Un organigramme de la fonction et de la sécurité informatique existe et est régulièrement mis à jour

Il existe un plan de route pour la sécurité. Concernant les Sauvegardes, ACS2I a un back up chez eux (même back up des mots de passes avec cryptage).

Une personne est désignée pour piloter la "fonction informatique" :

- En interne : Un Directeur des Système d'Information (DSI) existe. Pour l'instant la fonction de RSSI, est assurée par la même personne [un responsable Cyber est présent au sein de la société (DSI)]

- En externe : Un Responsable suivant les applications externalisés est nommé, cet accompagnement est réalisé par la société ACS2I (accompagne sur les deux fonctions).

Un responsable de la sécurité informatique a été désigné :

- En interne, la RSSI est assuré pour l'instant par le DSI.

- En externe : En externe le RSSI est accompagné par la société ACS2I (accompagne sur les deux fonctions.)

Dans le cas de prestataires externes, le(s) contrat(s) liant l'entité auditée au(x) prestataire(s) sont adaptés aux besoins de l'entité. Réadaptation du contrat, réunion hebdomadaire pour donner les missions.

Une politique de sécurité est définie par l'entité et est soutenue, comprise et évaluée par la direction.

Une charte ou politique d'entreprise sur l'utilisation du Système d'Information est définie. Mais celle-ci est à améliorer. Un guide d'hygiène informatique est transmis aux salariés et il est complété.

La politique de sécurité est régulièrement revue et mise à jour du fait de la veille réalisée par le DSI.

Les acteurs de la sécurité sont formés de manière appropriée.

Le directeur administratif et financier est sensibilisé à la sécurité des systèmes d'information sur les données comptables et financières.

Un responsable est désigné mais il peut gérer plusieurs applications.

Les règles de contrôle d'accès sont formalisées dans un format "tout est interdit sauf" plutôt que "tout est permis sauf". En effet tout est verrouillé et les autorisations sont levées au cas par cas. Par exemple dans les magasins, les mails autorisés ne concernent que des échanges avec le siège et les prestataires.

Une personne a-t-elle été désignée pour décider de l'attribution, retrait, modifications des ressources du SI et des contrôles sont-ils effectués :

- pour chaque utilisateur (ou groupe) en interne : Il s'agit du DSI et son adjoint technicien. Les droits sont gérés uniquement au niveau du Service informatique

- pour des tiers : N/A

L'ensemble des responsables et des employés sont sensibilisés aux problématiques de sécurité, des communications sont réalisés et mise en place d'un ChatBot pour former et évaluer la cyber sécurité (25 cours seront dispensés et avec système incitatif de récompense).

Il n’existe pas de supervision des comptes d'administration du Système d'Information par la direction. Il y a une délégation au RSI.

La séparation des tâches est maintenue et assurée lors de la rotation des équipes, des vacances et du départ d'un personnel. Le service informatique est composé de 4 personnes en tenant compte de ACS2I. Le DSI s'assure que dans l'équipe, il y a toujours une personne sur les projets et une sur la partie technique.

"Le système d'information est basé sur un ERP « Entreprise Resource Planning » SIGMA pour la comptabilité et l’ERP CEGID Y2 Retail pour l'activité.

"En cas de conduite de projets, un RACI est-il mis en place ?

(L'acronyme RACI signifie : R : Responsible, A : Accountable, C : Consulted, I : Informed. Le RACI est un outil de formalisation des rôles et responsabilités pour chaque partie prenante au projet.)" Oui Un RACI est mis en place uniquement suivant l'importance du projet.

Existe-t-il des développements en interne ? Oui Néanmois les applications sont initiées en interne mais la réalisation technique est externalisée.

Si oui, les fonctions de développement informatique, de tests et d'exploitation sont-elles séparées et menées par du personnel différent ? Oui Les deux fonctions sont assurées par des personnes differentes. Exemple sur l'application concernant le suivi en devise.

---------- ////////////////////

2 - Risques liés à la protection des données

2.1 - Concernant les données générailes (autres que données personnelles) ////////////////////

Les données sont-elles référencées et classifiées ? (clients, fournisseurs, plan compable, etc.) Oui

Les données référentielles (données référencées et classifiées vues ci-dessus) apparaissent-elles sur une unique base de données ? (pas de doublon) Oui

Un nombre limité d'utilisateur a-t-il été défini pour créer, supprimer, mettre à jour les données référentielles (création d’un nouveau fournisseur, modification d’une fiche client, etc.) ? Oui 2 personnes au service Informatique.

Le logiciel comptable utilisé est-il hébergé en interne ? Non C'est hébergé en Saas.

Si non, les conditions de mises à disposition des données sont-elles prévues contractuellement ? Oui

Les logiciels utilisés par l'entité auditée interdisent-ils des exports de données vers des fichiers non sécurisés (fichier excel, fichier texte...) ? Non Suivant les profils d'utilisateur cela peut être réalisé.

"Les études, tests sont effectués sur des données différentes que celles servant à l'exploitation de l'entité auditée ?

(Important pour la garantie de l'intégrité des données)" Oui Les application metiers les plus importantes ont une base de Test, idem pour le site internet,...

Existe-t-il des mesures de sécurisation des échanges de données ? (sécurité du courrier électronique, échange entre applications internes et externes Oui Il y a des filtres pour identifier des receptions de RIB ou coordonnées bancaires.

"2.2 - Concernant le traitement des données à caractère personnel

(Définition : Une donnée à caractère personnel est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.)" ////////////////////

L'entité auditée s'est-elle enquérie de la réglementation européeenne sur la protection des données à caractère personnel ? Oui

L'entité a-t-elle engagé un processus de mise en conformité ? Oui

"L'entité auditée sensibilise-t-elle son personnel à la nouvelle réglementation ?

(Exemple : Mise en place d'une charte informatique, formations, etc…)" Oui

L'entité auditée tient-elle une documentation destinée à prouver sa conformité au RGPD ? Oui

"Un DPO est-il obligatoire et/ou a-t-il été désigné par l'entité auditée ?

(Art. 37 RGPD - DPO = Data Protection Officer ou délégué à la protection des données personnelles / Un DPO est obligatoire lorsqu'il s'agit d'un traitement effectué par un organisme public ou une autorité public, lorsque l'entité traite de données sensibles ou lorsque l'entité traite de données à grande échelle)" Oui Le DPO est externe, c'est le cabinet d'avocat qui a mis en place une cellule concernant cela.

"L'entité a-t-elle mis à jour sa politique de confidentialité ?

(Permet de respecter les obligations d'information de l'intéressé sur le sort de ses données)" Oui

"Une politique de cookie a-t-elle été définie ?

(Par exemple : En cas d’utilisation de cookies publicitaires, de mesure d’audience ou de traceur de réseaux sociaux, un bandeau est présent en page d’accueil du site et permet à l'internaut de paramétrer ces cookies)" Oui Dans l'activité Web, les cookies sont traités par le prestataire web (COLORS prestataire qui intégre SHOPIFY (Technologie utilisée)

En cas de recours à un système de vidéo-surveillance, une information des personnes est-elle visible ? Oui

L'entité a-t-elle mis à jour ses contrats ? Oui

"L'entité a-t-elle déterminé si elle était responsable de traitement, co-responsable ou sous-traitant de chaque traitement identifié ?

(Art. 24, 26, 28 RGPD - Définition : Le responsable de traitement est celui qui fixe les finalités du traitement de la donnée récoltée)" Oui Le responsable Informatique

2.2.1 - En tant que responsable de traitement / co-responsable ////////////////////

"L'entité a-t-elle défini et/ou identifié les différentes nature de données à caractère personnel récoltées par elle ?

(Exemple : Nom, prénom, adresse, image, adresse IP, données bancaires, données fiscales, données sensibles, logs, données relatives à la vie familiale)" Oui

"L'entité auditée traite-t-elle de données sensibles, de données concernant des mineurs ou effectue-t-elle un traitement à grand échelle et a-t-elle mis en place des mesures particulières de récolte de ces données ?

(Art. 8,9,10 RGPD - Définition : """"""""""""""""""""""""""""""""à grande échelle"""""""""""""""""""""""""""""""" : traitements « qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées »)" Oui

L'entité a-t-elle identifié les différents traitements de données à caractère personnel qu'elle utilise ? Oui

L'entité a-t-elle identifié la finalité de chacun de ces traitements ? Oui

Les données collectées sont-elles pertinentes et nécessaires au regard de la finalité du traitement ? Oui Il s'agit de mise en place de cartes de fidélité.

"Les transferts internes/externes ou les interconnexions entre les différents traitements ont-ils été repérés ?

(Remarque : L'objectif étant d'éviter que les bases de données aux mêmes finalités se multiplient.)" Oui

"La base légale du traitement a-t-elle été identifiée ?

(Consentement, contrat, obligation légale, intérêt légitime…)" Oui

La preuve des consentements est-elle disponible ? Oui Accord données lors de la souscription.

Une durée de conservation des données à caractère personnel a-t-elle été définie ? Oui

"Une procédure de suppression des données ou d'anonymisation est-elle prévue ?

(Anonymisation = procédure visant à rendre inexploitable la donnée (cryptage...))" Oui

"L'entité auditée doit-elle et a-t-elle mis en place une Etude d'Impact sur la vie privée (DPIA) ?

(Art.35 RGPD)" Non

Les droits de l'intéressé d'accès, de rectification et d'opposition lui ont-ils été communiqués et sont-ils réellement mis en place au sein de l'entité ? Oui

Le responsable de traitement peut-il être sollicité en cas de demande du propriétaire de la donnée récoltée ? Oui

"Un registre des données personnelles traitées par l'entité auditée est-il tenu et régulièrement mis à jour ?

(Art. 30 RGPD - NB : pas obligatoire pour entreprise de moins de 250 salariés mais fortement recommandé.)" Non En reflexion

Les données sont-elles accessibles en dehors de l'UE ? Non

"Si oui, les partenaires respectent-ils le RGPD ?

(RGPD = """"""""""""""""""""""""""""""""Règlement Général sur la Protection des Données"""""""""""""""""""""""""""""""" ou GDPR en anglais pour """"""""""""""""""""""""""""""""General Data Protection Regulation"""""""""""""""""""""""""""""""")" N/A

Les violations sont-elles notifiées à la CNIL ? N/A

"2.2.2 - En tant que sous-traitant

(Art. 28 RGPD)" ////////////////////

L'entité auditée est-elle sous-traitante en terme de données à caractère personnel ? Non

"Si oui, tient-elle un registre des données sous-traitées et répond-elle aux exigences du RGPD en tant que sous-traitant ?

(Conformément au RGPD, le sous-traitant doit tenir un registre des traitements qu'il effectue sur instructions du responsable du traitement)" N/A

2.2.3 - L'entité auditée fait appel à un sous-taitant ////////////////////

"L'entité auditée fait-elle appel à des sous-traitants ?

(Au sens du RGPD un sous-traitant est toute personne qui traite des données à caractère personnel pour le compte du responsable de traitement sur instruction documentée de ce dernier)" Non Utilisation d'une application pour les mailling mais en interne.

Si oui, l'entité a-t-elle défini contractuellement les exigences en termes de protection des données avec son partenaire ? Le contrat avec le prestataire comprend-il les différentes clauses exigées par le règlement ? N/A

---------- ////////////////////

3 - Risques liés à la continuité d'activité pour l'entité auditée

"Les procédures de sauvegarde sont-elles mises en place ?

(Plans de sauvegarde, délai de rétention, cryptage des données…)" N/A

Existe-t-il un plan d'urgence approprié en matière de système d'information pour assurer la poursuite du fonctionnement de l'entité auditée en cas de sinistre ? Oui Sauvegardes externalisées

"Existe-t-il une copie externe à l'infrastructure pour les données critiques ?

(Sauvegarde dans un espace """"""""""""""""""""""""""""""""Cloud"""""""""""""""""""""""""""""""" sécurisé ou autre…)" Oui

Des tests de restauration sont-ils régulièrement effectués ? Oui

Les outils cloud repondent-ils aux besoins de l'entreprise en matière de procédure de sauvegarde des données ? Oui

Pour chaque ressource informatique mise en place (infrastructure, système d'information, ressource humaine intellectuelle), l'entreprise auditée a-t-elle défini leur degrès de criticité en observant ? ////////////////////

- un niveau de service minimum, N/A

- un niveau d'indisponibilité minimum, N/A

"- les ressources indispensables.

(Ressources humaines et/ou matérielles)" N/A

Dans le cadre d'un nouveau projet, l'entité auditée a-t-elle pris en compte les dépendances inhérentes au projet en termes de technologie, d'infrastructure et de période d'intégration pour son implantation au sein de l'entitée ? Oui

Le système d'information est-il compatible avec les évolutions de l'activité de l'entité auditée ? Oui

"Les sécurités mises en place contre les risques de dégats des eaux, d'incendie et de vol sont-elles suffisantes ?

(Contrôle d'accès (par badge par exemple), lieu du local/salle informatique, détection incendie…)" Oui

"Le système d'alimentation électrique permet-il d'assurer la continuité de l'activité ?

(Présence d'onduleurs, de groupe électrogène ou autres)" Oui

Les systèmes d'exploitation de l'ensemble du parc informatique (serveurs, postes...) sont-ils maintenus à jour par leurs éditeurs ? Oui Maintenance pour toutes les applications et ERP.

Les logiciels utilisés par l'entité sont-ils maintenus à jour par leurs éditeurs ? Oui

Des contrats sont-ils définis pour la maintenance des matériels et logiciels ? (extension de garantie, contrat de dépannage...) Oui

L'entité utilise-t-elle des applications spécialisées (en matière de production, gestion...) ? Oui

Si oui, existe-t-il un support utilisateur suffisant pour ne pas bloquer la continuité d'activité de l'entité auditée ? Oui

---------- ////////////////////

4 - Risques quant à l'exploitation informatique

Existe-t-il un inventaire du système d'information ? Oui

"Existe-t-il une cartographie du système d'information ?

(Liens entre les différents éléments du SI)" Oui

"Les procédures d'exploitation sont-elles documentées ?

(Procédure d'arrêt, démarrage, sauvegardes…)" Oui Un certains nombre sont documentées mais pas toutes.

"Les changements (Achats, Remplacements) apportés aux matériels, logiciels, systèmes d'exploitation sont-ils anticipés, contrôlés et approuvés ?

(Etudier les modalités d’installation et de validation des nouveaux systèmes informatiques pour déterminer leur incidence sur le risque inhérent. L’entreprise doit avoir mis en place des procédures de gestion de projet pour permettre une mise en place sans risque d’un nouvel outil ou d’une nouvelle application.)" Oui

Les prestations de services par des tiers sont-elles encadrées et gérées ? Oui

"Existe-t-il une cohérence et une homogénéité des technologies utilisées par l'entité (Système d'exploitation, base de données, postes de travail, standardisation des configurations des matériels et logiciels) ?

(La multiplication des technologies peut engendrer des coûts de formations, de maintenance, des problèmes d'adaptabilité entre les systèmes...)" Oui Le logiciel Paie n'est pas integré aux autres applications. Les remontées sont automatiques.

"L'intégrité des systèmes et la confidentialité des données sont-elles préservées par une protection appropriée contre les codes informatiques non autorisés et/ou malveillants, présents :

(Système Anti-virus, anti-ransomware par exemple)" ////////////////////

- sur les équipements de l'entreprise Oui

- sur les équipements personnels des utilisateurs connectés au système d'information. Oui

Existe-t-il un antivirus sur tous les équipements de l'entité auditée ? Oui

Si oui, sont-ils mis à jour ? Oui

Existe-t-il une politique de déploiement des mises à jour concernant : ////////////////////

- les systèmes d'exploitation Oui

- les logiciels et/ou applications Oui

"- les micrologiciels embarqués sur les matériels actifs (firmware)

(définition """"""""""""""""matériels actifs"""""""""""""""" : tout le matériel comportant un équipement électronique chargé d'assurer la répartition des signaux entre les différentes branches d'un réseau informatique. (ex : hubs ou des switches, convertisseurs, bornes wifi...))" N/S

"Existe-t-il une gestion centralisée et remontée automatique d'alertes concernant :

(Remontées par mail par exemple)" ////////////////////

- les antivirus Oui

- les systèmes de sauvegarde Oui

- les équipements de l'infrastructure informatique (serveurs, routeurs, parefeu...) Oui

"Existe-t-il un filtrage d'URL pour les utilisateurs ayant accès au système d'information ?

(définition """"""""URL"""""""" : de l'anglais Uniform Resource Locator, littéralement « localisateur uniforme de ressource ») c'est ce que l'on appelle l'adresse web. Filtrage rendant inaccessible des sites à caractères illicites)" Oui

"Existe-t-il des mesures de sécurisation des échanges de données ? (sécurité du courrier électronique, échange entre applications internes et externes, prise de contôle à distance)

(Utilisation d'un système de cryptage, connexion VPN, SSH, utilisation d'API sécurisée, ...)" Oui

"Les ressources de l'entreprise accessibles en ligne par le public, font-elle l'objet de mesure de sécurité spécifiques, régulièrement auditées ?

(Dans le cas ou l'entité auditée héberge des sites internet dans son infrastructure)" Oui