No option for assessment because of the statutory examples**
- **The results of the evaluation of the likely risks** to the rights and freedoms of natural persons posed by the breach
- **A description of the likely consequences of the data breach**
- A description of the **measures taken or proposed** to eliminate the breach and, if applicable, measures to mitigate any disadvantageous effects
- **A record of the decision** reached by the Data Protection Officer or the Data Breach Emergency Response Team regarding whether an obligation to notify the competent supervisory authority exists
- **Details of any other special circumstances** in relation to the specific data breach

7.4 Which establishment has to make the notification?

If a reportable data breach is found to have occurred within the HUGO BOSS Group, it is necessary in each specific case to check which establishment has to report the breach and to check which supervisory authority is the authority to which the report of the breach must be made.

For these purposes, the nature and manner of the processing of personal data must be checked. If personal data are **only** processed in one establishment, then the competent supervisory authority in the country where the establishment is located must be notified. Where there is **cross-border** processing of data and a breach occurs, the competent supervisory authority of the main establishment (i.e. the lead supervising authority) is competent and the notification should be submitted to it.

Example: If data are processed by an establishment together with HUGO BOSS AG (main establishment), notification must, as a rule, be made only to the main establishment's supervisory authority, i.e. in Germany.

7.5 Competent supervisory authorities

If a data breach occurs which leads to a notification obligation, the competent supervisory authority must be informed.

7.5.1 Competent supervisory authority for the main establishment (HUGO BOSS AG)

The State Commissioner for Data Protection and Freedom of Information in Baden-Württemberg (Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg) performs the tasks of the supervisory authority in the case of data breaches during the processing of data which are or are intended to be stored[3] in a HUGO BOSS AG filing system. The notification of a data breach must be sent to:

[3] This includes the processing of data wholly or partly by automated means and the processing other than by automated means of data which form part of a filing system or are intended to form part of a filing system.

State Commissioner for Data Protection and Freedom of Information in Baden-Württemberg

P.O. Box 10 29 32

70025 Stuttgart

Germany

poststelle@lfdi.bwl.de

Phone: 0711/615541-0 / Fax: 0711/615541-15

7.5.2 Competent supervisory authorities for other establishments

The competent supervisory authorities for other establishments in the HUGO BOSS Group (excluding HUGO BOSS AG) within the territorial scope of the GDPR are listed in **Appendix 1** or they may be accessed via the following link: https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

7.6 Minimum content of the notification to the competent supervisory authority

If it is necessary to inform the competent supervisory authority of a data breach, the notification must contain the following information:

- **A description of the type of data breach**
  (insofar as possible with mention of the categories and the approximate number of data subjects concerned and the categories and the approximate number of personal data records concerned)
- **Name and contact details of the Data Protection Officer** or other contact point for further information
- A description of the **likely consequences** of the data breach

- A description of the **measures taken or proposed** to eliminate the breach and, if applicable, measures to mitigate any disadvantageous effects

Where the competent supervisory authorities have an online form for giving notification of personal data breaches, this should be used and the requested information inserted.

7.7 Time limit and form

In the case of a reportable data breach, the controller must report the breach to the competent supervisory authority without undue delay and where feasible, not later than 72 hours after having become aware of the breach and must also provide the authority with at least the information listed in section 7.5. If it is not feasible to report the breach to the competent supervisory authority within 72 hours, an explanation for failing to meet this deadline must be provided and additional information (pursuant to section 7.6 "Minimum content of the notification to the competent supervisory authority") must, without undue delay, be supplied as soon as it becomes available.

In order to comply with the time limit, the notification may be sent by e-mail or fax or submitted online using the notification form provided by the competent supervisory authority:

- **Main establishment (HUGO BOSS AG)**
  State Commissioner for Data Protection:
  https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/
- **Other establishments**

  You can use the following link to find the competent supervisory authorities and the relevant online notification forms.
  https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

The information submitted in the first two cases must be encrypted.

8 Communication of a data breach to the data subject and the complainant

8.1 Communication of a breach to the data subject

8.1.1 Principle

A data breach must be communicated to the data subject without delay if the breach is likely to result in a high risk to the data subject's rights and freedoms. The Data Breach Emergency Response Team must investigate and assess whether the data breach in a specific case is likely to pose a high risk to the rights and freedoms of the data subject. A record must be kept of the assessment and the conclusions reached in accordance with section 7.3.

8.1.2 Exceptions

No communication of a breach is necessary where one of the following conditions is fulfilled:

- The controller has implemented appropriate technical and organisational security measures, and those measures were applied to the data affected by the data breach. This includes in particular access control to personal data through encryption.
- The controller has taken measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.
- Communication would involve disproportionate effort.
  In such a case, there will instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. The public must be informed through advertisements, which are at least half a page in size, in at least two national daily newspapers. Other suitable measures which are equally effective in informing the data subjects may be used (e.g. press releases). The communication must be checked and approved by the HUGO BOSS Legal Department so as to avoid any detrimental effects.

8.1.3 Statutory criteria for weighing interests

A high risk to the rights and freedoms of data subjects exists pursuant to the guidelines and definitions prescribed by law. These are binding for HUGO BOSS.

8.1.4 Form of communication

The communication to the data subject must be written in clear and plain language and contain at least the following points:

- Nature of the data breach
- Name and contact details of the Data Protection Officer
- A description of the likely consequences of the data breach
- A description of the measures taken or proposed to eliminate the breach and, if applicable, measures to mitigate any disadvantageous effects

8.2 Notification of the complainant

The complainant in respect of a data breach will receive confirmation of the receipt of the complaint and will be informed of the results of the examination of the data breach and any measures adopted. This does not apply in the case of anonymous complaints which are not channelled through the ombudsman or complaints whose outcome has already been notified to the complainant in the complainant's capacity as a data subject.

Notification will be made within four weeks or at the latest upon conclusion of the complaint procedure.

9 Applicability and general contact persons

This Policy enters into force on 25 May 2018 and replaces the previous Emergency Plan for Data Breaches in the version of 3 July 2014.
Any employee, customer, business partner or other third party who has questions or suggestions may contact the HUGO BOSS Data Protection Officer.

Any employee, customer, business partner or other third party may contact HUGO BOSS's external ombudsman, **Dr. Carsten Thiel von Herff** (ombudsman@thielvonherff.com), if they wish to report (also anonymously) a data breach or a suspected data breach.

Valid for:	HUGO BOSS Group	Version:	1.0
Valid from:	25 May 2018	Status:	released, valid
Approved by:	Managing Board		