

Privacy and Data Protection Introduction

Haskoning is dedicated to protecting personal data, as endorsed by our executive board through the signing of our Privacy and Data Protection policy.

In accordance with this policy, Haskoning has implemented appropriate controls (privacy framework) to ensure compliance with the General Data Protection Regulation, applicable in the European Union, and other related privacy legislation, such as the UK General Data Protection Regulation / Data Protection Act 2018 (both applicable in the United Kingdom).

Haskoning has appointed a Data Protection Officer to ensure compliance with appropriate legislation and our privacy and data protection framework, even though this is not a necessity based on GDPR requirements.

Personal data Haskoning process

Haskoning processes personal data only for business purposes and following client instructions when applicable. We may process personal information from clients, suppliers, business contacts, employees, and other stakeholders. Usually, we do not process sensitive personal data in normal operations unless required by a specific project.

Purpose and role for processing personal data

Haskoning processes personal data to maintain business relations with clients, sub-consultants, suppliers, stakeholders, and interested parties. Additionally, personal data is processed for employment purposes. Depending on the circumstances, Haskoning may act as the controller and/or processor of personal data.

Assessment of processing activities

Haskoning reviews each processing activity to determine data privacy applicability, risk, and compliance. This assessment considers factors such as the purpose, scope, role, and legal basis for the processing, personal data categories and types, data retention and protection, data security, applicable sub-processors, and ICT systems and assets. When necessary, Haskoning conducts Data Protection Impact Assessments to evaluate the impact of the processing activity on the data subject. A register of all processing activities is maintained, and these activities are periodically reviewed for compliance based on the level of risk.

Sub-processes and data transfer

Given the nature of our business, Haskoning utilises sub-processors in its daily operations to deliver engineering, consulting, and digital services. These sub-processes, including design applications, cloud data storage, SaaS solutions, and communication services (such as email), may process personal data and, in some cases, involve the transfer of data to third countries. Haskoning has instituted comprehensive contractual and security measures to regulate these sub-processes and is dedicated to maintaining personal data within the EEA whenever feasible.

Privacy by Design and change management

At Haskoning, we integrate privacy by design and by default in all our projects and digital services. We assess privacy throughout new processes, tools, and applications to ensure compliance with the 7 principles of Privacy by Design. Our change management process reviews any adjustments for data privacy adherence.

Data security.

Haskoning acknowledges the critical importance of information security in safeguarding the interests of our clients, employees, company, and other stakeholders. The information we manage includes data entrusted to us by clients and third parties, project-related information, as well as company-specific information such as intellectual property, employee details, and financial records.

In addition to securing our internal systems and data, there is a growing trend where IT services are becoming essential business operations themselves. Our strategy for information and privacy protection is centred around our Information Security Management System (ISMS), which adheres to the international ISO/IEC 27001 standard. We renewed our certification for ISO 27001 in 2024, with annual surveillance audits, following our initial certification in 2019. Moreover, we uphold the UK National Cyber Security Centre's (NCSC) Cyber Essentials and Cyber Essentials Plus certifications. Security governance remains a top priority for us, providing us with significant reassurance and confidence in our security measures.

Haskoning collaborates exclusively with ICT vendors and suppliers that maintain a robust level of security. To ensure the security of our own systems and those of our suppliers, we have implemented a comprehensive risk assessment and mitigation programme. This includes conducting periodic penetration tests and vulnerability assessments on critical systems.

Rights of the data subject

Haskoning recognises and upholds the rights of data subjects as defined by the General Data Protection Regulation (GDPR) and other relevant privacy legislation. These rights may include, depending on the circumstances: the right to access and obtain a copy of personal data, the right to withdraw consent, the right to rectification, the right to data portability, the right to erasure of personal data, the right to object, and the right to restrict processing. Haskoning has established a written procedure to effectively address and manage any data subject requests we receive.

Reporting of incidents

Haskoning has established written procedures for the identification, registration, investigation, and reporting of data privacy incidents and breaches in compliance with applicable data privacy legislation. When processing personal data on behalf of the client as stipulated in the data processing agreement, Haskoning, acting as the processor, will notify the client of any data breaches promptly upon detection. This ensures that the client can fulfil its responsibilities as the data controller according to privacy legislation requirements. Haskoning will take necessary actions to mitigate the risk of a breach and implement measures to prevent recurrence.

Training and awareness

Haskoning promotes awareness of data privacy throughout the organisation and ensures that employees handle personal data in compliance with data privacy requirements. Employees are informed through various channels, including the intranet and learning platforms. Data privacy is also incorporated into the company's 12 ethical principles and its Integrated Management System.