PRIVACY COMPLIANCE

BUREAU VERITAS

STATUS : FINAL
VERSION : 1.1

PUBLIC	INTERNAL	RESTRICTED	SECRET
X			

Shaping a World of Trust

Approvers

Name	Position
Sonia DELPY	Group Data Protection Officer
Julien ANICOTTE	Chief Information Security Officer

Revision history

Version	Author	Description	Date
1.0	Grégoire BARRAL	Creation of the policy	27/04/2020
1.1	Sonia DELPY	Update of the policy	18/05/2021

Reference documents

Document title	Document Name
Personal Data Protection	Bureau Veritas Group Personal Data Protection Policy For Users

Classification

Level	Confidentiality
C1	Public

PRIVACY COMPLIANCE

Bureau Veritas is committed to respect and protect personal data of every individual and to ensure compliance with applicable personal data protection laws and regulations.

Since 2016, Bureau Veritas has established a global privacy compliance programme in order to improve its practices, in particular to align them with the EU 2016/679 General Data Protection Regulation of 27 April 2016 (“GDPR”) enhanced requirements.

The global privacy compliance programme has been built and is led by the Group Data Protection Officer (DPO) and the Group Chief Information Security Officer (CISO), at group level, with the support of Data Protection Ambassadors and Security Officers locally, in the countries where Bureau Veritas operates, covering all Bureau Veritas’ businesses.

As part of such programme, Bureau Veritas has implemented a series of actions, systems and procedures, as follows:

- Awareness and training of its employees (top management, headquarter, IT, HR…);
- Design and deployment of an identical framework for all group entities, defining 59 legal and technical measures, serving as the reference for the compliance of each personal data processing implemented within the Bureau Veritas Group. The GDPR key principles are integrated from the conception of any new project or service (Privacy by design, Privacy by default, data minimization, etc.);
- Dissemination of Group policies for the protection of personal data applicable to employees and all users outside the Group ;
- Distribution of a Group IT charter reminding users of the Group's information systems of their rights and obligations with regard to the protection of personal data, in particular when they process personal data in the context of their mission for Bureau Veritas. Failure to comply with the terms of this charter may result in (i) the application of disciplinary measures, up to and including dismissal, for Bureau Veritas employees, or (ii) the termination of the contractual relationship with Bureau Veritas for external users (subcontractors, partners). The Group's IT charter also provides for the possibility for Bureau Veritas to report such use to the Police or any other law enforcement authority in the event of suspected use of its information systems for illegal or immoral purposes;
- Development of a public website enabling individuals to exercise their rights (available at https://personaldataprotection.bureauveritas.com);
- Maintenance of a record of processing operations ;
- Dissemination of an internal procedure to report a suspected or proved personal data breach with a view to notification (where mandatory) to the competent supervisory authority and eventually to individuals;
- Bureau Veritas Group risk mapping: it includes security and protection of personal data confidentiality and is the subject of action plans that are regularly monitored at head office level and in the various operating groups.

Furthermore, Bureau Veritas has set up technical and organizational measures to ensure the security and the confidentiality of personal data, based on ISO 27001 requirements and aligned with Group information security policies. These measures are organized according to the following categories:

- information security policies;
- access management and identity;
- third parties and sub-contracting;

- security monitoring;
- data management, deletion and archiving;
- systems development;
- applications and servers' security;
- network security;
- devices security;
- data leakage;
- physical security.

The above measures are detailed in Appendix A.

To ensure the effectiveness of compliance actions and procedures, Bureau Veritas set up two-tier checkpoints:

- Internal audits are conducted regularly to assess the Group processings' compliance. Major processings (e.g. HR and clients databases) are subject to special monitoring;

- Control of processors: Bureau Veritas selects service providers according to strict requirements in terms of data protection (e.g. ISO/SSAE certification, assessment of processor's compliance with the GDPR requirements). Contracts are strengthened: in addition to the provisions relating to the processor's obligations under the GDPR, a reference framework of security measures (Security Insurance Plan) must be implemented by the service provider and is incorporated into our contracts. These elements are also incorporated into the Business Partners Code of Conduct of Bureau Veritas applicable to all business partners (companies or individuals) of the Bureau Veritas Group.

APPENDIX A

Technical measures describe all the security requirements to be implemented on the applications, the infrastructure, and the people who use and maintain those.

They include organizational, functional and technical measures to be applied to data management, identity and access, asset management and network control.

Information security policies
The framework includes raising security awareness measures among Bureau Veritas' employees, by informing and communicating the Bureau Veritas security policies, duties and rules, and by training the employees regarding risks and best practices to adopt.

Access Management and identity
Access management and identity measures are key for security, allowing each user of the system to be able to access only the data needed for the exercise of activities and tasks. This includes establishing and reviewing an access control policy, classifying information hosted in the application with Confidentiality, Integrity, Availability and Traceability (CIAT) standards, the creation of authorization profiles that restrict access as actually needed, implementing a robust checkout process.

Third parties and subcontracting
To ensure that personal data communicated to or managed by subcontractors and/or third-parties, third parties' relationships must have security guarantees. This includes measures such as security frameworks for outsourced applications (e.g. SaaS Cloud apps), binding charters for cybersecurity and privacy protection, and on top of that mandatory implementation of a Security Insurance Plan (SIP) for all IT contracts.

Log management and security monitoring
Security monitoring is mandatory, in order to be able to identify a fraudulent access to personal data, abusive use of such data, or to determine the origin of an incident. The monitoring system records the relevant events, ensures that these records cannot be altered, and in any case, conserves these elements for an appropriate and proportionate duration. This includes defining rules for internal control processes to ensure that all actions performed on the personal data comply with Bureau Veritas security policies, as well as with legal and regulatory constraints.

Data management, deletion and archiving
Conservation of personal data is also an important matter, archives must be secured and encrypted if the archived data is sensitive or considered confidential by the company. This includes definition of needs in terms of data retention and archiving by the business on a case-by-case basis, definition of a process to ensure secure and complete removal of personal data upon data subject request. Same measures are applied to outsourced applications. Back-up of personal data are performed and regularly tested in accordance with the data back-up policy.

Systems development
The protection of personal data must be an integral part of the development of applications to prevent error, loss, modification, unauthorized use, or any misuse of them in applications. This includes among other separation of production and non-production environments, anonymization of data in non-production environments, and minimization of data collection.

Applications and servers' security
Applications and servers are critical assets and as such deserve advanced security measures, such as definition of procedures and implementation of technical measures for timely detection of vulnerabilities within Bureau Veritas' applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing, vulnerability scans) to ensure the efficiency of implemented security controls. A critical step is also the installation of critical operating systems and applications security updates without delay by scheduling periodic automatic check and update of applications and infrastructures when critical vulnerabilities have been identified and corrected.

Network security

For all network services, network functions and service levels essential for the proper functioning of the processing are identified and only these ones are authorized. This implies limiting the network flows to what is strictly necessary and use virtual networks (VLANs) for network segregation, accessing to Bureau Veritas' information system using only VPN connections which are based on strong cryptographic algorithms (IPSec, SSL/TLS), defining processes to protect Bureau Veritas network when interfaced or connected to third-parties network, and use an Intrusion Detection System (IDS) to analyze network traffic in real time to detect any suspicious activity.

Devices security

The security of devices requires the implementation of measures to prevent attempted fraudulent access, virus execution or remote control, especially via the Internet. The risks of intrusion into computer systems are important and can lead to the implantation of viruses or "spy" programs. The first step is to limit access to Bureau Veritas' services, applications and platforms to Bureau Veritas' equipment only. The second step is the definition of procedures and implementation of technical measures to prevent the execution of malware on Bureau Veritas users end-point devices (workstations, instruments, laptops, and mobile devices) and IT infrastructure network and system components (antivirus solution, WAF, etc.) which are regularly updated. When sensitive data is stored on a device, the owner must implement encryption for drives and databases.

Data leakage

In order to prevent data leaks, each application owner must design a plan to prevent it on its applications. A Data Leakage Prevention (DLP) solution has been acquired by Bureau Veritas in 2019 and it is deployed, based on sensitiveness and criticality, to specific users. The objective is to limit the leakage of sensitive data, whether accidental or intentional.

Physical security

Regarding physical security, in order to effectively protect the premises where personal data processing is hosted, facility management provide i) alarms to detect intrusion within a secured area, ii) measures to slow the progression of intruders within the building and offices, iii) means to put an end to the intrusion.