Data protection compliance programme summary

1. Data protection compliance programme

Hexagon AB, including all of its subsidiaries and joint ventures over which Hexagon AB exercises management control (collectively "Hexagon") is committed to data protection and to proactively address and correct business practices that lead to, or potentially could lead to, violations of individuals' privacy and breaches of applicable data privacy laws. Hexagon has developed and implemented a Data Protection Compliance Programme with the purpose to provide an overarching framework for the processing of personal data, and a commitment to apply privacy controls, throughout Hexagon (the "Programme").

The EU General Data Protection Regulation 2016/679 ("GDPR") is a regulation designed to harmonise data privacy laws across the European Union ("EU"), to protect and empower individuals' with respect to their privacy and to reshape the way companies across the EU approach data privacy. The GDPR may also apply to companies based outside the EU when they process personal data of EU residents.

The Programme is designed to ensure compliance with the GDPR for the parts of the business subject to the GDPR and to use the GDPR as a general standard across Hexagon worldwide. The GDPR sets a high standard and it can reasonably be expected that compliance with the GDPR fulfils the material requirements of corresponding data privacy regulations applicable in other jurisdictions. Therefore, Hexagon has decided to apply the Programme globally. However, individual Hexagon entities need to consider whether they are subject to additional data protection regulations applicable where they operate. Should a law conflict with the Programme, the Data Protection Compliance Manual or the GDPR, the more stringent requirement shall prevail.

The Programme is applicable to all directors, executive officers and employees (collectively referred to hereafter as "employees") of Hexagon and is available to all employees on the Hexagon intranet site. It is important that all employees are aware of the fundamental purposes and concepts of the GDPR and strive to maintain compliance with the GDPR and the Programme.

2. Data protection compliance manual

To facilitate and support compliance with the GDPR, Hexagon has drafted a Data Protection Compliance Manual, which sets out the standards and basic principles for Hexagon's processing of personal data. The Data Protection Compliance Manual includes a selection of practical guidelines and templates for consent forms, privacy notices, data processor agreements, etc.

In addition to the Data Protection Compliance Manual (including its appendices), other policies and guidelines may apply either holistically or to specific entities or individuals within Hexagon.

3. Key concepts

3.1 Personal data and processing of personal data

Personal data is information relating to an identified or identifiable individual. Examples of personal data are name, address, email address, phone number, IP address, gender, personal identification number, job position, CV, salary, interests, purchase history, health information, location data, work capacity, marital status, log-in details, etc.

Processing is the legal term for handling personal data. It includes collecting, structuring, storing, adapting, using, transmitting, and erasing personal data.

3.2 Data subjects

Individuals whose personal data is being processed are called data subjects.

3.3 Controller and processor

When Hexagon processes personal data, it might do so on its own initiative, determining why and how the personal data will be processed. For example, Hexagon collects information on its employees for the purposes of paying them a salary each month. In this situation, Hexagon is determining the purposes and means of the processing, and has the role as controller.

In other situations, Hexagon processes personal data on behalf of another entity and according to its instructions. For example, Hexagon might store customer personal data in a cloud solution on behalf of a customer. In this situation, the customer would have the role as controller and Hexagon would have the role as processor.

When a controller is engaging a processor, there is a legal requirement to enter into a data processor agreement. Template data processor agreements are included in the Data Protection Compliance Manual.

Data protection compliance programme summary

3.4 Special categories of personal data

Certain special categories of personal data, such as health data, are afforded special protection and should not be processed by Hexagon except under special circumstances.

3.5 Lawfulness of processing

Hexagon may only process personal data if at least one of the following legal grounds applies: consent, performance of a contract, compliance with a legal obligation, protection of vital interests of the data subject, performance of tasks carried out in the public interest, or the legitimate interests of Hexagon. A template consent form is included in the Data Protection Compliance Manual.

3.6 Rights of the data subject

Data subjects have defined rights under the GDPR. In order to protect their privacy, individuals shall be provided with information and choices concerning Hexagon's processing of their personal data. More information about the data subjects' rights and template privacy notices are included in the Data Protection Compliance Manual.

3.7 Global transfers of personal data

Transfers of personal data from the EU to countries outside the EU/EEA require certain safety measures. Guidance on how to undertake such transfers in compliance with the GDPR is included in the Data Protection Compliance Manual.

3.8 Handling personal data breaches

Transfers of personal data from the EU to countries outside the EU/EEA require certain safety measures. Guidance on how to undertake such transfers in compliance with the GDPR is included in the Data Protection Compliance Manual.

4. Basic principles for processing of personal data

Lawfulness, fairness and transparency – Firstly, this means that the processing of personal data by an entity must be justified on a legitimate basis. Secondly, it means that it must be clear for the individual that personal data related to the individual is being processed, the identity of the entity doing that and for what purpose.

Purpose limitation – The obligation to ensure that the purpose for the processing of personal data is specified, explicit and legitimate and that the personal data is not processed beyond this purpose.

Data minimisation – The obligation to ensure that the personal data processed is adequate, relevant and limited to what is necessary for the purpose.

Accuracy – The obligation to ensure that the personal data processed is accurate, kept up-to-date and to take every reasonable step to correct inaccurate data or erase it.

Storage limitation – The obligation to ensure that personal data is not stored for a longer period than is necessary for the purposes for which the personal data is processed, which means that entities processing personal data must have visibility of its processing activities, established retention periods and/or periodic review processes.

Integrity and confidentiality – The obligation to process personal data in a manner which ensures appropriate security data and prevents unauthorised access (such as hacker attacks) or accidental loss of data.

Accountability – Entities processing personal data must be able to demonstrate that they are in compliance with the obligations under the GDPR.