HAYS Working for your tomorrow

Information Sheet
"Obligation to Maintain Data Confidentiality"

Due to the responsibilities associated with your position in our company, you are obliged to maintain confidentiality with regard to personal data to which you gain access or of which you become aware in the course of your work. You are only permitted to process personal data to the extent and in the manner required to fulfil the tasks delegated to you. The relevant legal provisions require that personal data must be processed in a manner that ensures the data subjects' rights to confidentiality and integrity of their data. These provisions prohibit the unauthorised or unlawful processing of personal data as well as the intentionally or unintentionally violation of the processing's security in a manner which results in destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data.

Violations of the data protection regulations can be punished by a fine or imprisonment. If the data subject incurs a material or immaterial damage as a result of the unauthorised processing of his personal data, a claim for damages may arise. The violation of confidentiality and data protection regulations also constitutes a violation of contract obligations and can be punished accordingly.

This obligation remains valid after the termination of your Contract with our company.

Your general confidentiality obligations you are required to comply with are not affected by this Declaration of Confidentiality. You have to take note of the provisions which are attached to this Declaration of Confidentiality.

Should you have any questions, please do not hesitate to contact the company's data protection officer (see Privacy Policy) at any time.

The present selection of legal regulations should give you an overview of the data protection regulations. The presentation is exemplary and by no means complete. You can obtain further information on data protection issues from the company's data protection officer.

Chapter I of the GDPR
General provisions

Art. 4 (1), (2) and (12) of the GDPR
Definitions

For the purposes of this Regulation:

1. "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission[1], dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

12. "personal data breach" means 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;

1 The GDPR does not provide for a definition of „transmission". A transmission means any disclosure of personal data to a third party outside the respective SGL group company.

Chapter II of the GDPR
Principles

Art. 5 para. 1 of the GDPR
Principles relating to processing of personal data

(1) Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 paragraph 1, not be considered to be incompatible with the initial purposes ("purpose limitation");

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 paragraph 1 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

Art. 29 of the GDPR
Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Chapter V of the GDPR
Transfers of personal data to third countries or international organisations

Art. 44 of the GDPR
General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Art. 45 para. 1 of the GDPR
Transfers on the basis of an adequacy decision

(1) A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Article 46 para. 1 and 2 of the GDPR
Transfers subject to appropriate safeguards

(1) In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

a) a legally binding and enforceable instrument between public authorities or bodies;

b) binding corporate rules in accordance with Article 47;

c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

HAYS

Chapter VIII
Remedies, liability and penalties

Art. 82 para. 1, 2 and 4 of the GDPR
Right to compensation and liability

(1) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

(2) Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. [...]

(4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

Art. 83 para. 1, 4, 5 and 6 of the GDPR
General conditions for imposing administrative fines

(1) Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

(4) Infringements of the following provisions shall, in accordance with paragraph2, be subject to administrative fines up to 10.000.000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

b) the obligations of the certification body pursuant to Articles 42 and 43;

c) the obligations of the monitoring body pursuant to Article 41(4).

(5) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

b) the data subjects' rights pursuant to Articles 12 to 22;

c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

d) any obligations pursuant to Member State law adopted under Chapter IX;

e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58 paragraph 2 or failure to provide access in violation of Article 58 paragraph 1.

(6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

National law

Sec. 42 para. 1 and 2 of the BDSG
Criminal offences

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:
1. transferring the data to a third party or
2. otherwise making them accessible for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:
1. processing without authorization, or
2. fraudulently acquiring and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

Sec. 43 para 1 and 2 of the BDSG
Administrative fines

(1) Intentionally or negligently engaging in the following shall be deemed an administrative offence:
1. in violation of Section 30 (1) failing to treat a request for information properly, or
2. in violation of Section 30 (2), first sentence, failing to inform a consumer or doing so incorrectly, incompletely or too late.

(2) An administrative offence may be punished by a fine of up to fifty thousand euros.

Sec. 202a of the StGB
Data espionage

(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access and if he has circumvented the protection shall be punishable with imprisonment of up to three years or a fine.

(2) Within the meaning of paragraph 1 above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

Sec. 303a para. 1 of the StGB
Data alteration

(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a paragraph 2) shall be punishable with imprisonment of up to three years or a fine.