RESPECT DE LA VIE PRIVEE

BUREAU VERITAS

STATUT : FINAL

VERSION : 1.0

PUBLIC	INTERNE	RESTREINT	SECRET
X			

Shaping a World of Trust

Approbateurs

Nom	Fonction
Sonia DELPY	Déléguée à la Protection des Données Groupe
Julien ANICOTTE	Responsable de la Sécurité des Systèmes d'Information

Historique des révisions

Version	Auteur	Description	Date
1.0	G. Barral	Création de la politique	27/04/2020

Documents de référence

Titre du document	Nom du document
Respect de la vie privée	Politique de Protection des Données à Caractère Personnel du Groupe Bureau Veritas pour les Utilisateurs

Classification

Niveau	Confidentialité
C1	Public

RESPECT DE LA VIE PRIVEE

Bureau Veritas s'engage à respecter et à protéger les données personnelles de chaque individu et à assurer le respect des lois et règlements applicables en matière de protection des données personnelles.

Depuis 2016, Bureau Veritas a mis en place un programme mondial de respect de la vie privée afin d'améliorer ses pratiques, en particulier pour les aligner sur les exigences renforcées du Règlement Général sur la Protection des Données de l'UE 2016/679 du 27 avril 2016 ("RGPD").

Le programme mondial de respect de la vie privée a été élaboré et est conduit par le Délégué à la Protection des Données (DPD) et le Responsable de la Sécurité des Systèmes d'Information (RSSI), au niveau du groupe, avec le soutien des ambassadeurs de la protection des données et des responsables de la sécurité au niveau local, dans les pays où Bureau Veritas opère, couvrant toutes les activités de Bureau Veritas.

Dans le cadre de ce programme, Bureau Veritas a mis en œuvre une série d'actions, de systèmes et de procédures, comme suit :

- Sensibilisation et formation de ses employés (direction générale, siège, informatique, RH, ventes...);
- Conception et déploiement d'un cadre identique pour toutes les entités du groupe, définissant 63 mesures juridiques et techniques, servant de référence pour la conformité de chaque traitement de données à caractère personnel mis en œuvre au sein du groupe Bureau Veritas. Les principes clés du RGPD sont intégrés dès la conception de tout nouveau projet ou service (protection des données dès la conception /*« Privacy by design »,* protection des données par défaut / *« Privacy by default »,* minimisation des données, etc.) ;
- Diffusion des politiques du Groupe pour la protection des données personnelles applicables aux employés et à tous les utilisateurs en dehors du Groupe ;
- Développement d'un site web public permettant aux individus d'exercer leurs droits et de répondre aux requêtes (disponible à l'adresse : https://personaldataprotection.bureauveritas.com/home/1.1.2/#/home);
- Tenue d'un registre des opérations de traitement ;
- Diffusion d'une procédure interne pour signaler une violation suspectée ou avérée de données à caractère personnel en vue de la notification (lorsqu'elle est obligatoire) à l'autorité de contrôle compétente et, éventuellement, aux personnes concernées.

En outre, Bureau Veritas a mis en place des mesures techniques et organisationnelles pour assurer la sécurité et la confidentialité des données personnelles, basées sur les exigences de la norme ISO 27001 et alignées sur les politiques de sécurité de l'information du Groupe. Ces mesures sont organisées selon les catégories suivantes :

- les politiques de sécurité de l'information ;
- la gestion de l'accès et de l'identité ;
- les tiers et la sous-traitance ;
- la gestion des journaux et la surveillance de la sécurité ;
- la gestion, la suppression et l'archivage des données ;
- le développement de systèmes ;
- la sécurité des applications et des serveurs ;
- la sécurité des réseaux ;

- la sécurité des appareils ;
- la fuite de données ;
- la sécurité physique.

Les mesures ci-dessus sont détaillées dans l'Annexe A.

Pour garantir l'efficacité des actions et des procédures de conformité, Bureau Veritas a mis en place des points de contrôle à deux niveaux :

- Des audits internes sont effectués régulièrement pour évaluer la conformité des traitements du groupe. Les principaux traitements (par exemple, les bases de données RH et clients) font l'objet d'un suivi particulier ;

- Contrôle des sous-traitants: Bureau Veritas sélectionne les prestataires de services en fonction d'exigences strictes en matière de protection des données (par exemple, certification ISO/SSAE, évaluation de la conformité des sous-traitants aux exigences du RGPD). Les contrats sont renforcés: en plus des dispositions relatives aux obligations du sous-traitant dans le cadre du RGPD, un cadre de référence de mesures de sécurité (Plan d'Assurance Sécurité) doit être mis en œuvre par le prestataire de services et est intégré dans les contrats. Ces éléments sont également intégrés dans le Code de Conduite des Partenaires d'Affaires de Bureau Veritas, applicable à tous les partenaires d'affaires (entreprises ou particuliers) des sociétés affiliées du Groupe Bureau Veritas.

ANNEXE A

Les mesures techniques décrivent toutes les exigences de sécurité à mettre en œuvre sur les applications, l'infrastructure et les personnes qui les utilisent et les maintiennent.

Elles comprennent les mesures organisationnelles, fonctionnelles et techniques à appliquer à la gestion des données, à l'identité et à l'accès, à la gestion des actifs et au contrôle du réseau.

Politiques de sécurité de l'information
Le cadre comprend des mesures de sensibilisation des employés de Bureau Veritas à la sécurité, en informant et en communiquant les politiques, les devoirs et les règles de sécurité de Bureau Veritas, et en formant les employés aux risques et aux meilleures pratiques à adopter.

Gestion des accès et de l'identité
La gestion des accès et les mesures d'identité sont essentielles pour la sécurité, car elles permettent à chaque utilisateur du système de ne pouvoir accéder qu'aux données nécessaires à l'exercice de ses activités et tâches. Cela inclut l'établissement et la révision d'une politique de contrôle d'accès, la classification des informations hébergées dans l'application selon les normes de Confidentialité, d'Intégrité, de Disponibilité et de Traçabilité (CIDT), la création de profils d'autorisation qui restreignent l'accès en fonction des besoins réels, la mise en œuvre d'un processus de vérification robuste.

Tiers et sous-traitance
Pour garantir que les données personnelles communiquées ou gérées par des sous-traitants et/ou des tiers, les relations avec ces tiers doivent présenter des garanties de sécurité. Cela inclut des mesures telles que des cadres de sécurité pour les applications externalisées (par exemple, les applications SaaS Cloud), des chartes contraignantes pour la cybersécurité et la protection de la vie privée, et en plus de cela, la mise en œuvre obligatoire d'un plan d'assurance sécurité (PAS) pour tous les contrats informatiques.

Gestion des journaux et surveillance de la sécurité
La surveillance de la sécurité est obligatoire, afin de pouvoir identifier un accès frauduleux à des données personnelles, une utilisation abusive de ces données ou de déterminer l'origine d'un incident. Le système de surveillance enregistre les évènements pertinents, veille à ce que ces enregistrements ne puissent être modifiés et, en tout état de cause, conserve ces éléments pendant une durée appropriée et proportionnée. Cela inclut la définition de règles pour les processus de contrôle interne, afin de garantir que toutes les actions effectuées sur les données personnelles sont conformes aux politiques de sécurité de Bureau Veritas, ainsi qu'aux contraintes légales et réglementaires.

Gestion, suppression et archivage des données
La conservation des données personnelles est également une question importante, les archives doivent être sécurisées et cryptées si les données archivées sont sensibles ou considérées comme confidentielles par l'entreprise. Cela inclut la définition des besoins en termes de conservation et d'archivage des données au cas par cas, la définition d'un processus pour assurer la suppression complète et sécurisée des données personnelles à la demande de la personne concernée. Les mêmes mesures sont appliquées aux demandes externalisées. Des sauvegardes des données à caractère personnel sont effectuées et régulièrement testées conformément à la politique de sauvegarde des données.

Développement de systèmes
La protection des données à caractère personnel doit faire partie intégrante du développement des applications afin d'éviter les erreurs, les pertes, les modifications, les utilisations non autorisées ou toute utilisation abusive de celles-ci dans les applications. Cela inclut notamment la séparation des environnements de production et de non-production, l'anonymisation des données dans les environnements de non-production et la minimisation de la collecte de données.

Sécurité des applications et des serveurs
Les applications et les serveurs sont des actifs critiques et méritent à ce titre des mesures de sécurité avancées, telles que la définition de procédures et la mise en œuvre de mesures techniques pour la détection rapide des vulnérabilités au sein des applications, du réseau d'infrastructure et des composants du système de Bureau Veritas (par exemple, évaluation de la vulnérabilité du réseau, tests de pénétration, analyses de vulnérabilité), afin de garantir l'efficacité des contrôles de sécurité mis en œuvre. Une étape critique est également l'installation sans délai des mises à jour de sécurité des systèmes d'exploitation et des applications critiques, en programmant un contrôle et une mise à jour automatiques périodiques des applications et des infrastructures lorsque les vulnérabilités critiques ont été identifiées et corrigées.

Sécurité des réseaux
Pour tous les services de réseau, les fonctions de réseau et les niveaux de service essentiels au bon fonctionnement du traitement sont identifiés et seuls ceux-ci sont autorisés. Cela implique de limiter les flux réseau au strict nécessaire et utiliser des réseaux virtuels (VLAN) pour la séparation des réseaux, accéder au système d'information de Bureau Veritas en utilisant uniquement des connexions VPN basées sur des algorithmes cryptographiques puissants (IPSec, SSL/TLS), définir des processus pour protéger le réseau de Bureau Veritas lorsqu'il est interfacé ou connecté à un réseau tiers, et utiliser un système de détection d'intrusion (IDS) pour analyser le trafic réseau en temps réel afin de détecter toute activité suspecte.

Sécurité des appareils
La sécurité des appareils exige la mise en œuvre de mesures visant à empêcher les tentatives d'accès frauduleux, l'exécution de virus ou le contrôle à distance, notamment via Internet. Les risques d'intrusion dans les systèmes informatiques sont importants et peuvent conduire à l'implantation de virus ou de programmes "espions". La première étape consiste à limiter l'accès aux services, applications et plates-formes de Bureau Veritas aux seuls équipements de Bureau Veritas. La deuxième étape consiste à définir des procédures et à mettre en œuvre des mesures techniques pour empêcher l'exécution de logiciels malveillants sur les terminaux des utilisateurs de Bureau Veritas (postes de travail, instruments, ordinateurs portables et appareils mobiles) et sur les composants réseau et système de l'infrastructure informatique (solution antivirus, WAF, etc.) qui sont régulièrement mis à jour. Lorsque des données sensibles sont stockées sur un appareil, le propriétaire doit mettre en œuvre un cryptage pour les lecteurs et les bases de données.

Fuite de données
Afin de prévenir les fuites de données, chaque propriétaire d'application doit concevoir un plan visant à les empêcher sur ses applications. Une solution de prévention des fuites de données (DLP) a été acquise par Bureau Veritas en 2019 et elle est déployée, en fonction de la sensibilité et de la criticité, auprès d'utilisateurs spécifiques.
L'objectif est de limiter les fuites de données sensibles, qu'elles soient accidentelles ou intentionnelles.

Sécurité physique
En ce qui concerne la sécurité physique, afin de protéger efficacement les locaux où le traitement des données à caractère personnel est hébergé, la gestion des installations prévoit i) des alarmes pour détecter les intrusions dans une zone sécurisée, ii) des mesures pour ralentir la progression des intrus dans le bâtiment et les bureaux, iii) des moyens pour mettre fin à l'intrusion.