VGP

Data Protection and Information Security Policy

www.vgpparks.eu

VERSION 3.0/ JULY 2025

Data Protection and Information Security Policy

Version 3.0/ July 2025

1. Purpose

This policy establishes the framework of VGP NV and its group companies ("VGP" or "the Group") for safeguarding all of its data and securing its information assets. It supports legal compliance, operational resilience and the protection of stakeholder trust across all European operations.

2. Scope

This policy applies to:

— All employees, contractors and third-party providers across the VGP Group;
— All data types, including personal, operational and proprietary information;
— All systems, platforms and processing environments operated by,on behalf of or as a Service to the Group.

3. Governance and Responsibilities

3.1 Board-Level Oversight
VGP's Audit Committee is responsible for high-level monitoring and supervising information security risks as part of its wider governance remit (*see Corporate Governance*).

3.2 Executive Management
The CEO, joint COOs, CFO, General Counsel and IT Director jointly oversee the information security program. Accountability for data protection is delegated to the IT Director in his role as Data Protection Officer (DPO).

3.3 Independent Assurance
Information security controls are regularly reviewed through:
— internal IT audits by the IT Security Officer
— Independent external audits
— performed by a qualified third party
— as part of the annual financial audit

4. Information Security Management Program

VGP maintains an information security management program that includes:

4.1 Business Continuity & Resilience
— Given VGP's 'SaaS First' and Cloud IT strategy, business critical applications and data (e.g. ERP, contracts) are externally hosted in high available and highly redundant environments.
— Site-specific emergency protocols for IT data recovery and data integrity are in place.

4.2 Vulnerability Management
— Vulnerability scanning, patching, and penetration testing conducted periodically.
— Risk-based prioritization and remediation procedures coordinated by the IT security Officer.

4.3 Security Incident Management
— An incident escalation process allows employees to report security incidents, suspicious activity or vulnerabilities via a dedicated internal hotline or email to *dataprotection@vgpparks.eu*.
— Incidents are assessed within 24 hours and handled according to predefined severity levels.

4.4 Internal & External Audits
— Internal audits of infrastructure and systems are conducted biannually by the internal IT security Officer.
— External audits are conducted periodically by a certified cybersecurity firm using, the NIST and the MITRE Framework.

4.5 Awareness Training
— All employees receive a mandatory an (online, including scenario-based exercises) phishing program.
— Security awareness guidelines are shared during the onboarding program
— Policy and procedure, including Q&A, is published on the intranet including update alerts.

5. Data Protection Framework

VGP adheres to GDPR principles, including:
- Lawfulness, transparency, and accountability;
- Risk-based retention and access management;
- Vendor oversight and DPIAs where applicable.

The DPO acts as the point of contact for supervisory authorities and data subjects (dataprotection@vgpparks.eu).

6. Third-Party Security

Prior to engaging third parties, VGP:
- Verifies technical and organizational security controls.
- Conducts KYC Compliance checks for its business partners with focus on but not restricted to AML laws, sanctions screening, ethical sourcing and data protection regulations

7. Monitoring and Compliance

Compliance is reviewed through:
- Daily monitoring and alerting of information security logs by the IT security Officer and third-party hosting providers.
- Annual review of this policy;
- Internal control audits and corrective action plans.

Non-compliance may lead to disciplinary action or contract termination.

8. Where to Find More Information (Public URLs)

- Corporate Governance documents and policies: *https://www.vgpparks.eu/en/investors/corporate-governance/*
- Privacy Contact Page: *https://www.vgpparks.eu/en/data-protection-policy/*
- Employees can report an issue or refer to the suite of IT security and data protection policies and guidelines as available on VGP Connect or the intranet IT Sharepoint drive: *https://vgp.freshservice.com/support/home*

VGP NV
Generaal Lemanstraat 55 box 4
2018 Antwerp
Belgium
TEL +32 3 289 14 30
FAX +32 3 289 14 39
E-MAIL info@vgpparks.eu

www.vgpparks.eu