Vertom

Document number: CRP.P.08.007
Revision: 0
Issued: January 2026
Reviewed: -

Corporate Data Protection & Privacy Policy

CEO statement & endorsement

"As Chief Executive Officer of the Vertom Group, I fully support this Corporate Data Protection & Privacy Policy. This policy reflects the Vertom Group's commitment to responsible, ethical, and sustainable business conduct, and provides a clear framework for consistent implementation across all our Group entities.

I expect all employees, managers, and business partners to understand, comply with, and actively support the principles set out in this policy."

Endorsed by:

Name: **A.A.H. de Jong**
Title: **Chief Executive Officer - Vertom Group**
Date: 30 January 2026

This policy is formally endorsed by the Chief Executive Officer. Signed originals are retained in accordance with the Vertom Group's document control procedures.

Introduction

The Vertom Group and its affiliated companies ("the Group") are committed to protecting the personal data of employees, customers, suppliers, and other stakeholders. Personal data is processed lawfully, fairly, and transparently, in full compliance with the General Data Protection Regulation (GDPR) and any other applicable privacy laws. In addition, The group acknowledges the United Nations Sustainable Development Goals (UNSDGs) as guiding principles for responsible business conduct. These references are aspirational in nature and do not create binding obligations beyond the requirements of applicable law.

Purpose

The purpose of this policy is to safeguard personal data and the rights of individuals, ensure compliance with legal and regulatory requirements, provide transparency about how personal data is collected, processed, and stored, and maintain trust with employees, clients, and partners.

Scope

This policy applies to all the Group's employees (permanent, temporary, or contracted), all subsidiaries, joint ventures, and affiliates. Furthermore, this policy also applies to agents, consultants, suppliers, contractors, and any third parties acting on behalf of the group.

Our Commitment

At the Vertom Group, we are committed to:

Data protection principles

The Group applies core data protection principles: personal data is retained strictly for as long as necessary to achieve the legitimate purposes for which it was collected, or to comply with legal and contractual retention obligations. The Group aims to delete or anonymize personal data as soon as reasonably possible after the retention period expires. Where immediate deletion is not practically feasible, compensating measures are applied to keep the data secure and access restricted until final deletion is possible.

Human resources data

Employee and applicant data is processed only for legitimate HR purposes, such as recruitment, payroll, training, performance management, contract administration and termination. Access to HR data is restricted to authorized staff bound by confidentiality obligations. Applicant data is retained only for the duration of the recruitment process and is securely deleted once the process concludes, unless a longer retention period is legally required or the applicant has provided explicit, informed consent for extended storage.

Client, vendor & website data

The Group processes the personal data of clients, vendors, and website users only for legitimate business purposes. Where such data is shared with trusted service providers or public authorities, this is done strictly on a need-to-know basis, subject to equivalent protection standards, contractual safeguards, and appropriate technical and organizational measures to ensure compliance with applicable data protection law.

Rights of individuals

All individuals whose personal data is processed by the Group have rights under applicable law, including access, rectification, deletion (“the right to be forgotten”), restriction or objection to processing, and portability in a machine-readable format. Requests must be addressed to privacy@vertom.nl and will be handled promptly, within the timelines established under applicable law (such as GDPR Article 12). All requests are subject to verification of the requester’s identity and applicable legal limitations.

Data Governance

Data security & confidentiality

The Group ensures the security of personal data through appropriate technical and organizational measures, including encryption, access controls, and secure storage. All employees are required to maintain confidentiality and to comply with established security protocols. When personal data is transferred outside the EU/EEA, the Group only uses legally recognized mechanisms (e.g. SCCs, adequacy decisions). The IT department, in collaboration with the Group Legal and QHSE departments, ensures that appropriate technical and organizational safeguards are implemented to protect such data.

Data breach management

The Group promptly assesses all reported data incidents and ensures that supervisory authorities are notified within 72 hours where required by law. If a breach is likely to result in a high risk to the rights and freedoms of individuals, affected parties will also be informed without undue delay, in line with applicable legal obligations.

Responsibilities

The Divisional Board retains ultimate accountability. The Group’s CTO is responsible for technical and organizational safeguards. The Group Legal and QHSE departments provide oversight and advice. Local management ensures compliance within their entities. These responsibilities will be detailed in a governance matrix to make accountability and responsibility fully transparent. The Group recognizes that implementation is an ongoing process. The principles outlined in this policy represent target states, which will be phased in where necessary. Annual reviews will document progress and next steps.

Employee obligations in handling data

Employees are expected to handle personal data with care and diligence at all times. This includes collecting and processing only the information necessary for their role, ensuring that such data remains accurate and up to date, and avoiding retention for longer than required. Employees must use secure systems and methods when storing or transferring personal data and are required to keep all such information confidential. Personal data may not be shared with unauthorized individuals, and sensitive information must always be communicated via secure and approved channels.

Monitoring, Review & Document Control

Monitoring & review

This policy is reviewed annually by the Board of Directors, or earlier if legal, regulatory, or business developments require. Compliance is monitored through audits, HR and Legal reviews, IT security testing, and incident follow-up. Lessons learned from incidents, audits, and external assessments (e.g. customer audits, privacy ratings) are used to strengthen the Group's data protection framework.

Document control

This policy is governed by CRP.P.02.004 – Quality, Governance & Document Control Policy. The corporate QMS ensures that only valid, current versions are in use across the Group. All Group entities, including affiliated companies with their own management systems, must adopt and comply with the latest approved corporate policies, provided this does not conflict with applicable local law. Version control and revision history must remain transparent and traceable. The Group QHSE Manager retains oversight to ensure consistency across the Group.