Plan d’Assurance Sécurité

(PAS)

-

02/12/2024

Contrôle de document

Version	Mis à jour par	Date	Description des changements
1.0	GHS	27/06/2024	Initialisation du document
1.1	GHS	09/07/2024	Modifications diverses : gestion des logs, stockage des données, prestataire gestion sécurité.
1.2	GHS	10/07/2024	Clarifications sur la section traitement des données personnelles
1.3	GHS	02/12/2024	Ajout du service SADV dans les traitements de données et les responsabilités de GHS en tant que sous-traitant

Révisé par	Rôle du réviseur	Approuvé par	Date
Vincent COQUART	CTO	David LESCURE	02/12/2024

Table des matières

1. Introduction

Le Plan d'Assurance Sécurité, désigné sous le terme « PAS » dans la suite de ce document, décrit les engagements pris par GHS en termes de sécurité de ses données, de ses applications et des infrastructures.

Ce document a pour but de préciser les engagements de sécurité pris par GHS dans le cadre de ses prestations. Il définit notamment l'organisation, la méthodologie et les mesures techniques, matérielles et organisationnelles mises en place pour gérer la sécurité de ses prestations.

2. Enjeux et objectifs

La sécurité des applications proposées par GHS et de leur hébergement sont des composantes essentielles pour la protection des intérêts de la société GHS et de ses clients.

Notre PAS est mis en œuvre dans ce sens afin de prendre en compte les principaux risques identifiés :

- Risque de divulgation, perte de confidentialité accidentelle ou volontaire des informations gérées pour le compte de nos clients.
- Risque d'altération, ou perte d'intégrité, qui pourrait amener à une perte d'information pour nos clients.
- Risque de perte de disponibilité de nos services pour nos clients.

Il sera fait référence à la gestion des données des clients dans la suite de ce document. Toutefois, ces données ne concernent que les services Transat et de paie en mode hébergé (cf. sPAIEctacle / La Paie en fonctionnement hébergé). En aucun cas, GHS n'est responsable de la gestion des données clients en mode sur site (cf. sPAIEctacle / La Paie en fonctionnement sur site).

3. Description de la prestation ou du service

GHS est le concepteur et l'éditeur d'une suite de logiciels de paie conçus notamment pour les PME employant une forte proportion de contrats courts (le(s) « **Logiciel(s)** »). Parmi cette suite figurent sPAIEctacle, spécialement conçu pour les entreprises culturelles, ou encore La Paie, pour les TPE/PME hors secteur culturel. Les solutions et services proposés par GHS autour des Logiciels sont notamment les suivants :

- Un service de support et de maintenance **« Privilège** ».
- Une solution de signature électronique « **Signature électronique** ».
- Un service de « **Notes de droits d'auteur** ».
- La possibilité de déposer des documents tels que les bulletins de paies, et de partager des informations avec le salarié, sur un espace « **Transat** » permettant aux salariés de disposer d'un espace en ligne facilitant l'établissement de leur paie et de la documentation sociale afférente.

- Un service « **Connectivité** » consistant en la mise à disposition d'un bouquet d'API et de connexions natives avec d'autres plateformes permettant de mettre en place et d'activer des échanges de données et des automatisations entre les outils proposés par ladite plateforme et les solutions de GHS.
- Un service de « **Gestion des embauches en contrat court** » consistant en la mise à disposition d'une plateforme web, connectée à la paie en temps réel, et permettant la préparation des embauches (demande de documents et d'état-civil, DPAE) ainsi que la saisie des contrats courts dans un tableur.
- Un service de « **Gestion des congés** » permettant aux salariés d'effectuer des demandes d'absences via leur compte Transat, et à l'employeur de valider ces dernières puis de les intégrer automatiquement en paie

3.1 sPAIEctacle / La Paie en fonctionnement sur site

Les clients disposent d'un Logiciel installé sur leurs machines, utilisant des données stockées sur leurs serveurs. Grâce à des connecteurs dans le Logiciel, ce dernier peut étendre ses fonctionnalités en communiquant avec des applications web hébergées sur les infrastructures cloud de GHS. Dans ce mode de fonctionnement :

- GHS n'est pas en mesure d'appliquer ses politiques de sécurité à l'infrastructure du client, qui est donc entièrement responsable de la sécurité des données qu'il y héberge
- GHS réplique et stocke uniquement les données personnelles des salariés et des dirigeants des sociétés du Client sur ses infrastructures cloud

3.2 sPAIEctacle / La Paie en fonctionnement hébergé

Le Logiciel se présente sous la forme d'une application en mode SaaS hébergée par GHS. Les données sont alors stockées sur l'infrastructure cloud de GHS.

4. Traitement des données personnelles et conformité juridique

4.1 Conformité juridique

4.1.1 Lois et règlementations applicables en matière de confidentialité et de protection des données personnelles

GHS traite les données personnelles conformément à la réglementation en vigueur applicable au traitement de données à caractère personnel (« DCP »), en particulier, la Loi Informatique et Libertés n°78-17 du 6 janvier 1978 modifiée et le règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018 (« RGPD »).

GHS fait respecter la confidentialité des DCP par les intervenants susceptibles d'y accéder.

Dans le cadre du service Transat, GHS s'acquitte de l'obligation de répondre aux demandes d'exercice de droits des personnes concernant leurs données personnelles, afin notamment de respecter le délai légal de réponse d'un mois

GHS met à disposition toutes les informations nécessaires pour permettre à l'entreprise cliente ou un auditeur externe, de réaliser des audits.

GHS met à dispositions de ses clients les outils nécessaires à la restitution ou suppression des DCP en accord avec les exigences légales de conservation des données, respectant ainsi l'obligation de « privacy by design » posée par le RGPD.

4.1.2 DPO

Un délégué à la protection des données (« DPO ») est désigné au sein de GHS. Ses coordonnées sont les suivantes :

Prénom Nom : Drissia Landragin
Courriel : dpo@ghs.fr

4.2 Traitement de données à caractère personnel réalisé par GHS

GHS responsable de traitement : GHS agit en tant que responsable de traitement pour ce qui concerne :

- les données personnelles des Utilisateurs Autorisés (Licence en mode hébergé). Ces données sont traitées exclusivement aux fins de permettre l'accès au Logiciel Hébergé.

- les données personnelles des interlocuteurs support et maintenance de GHS au sein du Client. Ces données sont traitées exclusivement aux fins de permettre l'exécution du support et de la maintenance.

Chaque personne concernée dispose d'un droit d'accès et de rectification de ses données personnelles. Elle peut également en demander la suppression, mais dans un tel cas, elle ne pourra plus accéder au

Logiciel hébergé et/ou au service considéré. Les données personnelles des personnes concernées sont conservées pendant la durée indiquée dans sa Politique de protection des données personnelles, accessible à l'adresse https://www.ghs.fr/donnees-personnelles/.

GHS sous-traitant : GHS agit en tant que sous-traitant du Client dans les cas suivants :

(i) pour tous les clients, en ce qui concerne les données à caractère personnel liées aux salariés du Client et aux dirigeants des sociétés du Client, afin d'utiliser le service SADV proposé par le GIP-MDS (Groupement d'intérêt public Modernisation des déclarations sociales)

(ii) en mode Hébergé, pour ce qui concerne les données à caractère personnel contenues dans les documents et informations de toute nature appartenant au Client

(iii) lorsque de façon ponctuelle et avec l'accord du Client, GHS est amenée à accéder aux données à caractère personnel des salariés figurant dans les documents du Client aux fins, par exemple, de traiter une anomalie

(iv) gestion des embauches en contrat court

Accès à l'espace Transat

Si le Client invite un salarié à s'inscrire sur Transat aux fins de partager des informations et documents, GHS agira en tant que responsable de traitement des données gérées par Transat et recueillera le consentement de chaque salarié pour l'utilisation de ses données dans le cadre de Transat.

4.2.1 Type de données personnelles

Les catégories de données traitées par GHS à titre de responsable de traitement ou de sous-traitant sont les suivantes :

- État civil, identité, données d'identification, images.
- Vie professionnelle (CV, école, formations, distinctions, ...).
- Données RH (contrats, fiche de paie).
- Données de connexion (adresse IP, logs, etc.).
- Données bancaires (RIB, IBAN).

Selon le principe de minimisation des données, les DCP sont adéquates, pertinentes et limitées à ce qui est strictement nécessaire au regard des finalités pour lesquelles elles sont traitées pour le compte de GHS ou de son client.

Le principe de minimisation appliqué par GHS porte notamment sur :

- La nature des données utilisées (seules celles nécessaires au traitement).
- La diffusion raisonnable et proportionnée des informations (un minimum de destinataires des données, un minimum d'envoi de courriels).

- Une durée de conservation des données adaptée, sous le contrôle du client si elles sont traitées par GHS en qualité de sous-traitant.

Chaque fois que leurs données sont collectées par GHS à titre de responsable de traitement, les personnes concernées ont connaissance de la finalité pour laquelle les données sont collectées ainsi que la durée de conservation de ces données.

Ils sont informés de la possibilité d'exercer leurs différents droits en faisant la demande au DPO de GHS.

4.2.2 Cas spécifique des données RH

Conformément au code du travail français, les clients de GHS sont légalement tenus de conserver certaines données relatives aux ressources humaines, dont le détail est donné ci-dessous. GHS en qualité de sous-traitant peut les conserver sur ces durées, sur ordre de son client.

Type de document	Durée de conservation
Bulletin de paie (électronique)	50 ans ou jusqu'à 6 ans après le départ à la retraite du salarié.
Document concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régimes de retraite.	5 ans
Document relatif aux charges sociales et à la taxe sur les salaires	3 ans
Comptabilisation des jours de travail des salariés sous convention de forfait	3 ans
Comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation	1 an
Déclaration d'accident du travail auprès de la caisse primaire d'assurance maladie	5 ans

4.2.3 Opérations de traitement des DCP

GHS a identifié la liste des traitements de données personnelles nécessaires à l'exécution du service. GHS est, selon les cas, responsable de traitement ou sous-traitant pour le compte d'un donneur d'ordre.

Pour chaque traitement a été établi un registre des données conformément aux exigences du règlement.

Sept types de traitements des données sont identifiés :

Nom du traitement	Position GHS dans le traitement	Description du traitement	Données collectées dans le cadre du traitement
Maintenance	Sous-traitant	Opérations de maintenance sur demande d'un client, sur	Données personnelles : • État civil, identité, données d'identification (Nom,

		la base d'une copie de sa base de données (pas de modification des données, lecture seule). Une fois l'opération terminée, les données sont détruites.	prénoms, adresses, emails, téléphones, NIR) • Données RH (contrats, fiches de paie) Données sensibles : • Données bancaires (SEPA, RIB)
Signature électronique	Sous-traitant	Envoi par l'employeur, depuis le logiciel de paie, de contrats en signature électronique à ses employés. La signature électronique est assurée par YouSign.	Données personnelles : • Prénom, nom, n° téléphone, email • Contrat de travail
Hébergement	Sous-traitant	Hébergement par GHS des données du client et de l'applicatif de paie.	Données personnelles : • État civil, identité, données d'identification (Nom, prénoms, adresses, emails, téléphones, NIR) • Données RH (contrats, fiches de paie) Données sensibles : • Données bancaires (SEPA, RIB)
Flux Transat	Sous-traitant	Récupération, par le logiciel de paie, d'informations nécessaires à l'embauche envoyées par le salarié depuis son compte Transat Envoi vers Transat, par l'employeur depuis le logiciel de paie, de contrats signés électroniquement	Données personnelles : • État civil, identité, données d'identification (Nom, prénoms, adresses, emails, téléphones, NIR) • Données RH (contrats) Données sensibles : • Données bancaires (SEPA, RIB)
Flux API	Sous-traitant	Utilisation des API par des éditeurs tiers pour le compte de clients communs, ou directement par des clients pour leur propre usage	Données personnelles : • État civil, identité, données d'identification (Nom, prénoms, adresses, emails, téléphones, NIR) • Données RH (contrats, fiches de paie) Données sensibles : • Données bancaires (SEPA, RIB)

Gestion des embauches	Sous-traitant	Saisie de contrats par l'employeur sur une interface web de type tableur, synchronisation avec la paie, envoi des DPAE et de contrats en signature électronique.	Données personnelles : • État civil, identité, données d'identification (Nom, prénoms, emails, téléphones) • Données RH (contrats)
Gestion des congés	Sous-traitant	Saisie par le salarié de demandes d'absences depuis son compte Transat, validation par l'employeur par mail ou sur une interface dédiée, intégration en paie.	Données personnelles : • Matricule salarié • Données RH (paies, soldes de congés)
SADV	Sous-traitant	Envoi, sur action du Client, à la plateforme Net-Entreprises.fr des données des salariés concernés par la déclaration d'amorçage : Nom, Prénoms, Adresse, Date et lieu de naissance et NIR	Données personnelles des salariés du Client : • État civil, identité, données d'identification (Nom, prénoms, adresses, emails, téléphones, NIR) • Données bancaires (SEPA, RIB) Données personnelles des dirigeants des sociétés du Client : • État civil, identité, données d'identification (Nom, prénom, email)

4.2.4 Transfert des DCP

Le transfert de données personnelles est limité au strict nécessaire. Il est sécurisé selon les dispositions décrites dans le présent document.

A noter qu'aucun transfert n'est effectué en dehors de l'Union Européenne.

4.2.5 Procédures de notification de violation de données personnelles et de respect des droits des personnes concernées

GHS notifie toute violation de données concernant les DCP auxquelles il a accès dans le cadre du contrat dans les plus brefs délais après en avoir eu connaissance.

Le personnel et les sous-traitants concernés ont été informés de la conduite à suivre en cas de violation de données personnelles.

GHS met en place une procédure en cas de violation des données comprenant la liste des rôles et responsabilités définis avec le client.

4.2.6 Sécurité des données à caractères personnelles

Les mesures de sécurité suivantes sont appliquées afin de garantir la sécurité de ces données :

Bases de données dédiées :

- GHS met à disposition de ses clients des bases de données leur étant dédiées.

Utilisation du Chiffrement :

- Le chiffrement TLS1.2 est utilisé afin de s'assurer que les données ne transitent jamais en clair sur le réseau.

Définition de la durée de conservation des données :

- GHS respecte la durée de conservation des données de ses clients défini conformément aux dispositions contractuelles.

4.2.7 Les tiers intervenants / sous-traitants

Les tiers intervenants ou sous-traitants qui collectent et traitent des données personnelles pour le compte de GHS, engagent leur responsabilité dans la chaine des traitements de données personnelles concernées. Une revue contractuelle visant à valider la présence d'engagements dans le contrat concernant la confidentialité des données personnelles traitées est effectuée pour chaque sous-traitants.

5. Exigences en matière de sécurité

5.1 Organisation de la sécurité

5.1.1 Responsabilités et rôles sécurité

Vincent Coquart, CTO de GHS, agit en tant que responsable de la sécurité de l'information de l'entité.

Ses principales missions sont d'être :

- L'interlocuteur privilégié pour les questions relatives à la sécurité, notamment les enquêtes sur les incidents de sécurité, les rapports sur les failles de sécurité.
- Responsable du maintien en conditions de sécurité et de la bonne application du PAS.

5.1.2 Pilotage de la Sécurité des Systèmes d'Information

GHS s'est engagé dans une démarche de pilotage et d'établissement de principes directeurs lui permettant de garantir :

- Une maitrise des risques informatiques.
- Un niveau de sécurité de son SI.

5.1.3 Détection, alerte et traitement des incidents de sécurité

GHS informera ses clients de la survenance de toute faille de sécurité entraînant des conséquences directes ou indirectes sur le traitement de ses données de toute nature, ainsi que de toute réclamation qui lui serait adressée par toute personne concernée par le traitement des données réalisé dans le cadre d'une prestation.

GHS informera ses clients en cas d'incident de sécurité pouvant impacter son service ou son Système d'Information. Un incident de sécurité SI sera défini par : un évènement potentiel ou avéré, indésirable ou inattendu, impactant la sécurité de l'information.

5.1.4 Clause de confidentialité

GHS respecte et fait respecter par ses employés les obligations contenues dans la clause de confidentialité conclue avec ses clients.

En tout état de cause, les employés de GHS intervenant dans le cadre des prestations et amenés à manipuler des DCP sont tenus par obligation de confidentialité intégrée à leur contrat de travail.

5.1.5 Sensibilisation des intervenants

GHS s'engage à ce que son personnel respecte les règles de protection de base des Systèmes d'Information tel que recommandées par l'ANSSI.

De plus, des formations dédiées à la sécurité des systèmes d'information sont organisées et présentées à l'ensemble des collaborateurs.

Par ailleurs, GHS veille à ce que son personnel respecte les exigences de sécurité telles que décrites dans le PAS, dont notamment :

- L'organisation de la sécurité.
- La confidentialité des informations.
- Le signalement des incidents de sécurité ou des incidents de sécurité présumés.

5.2 Sécurité

5.2.1 Localisation géographique du Service, des données et des serveurs.

Toutes les infrastructures (techniques ou organisationnelles) de GHS sont gérées au sein de l'Union Européenne.

Les datacenters principaux hébergeant les données et les applications mis à disposition des clients sont gérés par Microsoft et Google et localisés en Belgique. Concernant les données de sauvegarde, celle-ci sont stockées France métropolitaine et en Allemagne.

5.2.2 Audits sur les exigences de sécurité

GHS fait appel à des auditeurs externes indépendants de manière récurrente afin de s'assurer du niveau de sécurité de son système d'information et de ses services :

- Test d'intrusion du système d'information interne en octobre 2023 par DND Agency.
- Test d'intrusion de la plateforme Transat en juillet 2024 par Synacktiv.
- Test d'intrustion de la plateforme d'hébergement (Azure) prévu en Janvier 2025 par Synacktiv.

5.2.3 Correction des écarts identifiés

Lorsque des vulnérabilités sont identifiées durant les audits de sécurité, un plan de remédiations est établi.

GHS met en action ce plan de remédiations afin de corriger les vulnérabilités au plus vite.

6. Sécurité des environnements

6.1 Protection contre les attaques

GHS mets en place des mesures nécessaires afin de protéger ses équipements (postes de travail et machines virtuelles) contre les attaques, notamment les codes malveillants. Pour ce faire, GHS fait appel à un prestataire, Everping, pour gérer la sécurité des postes de travail. Avant utilisation, chaque machine Mac est configurée comme suit :

- Chiffrement des disques durs.
- Installation de l'EDR ThreatDown par Malwarebytes.
- Activation de Gatekeeper.
- Renforcement de la stratégie de déverrouillage.

Les serveurs supportant les services de travail collaboratif sont gérés par Google (GSuite) tout comme leur sécurité. Les engagements de sécurité de Google sont définis dans les '' Règles de confidentialité et conditions d'utilisation '' du contrat Google Workspace, disponible en ligne.

Les services de GHS sont distribués sur deux fournisseurs cloud. Azure regroupe l'ensemble des instances sPAIEtacle / La Paie et GCP les applications web et le service Transat. Leur sécurité est gérée par les fournisseurs, dont les mesures sont explicitées sur leur site respectif :

- Google: https://cloud.google.com/docs/security
- Microsoft : https://www.microsoft.com/fr/trust-center

GHS s'engage également à mettre en place les bonnes pratiques de sécurité émises par Google et Microsoft pour la gestion des ressources Cloud.

Les clients du mode hébergé bénéficient de la protection de Microsoft Defender pour la surveillance des instances cloud Azure.

6.2 Suivi de protection contre les menaces

Le prestataire Everping utilise le MDM Jamf Pro afin de réaliser un suivi régulier de l'état de mise à jour des systèmes de protection des postes de travail (Windows et Macs) contre les programmes malveillants (versions, signatures antivirales).

Le prestataire Everping supervise également l'activité de l'EDR ThreatDown.

6.3 Correctifs de sécurité

GHS et ses sous-traitants maintiennent à jour tous les logiciels et les composants techniques dont ils ont la responsabilité. Cela concerne notamment :

- Tous les logiciels, bases de données, systèmes d'exploitation.
- Tous les équipements d'infrastructure de réseau.
- Tous les logiciels et systèmes d'exploitation des périphériques.

- Tous les logiciels ou infrastructures de sécurité.

6.4 Obsolescence des logiciels et des composants et suivi

GHS et ses sous-traitants gèrent et préviennent l'obsolescence de tous les logiciels et composants techniques sous leur responsabilité.

7. Gouvernance des données

7.1 Gestion des données

La sécurité de l'accès, le stockage, l'échange et la destruction des documents et des données sensibles est gérée par GHS.

GHS informe immédiatement ses clients en cas de perte de données.

Les disques de l'ensemble des postes de travail utilisés par les collaborateurs du GHS sont chiffrés.

Les disques des bases de données Transat et sPAIEctacle sont chiffrées au repos avec l'algorithme AES-256.

7.2 Cloisonnement des données

Un cloisonnement des données client est assuré par GHS. Un cloisonnement logique est assuré, a minima, pour l'ensemble des clients. A terme, GHS a prévu d'implémenter un cloisonnement logique avancé en utilisant une clé de chiffrement unique par client.

De plus, les données des clients de GHS sont accessibles uniquement par les personnes habilitées au sein du personnel de GHS.

7.3 Destruction et/ou restitution des données

GHS dispose d'un processus de restitution et destruction définitive des données de ses clients.

Ce processus comprend :

- La restitution des données au client.
- L'effacement des données de tout environnement (production)
- L'effacement des données sur les supports de sauvegardes.

Lorsque demandé par son client, GHS pourra fournir un rapport de destruction décrivant à minima :

- Le succès ou l'échec de l'opération.
- Les justifications/documents à fournir.

Avant la destruction définitive, le client aura la possibilité de réaliser un export de ses données depuis son compte.

7.4 Sauvegarde des données

GHS met en place un système de sauvegarde de ses données et des données de ses clients. Ce système de sauvegarde est basé sur les services de Google Cloud et Azure (Microsoft). Ces données sont isolées logiquement et physiquement du reste du SI.

Sur la plateforme web (GCP), GHS réalise 4 sauvegardes de fréquence différentes :

Fréquence	Rétention
Toutes les 6 heures	2 jours
Journalier	1 mois
Hebdomadaire	3 mois
Mensuel	6 mois

Sur la plateforme Azure, GHS réalise 4 sauvegardes de fréquence différentes :

Fréquence	Rétention
Toutes les 5 heures	15 heures
Journalier	1 mois
Hebdomadaire	3 mois
Annuelle	Jusqu'à la fin du contrat

7.5 Restauration des sauvegardes

GHS réalisé des tests de restauration des sauvegardes.

Les résultats de ces tests peuvent être communiqués aux clients sur demande.

7.6 Stockage des sauvegardes

Chaque sauvegarde est stockée avec redondance sur plusieurs serveurs européens : Belgique, France et Allemagne.

8. Sécurité des accès logiques

8.1 Gestion des identités

GHS applique les bonnes pratiques gestion des identités fondées sur :

- Les comptes nominatifs (identifiants individualisés).
- L'interdiction de comptes génériques.
- Le renommage ou la désactivation des comptes administrateurs par défaut.
- Un processus de gestion des arrivées / sorties et de gestion des comptes associés.

8.2 Authentification des utilisateurs

GHS met en œuvre des moyens pour garantir la sécurité et l'authentification des utilisateurs :

- La politique de Microsoft concernant le renouvellement et le blocage des mots de passe des comptes Microsoft Azure.
- La politique de GHS concernant le renouvellement et le blocage des mots de passe des comptes Transat.
- L'utilisation obligatoire du MFA pour les clients en mode hébergé.
- Utilisation du MFA optionnel (mais activé par défaut) pour les utilisateurs du service Transat.
- Configuration du MFA obligatoire pour les employés.
- La mise en place du SSO avec Google Workspace pour les applications internes à chaque fois que cela est possible.
- L'utilisation de gestionnaire de mots de passes sécurisés lorsque le SSO est impossible.

8.3 Gestion des comptes à privilèges

GHS met en œuvre une politique de gestion des comptes à privilèges conforme aux bonnes pratiques de sécurité. Cela se traduit par l'octroi d'autorisations selon le principe du moindre privilège via notamment :

- Une limitation du nombre d'administrateurs.
- Privilèges juste à temps pour le support.
- Journalisation des élévations de privilèges et des opérations effectuées.
- Accès à l'environnement de production restreint.

8.4 Protection des flux d'authentification

GHS s'assure du bon chiffrement de l'ensemble des flux d'authentification (utilisateurs et administrateurs).

8.5 Revue des comptes et des droits d'accès associés

GHS réalise une revue périodique des comptes et des droits d'accès aux ressources informatiques (serveurs, postes de travail, applications).

Le groupe met en œuvre des mesures pour s'assurer que les personnes autorisées à utiliser un système de traitement de données n'ont accès qu'aux données auxquelles elles sont autorisées à accéder, et que les DCP ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation pendant leur traitement, leur utilisation ou après leur enregistrement.

Une procédure de suppression des droits et des accès du collaborateur lors de son départ de l'entreprise est définie et effectuée.

8.6 Traçabilité des accès logiques

GHS met en place sur ses ressources (systèmes et applications) des logs permettant d'assurer l'imputabilité des actions réalisées. Ces journaux contiennent à minima les informations listées ci-dessous :

- L'identifiant du compte.
- L'ID des ressources.
- Les accès fructueux et infructueux aux ressources.
- L'origine des connexions.
- Les actions réalisées (modification, suppression, etc.).
- Les informations d'horodatage.

Ces journaux sont conservés pendant une durée de 1 an sur la plateforme GCP et 90 jours sur la plateforme Azure.

En matière de confidentialité des données, GHS met à la disposition de ses client les journaux des personnes concernées, pendant une durée maximum de 1 an.

8.7 Suivi des mécanismes de traçabilité des accès logiques

GHS assure le bon fonctionnement de son système de traçabilité et notamment :

- La collecte effective des logs.
- Une protection efficace des logs.

Le groupe met en œuvre des mesures permettant d'identifier et de vérifier ultérieurement si des DCP ont été modifiées ou supprimées des systèmes de traitement et, le cas échéant, par qui.

Par ailleurs, il maintient accessibles à tout moment les mécanismes de traçabilité mis en œuvre.

GHS informe ses clients de toute anomalie qui serait détectée dans ces registres de connexion.

9. Sécurité des communications

9.1 Cloisonnement de l'hébergement

Le SI bureautique est à logiquement et physiquement isolé du SI client GHS.

Un cloisonnement logique est assuré, a minima, pour l'ensemble des clients utilisant le mode hébergé.

9.2 Chiffrement des flux

L'ensemble des flux mis en œuvre par GHS sont chiffrés suivant l'état de l'art, cela concerne notamment les flux suivants :

- Tous les flux d'authentification des utilisateurs et des administrateurs ;
- Tous les flux relatifs à des accès distants ;
- Tous les flux de communications avec les web app et API.
- Tous les flux spécifiés comme sensibles.

9.3 Protection contre les intrusions

GHS met en œuvre les moyens et mesures techniques et organisationnelles nécessaires pour protéger son système d'information contre les intrusions.

Les mesures suivantes sont actuellement en place au sein du SI du GHS :

- Pare-feu WatchGuard afin de filtrer les flux entrants et sortant.
- Un serveur VPN.
- Un filtrage par adresse MAC sur le réseau interne.
- Isolation logique du wifi pour les invités et les employés.

GHS fait appel à un prestataire de sécurité (Viveris) pour assurer la bonne configuration des équipements de protection.

Ce prestataire réalise une revue complète des équipements tous les 3 mois.

9.4 Traçabilité des accès réseau

Les équipements réseau utilisés par GHS et ses sous-traitant consigne et protège les traces d'accès au réseau/service et protéger ces journaux qui comprennent au moins :

- L'adresse IP de l'émetteur ;
- L'adresse IP du destinataire ;
- La date ;

- L'heure ;
- Le cas échéant, l'identifiant de l'utilisateur.

Ces logs sont conservés pendant une durée maximale d'un (1) an en accord avec les exigences légales et réglementaires en vigueur.

10. Sécurité physique

10.1 Contrôle des accès physiques aux locaux

Les locaux de GHS sont équipés d'un dispositif de contrôle d'accès individuel dans le but de restreindre l'accès au site et salles serveurs uniquement au personnel autorisé.

10.2 Contrôle des accès physiques aux ressources techniques

Les locaux hébergeant les ressources techniques (ex : salles des équipements réseaux) sont équipés d'un dispositif de sécurité physique afin de limiter l'accès aux personnes habilitées.

10.3 Protection contre les vols

GHS met en place des mécanismes de protection contre le vol. Les ordinateurs portables Mac de l'entreprise sont équipés d'un système de traçage permettant de les géolocaliser.

Cette mesure de sécurité informatique permet de situer les ordinateurs en cas de vol ou de perte et ainsi d'être en mesure de les retrouver ou de supprimer les données à distance.

L'entreprise s'interdit tout traçage des appareils en dehors de ces deux cas de figure (perte ou vol). Les systèmes de localisation mis en place seront celui d'Apple (Localiser mon mac).

Les données liées à ces cas de figure seront conservées durant 24 heures (chez Apple). Les données relatives aux déplacements ne seront pas exploitées. Conformément à la loi informatique et libertés, les collaborateurs disposent d'un droit d'accès aux données liées à leur matériel sur simple demande et demeurent en mesure d'introduire une réclamation auprès de la CNIL en cas de désaccord avec l'entreprise.

10.4 Certification des sites d'hébergement des ressources techniques

Dans le cadre de ses activité, GHS fait appel à plusieurs hébergeurs. Voici les certifications de chacun des partenaires :

Certifications	Microsoft	Google CLOUD
ISO 27001	☑	☑
ISO 27017	☑	☑
ISO 27018	☑	☑
ISO 27701	☑	☑

ISO 50001		☑
RGPD	☑	☑
SOC 1,2,3	☑	☑
CSA STAR	☑	☑
HDS	☑	☑
PCI-DSS	☑	☑
EBA	☑	☑
ACPR PSEE	☑	☑
SWIPO		☑
C5	☑	☑
EIOPA		☑
ESMA		☑
EU Cloud Code of Conduct	☑	☑
EU Standard Contractual Clauses	☑	☑

11. Intégration de la sécurité dans les développements

11.1 Gestion de projet

L'équipe de développeurs de GHS travaille en méthode Agile. Ce mode de fonctionnement permet de mettre en place des mécanismes de validation et de vérification du code source à chaque étape avant sa mise en production.

11.2 Chaine d'intégration et déploiement continu

GHS a mis en place une chaîne d'intégration continue (CI) et de déploiement continu (CD) afin de restreindre l'accès aux environnements de production en direct uniquement aux interventions d'urgences réalisées par des administrateurs de la plateforme. Aucun développeur n'a accès aux environnements de productions en direct.

GHS a mis en place une double authentification pour l'accès au service de déploiement continu (CD). Les comptes d'administrations sur ce service sont nominatifs et le principe de moindre privilège est appliqué.

11.3 Architecture de développement

L'architecture de GHS, pour l'édition de nouvelles solutions, comporte deux environnements : développement et production. Aucune donnée des clients n'est utilisée dans l'environnement de développement. Toutes les opérations effectuées dans l'environnement de production sont journalisées et l'accès à celui-ci et à ses données est limité au personnel autorisé.

11.4 Sensibilisation

Les développeurs de GHS sont sensibilisés aux bonnes pratiques de sécurité par le biais de campagnes de sécurité générales, ainsi que de campagnes spécifiques à leurs opérations. Des bonnes pratiques de sécurité sont émises par le CTO, et l'application de ces pratiques est contrôlée lors des revues de code.

1.1 Signature du code

Toutes les briques logicielles livrées par GHS sont signées numériquement.

Les clés privées permettant la signature sont stockées sur des supports physiques sécurisés dédiés au stockage d'éléments cryptographiques.

2. Sécurité lors de la réversibilité

Après la fin du service (c'est-à-dire la fin du Contrat ou l'activation d'une clause de réversibilité par exemple), et pendant la durée de la phase de transfert, GHS s'engage à assurer le maintien du niveau de sécurité décrits dans les documents contractuels.