

21630 POMMARD

03.80.22.61.85

383967334600016

Conformité RGPD : Registre général

Sensibiliser les utilisateurs

- Informer les manipulateurs (Informer et sensibiliser les personnes manipulant les données.)

Avez-vous informé les personnes utilisant des données sur la RGPD ?	Oui cette mesure a été mise en oeuvre.
---	--

- Charte informatique (Rédiger une charte informatique et lui donner une force contraignante en l'annexant au contrat de travail ou au règlement intérieur + la faire signer aux salariés : engagement de confidentialité, aver)


Disposez-vous d'une charte informatique contraignante?	La charte informatique a été envoyée aux salariés
--	---

Authentifier les utilisateurs

- Login à chaque utilisateur (Définir un identifiant (login) unique à chaque utilisateur)

 Avez-vous défini un identifiant unique pour chaque utilisateur ?	Non cette mesure n'a pas encore été mise en oeuvre.
--	---

- politique de mot de passe (Adopter une politique de mot de passe utilisateur conformes aux recommandations de la CNIL (au moins 8 caractères comportant majuscules, minuscules, chiffres, caractères spéciaux) Faire changer les mots de passe après réinitialisation & limiter le nombre de tentatives d'accès à un compte)

 Avez-vous mis en place un politique de mot de passe complexe incluant une réinitialisation et limitation de tentatives de connections ?	Non cette mesure n'a pas encore été mise en oeuvre.
---	---

Gerer les habilitations

- Définir les profils d'habilitation

 Avez-vous défini un profil d'habilitation ?	Non cette mesure n'a pas encore été mise en oeuvre.
---	---

- Gestion des permissions d'accès

 Les accès obsolètes sont-ils systématiquement supprimés ?	Non cette mesure n'a pas encore été mise en oeuvre.
---	---

- Révision annuelle des habilitations (Réaliser une revue annuelle des habilitations)

Effectuez-vous une révision annuelle des personnes habilitées ?	Non cette mesure n'a pas encore été mise en oeuvre.
---	---


Tracer les accès et gérer les incidents

- Prévoir un système de journalisation

Avez-vous un système permettant l'enregistrement des actions quotidiennes effectuées sur le système informatique ?	Oui cette mesure a été mise en oeuvre. Windows Serveur : Journal d'événements. Isagri : Traçabilité du logiciel par les logins.
- Informer les utilisateurs du système de journalisation (Informer les utilisateurs de la mise en place du système de journalisation (par charte informatique, clause contrat de travail ou message d'information spécifique))	
Le personnel est-il informé de la mise en place d'un système de journalisation ?	Oui cette mesure a été mise en oeuvre. via la charte
- Protéger les équipements	
Avez-vous mis en place un système de protection des équipements de journalisation et des informations journalisées ?	Oui cette mesure a été mise en oeuvre.
- Prévoir des procédures (Prévoir les procédures pour les notifications de violation de données à caractère personnel)	
Existe t-il une procédure en cas de violation des données à caractère personnel ?	Oui cette mesure a été mise en oeuvre. Oui le responsable du traitement informera la CNIL sous 72h via le formulaire spécifique fourni par celle-ci.

Sécuriser les postes de travail


- Verrouillage des sessions (Verrouiller automatiquement les sessions)

 Existe t-il un système de verrouillage automatique des session en cas de non utilisation durant un temps donné ?	Non cette mesure n'a pas encore été mise en oeuvre.
---	---

- Utiliser des antivirus (Utiliser des antivirus régulièrement mis à jour)

Disposez-vous d'anti-virus professionnelle ?	Oui cette mesure a été mise en oeuvre.
Votre anti-virus est-il à jour ?	Oui cette mesure a été mise en oeuvre.

- installer un pare feu (installer un logiciel pare feu)

 Disposez-vous d'un pare-feu ?	Non cette mesure n'a pas encore été mise en oeuvre. En cours
--	---

- Recueillir les accords avant toute intervention (Recueillir l'accord de l'utilisateur avant toute intervention sur son poste)

Existe-t-il une procédure permettant de recueillir l'accord de l'utilisateur avant toute intervention sur son poste ?	Oui cette mesure a été mise en oeuvre.
---	--

Sécuriser l'informatique mobile (pc portables, smartphones, tablettes..)

- Prévoir des moyens de chiffements (Prévoir des moyens de chiffements des équipements mobiles)

Disposez-vous de moyens de chiffement pour les équipement mobiles ?	Non cette mesure n'a pas encore été mise en oeuvre. Pas concerné
---	---

- Sauvegarde des données (faire des sauvegardes ou synchronisations régulières des données)

Avez-vous un moyen de sauvegarde ou synchronisation des données ?	Non cette mesure n'a pas encore été mise en oeuvre. pas concerné
La sauvegarde ou synchronisation est-elle régulière ?	Non cette mesure n'a pas encore été mise en oeuvre. Pas concerné

- Verrouillage des smartphones (exiger un secret pour le verrouillage des smartphones)

Les smartphone dispose-t-ils d'un mode de verrouillage par code Pin ?	Oui cette mesure a été mise en oeuvre.
---	--

Protéger le réseau informatique interne

- Limiter les flux réseau (Limiter les flux réseau au strict nécessaire)

 Disposez-vous des équipements nécessaires à la limitation des flux réseau ?	Non cette mesure n'a pas encore été mise en oeuvre.
--	---

- Sécuriser les accès distants (sécuriser les accès distants des appareils informatiques nomades par VPN)

L'accès à vos appareil distant est-il sécurisé par un VPN ?	Non cette mesure n'a pas encore été mise en oeuvre. Pas concerné.
---	--

- Sécuriser les accès sans fil (mettre en œuvre le protocole WPA2 OU WPA2-PSK pour les réseaux wifi (ces mécanismes sécurisent notamment les connexions sans fil et empêchent les accès non autorisés à votre réseau de communication)

Avez-vous mis en œuvre un mécanisme de sécurisation de vos réseaux Wifi ?	Oui cette mesure a été mise en oeuvre. Oui différenciation Public - privé
---	--

sécuriser les serveurs

- Limiter l'accès (limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées)

Les accès aux outils et interfaces d'administration sont-ils limités aux personnes habilitées ?	Oui cette mesure a été mise en oeuvre. via un agent de supervision. Accès régit par la charte info
---	---

- Installer les mises jour (installer sans délai les mises à jour critiques (permettant de colmater une faille de sécurité majeure sur vos équipements fixes ou portables))

Les mises à jours critiques sont-elles installées sans délais ?	Oui cette mesure a été mise en oeuvre. géré par Soft Avenir
---	--

- Assurer une disponibilité des données (Assurer une disponibilité des données)

Les données sont-elles disponible et accessibles à tout moment ?	Oui cette mesure a été mise en oeuvre.
--	--

Sécuriser les sites internet

- Utilisez le protocole TLS (Utilisez le protocole TLS et vérifiez sa mise en oeuvre)

 Le site internet est-il uniquement disponible en https ?	Non cette mesure n'a pas encore été mise en oeuvre. A faire appliquer à l'éditeur du site
---	--

- Vérification mot de passe et identifiant (vérifier qu'aucun mot de passe ou identifiant ne passe dans les URL (adresses des pages internet consultées))

Vous êtes-vous assuré qu'aucun mot de passe ou identifiant ne passe dans les URL ?	Oui cette mesure a été mise en oeuvre.
--	--

- Contrôler l'accès au site (Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu (qu'ils n'aient pas accès, de façon accidentelle, à une partie interdite du site))

Vous êtes vous assurés que le site internet ne présente aucune faille permettant à une utilisateur d'accéder à un contenu, une partie du site interdite ?	Oui cette mesure a été mise en oeuvre.
---	--

- Consentement pour les cookies (Mettre un bandeau de consentement pour les cookies non nécessaires au service)

Existe t-il un bandeau de consentement pour les cookies non nécessaires aux services ?	Oui cette mesure a été mise en oeuvre.
--	--

Sauvegarder et prévoir la continuité d'activité

- Effectuer des sauvegardes régulières (Effectuer des sauvegardes régulières)

Effectuez-vous de façon régulière des sauvegardes de vos données ?	Oui cette mesure a été mise en oeuvre. Une sauvegarde quotidienne, une mensuel et une à distance (sur demande).
--	--


- Stockage des sauvegardes (Stocker les supports de sauvegarde dans un endroit sûr)

 Disposez-vous d'un moyen de sauvegarde crypté et externalisé en Union Européenne ?	Non cette mesure n'a pas encore été mise en oeuvre. A étudier
---	--

- Sécuriser le transfert des sauvegardes (Prévoir les moyens de sécurité pour le transfert des sauvegardes)

 Lors des transferts, vos données sont-elles cryptées selon la norme militaire ?	Non cette mesure n'a pas encore été mise en oeuvre. Non puisque pas de sauvegarde externalisée
--	---

- Prévoir et tester la continuité d'activité (Prévoir et tester régulièrement la continuité d'activité (s'assurer que les sauvegardes des données fonctionnent et instaurer, même sommairement , une procédure à suivre en cas d'attaque portant atteinte à la poursuite des activités))

 En cas d'attaque portant atteinte à l'entreprise, avez-vous prévu une procédure ?	Non cette mesure n'a pas encore été mise en oeuvre.
Testez-vous régulièrement cette procédure (restauration des données entre autre) ?	Oui cette mesure a été mise en oeuvre.

Archiver de manière sécurisée

- Modalités d'accès aux données archivées (Mettre en œuvre des modalités d'accès spécifiques aux données archivées)

 L'accès aux données sauvegardées est-il régit par une procédure ?	Non cette mesure n'a pas encore été mise en oeuvre.
--	---

- Destruction des archives obsolètes (Détruire les archives obsolètes de manière sécurisée)

Les données sauvegardées sont-elles détruites de manière sécurisée lorsqu'elles sont devenues obsolètes ?	Oui cette mesure a été mise en oeuvre.
---	--

Encadrer la maintenance et la destruction des données

- Enregistrer les interventions de maintenance (enregistrer les interventions de maintenance dans un document)

 Disposez-vous d'un registre permettant de répertorier les interventions de maintenance ?	Non cette mesure n'a pas encore été mise en oeuvre.
---	---

- Encadrer les interventions des tiers (Encadrer par un responsable de l'entreprise les interventions par des tiers)

L'intervention de tierce personne au sein de votre entreprise est-elle encadré par une personne ?	Oui cette mesure a été mise en oeuvre.
---	--

- Mise au rebut du matériel ou départ d'un salarié (effacer les données de tout matériel avant sa mise au rebut ou en cas de départ du salarié)

Disposez-vous d'une procédure afin d'effacer les données en cas de mise au rebut d'un matériel, ou en cas de départ d'un salarié ?	Oui cette mesure a été mise en oeuvre. Mis au rebut par nos soins après destruction physique du disque dur
--	---

Gérer la sous traitance (vos prestataires)


- Le contrat du prestataire (prévoir une clause spécifiques dans les contrats des prestataires qui traitent des données personnelles pour votre compte)

Disposez-vous d'un contrat avec vos prestataires qui traitent des données personnelles pour votre compte ?	Oui cette mesure a été mise en oeuvre. Oui via la charte
Ce contrat contient-il des clauses définissant les conditions dans lesquelles le prestataire s'engage à effectuer les opérations de traitement des données ?	Oui cette mesure a été mise en oeuvre. Oui dans la charte informatique

- Restitution et de destruction des données (prévoir les conditions de restitution et de destruction des données)


Avez-vous déterminé avec votre sous-traitant les conditions de restitution ou de destruction des données ?	Oui cette mesure a été mise en oeuvre.
--	--

- Vérifier l'efficacité des garanties (s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites...))

 Vos prestataires disposent-ils d'attestation de conformité à la RGPD ?	Non cette mesure n'a pas encore été mise en oeuvre. Non un courrier leur demandant des justification leur a été adressé. Attente des retours
---	--

Sécuriser les échanges avec d'autres organismes

- Politique de mots de passe complexe (politique de mots de passe complexe)

 Votre politique concernant les mots de passe est-elle conforme à la CNIL ? (au moins 8 caractères comportant majuscules, minuscules, chiffres, caractères spéciaux)	Non cette mesure n'a pas encore été mise en oeuvre.
--	---

- vérification du destinataire (s'assurer qu'il s'agit du bon destinataire)

Disposez-vous d'une liste de destinataire prédéfini lors d'envoi de données personnelles ?	Oui cette mesure a été mise en oeuvre.
--	--

- Transmission de données sensibles (pour les données sensibles, transmettre le code secret d'ouverture d'un fichier lors d'un envoi distinct, et si possible, par un canal différent)

Disposez-vous d'une procédure d'envoi pour les données sensibles (envoi du fichier et mot de passe par un canal différent et par 2 envoi distincts) ?	Non cette mesure n'a pas encore été mise en oeuvre.
---	---

Encadrer les développements informatiques

- Respect de la vie privée (proposer des paramètres respectueux de la vie privée aux utilisateurs (ne prendre que des données strictement nécessaires à l'objectif poursuivi))

Les données collectées sont-elles uniquement des données nécessaires ?	Non cette mesure n'a pas encore été mise en oeuvre. pas concerné
--	---

- Encadrer les zones de commentaires (éviter les zones de commentaires ou les encadrer strictement de manière à éviter les dérives ou que des personnes insèrent des données sensibles: positions politiques, syndicales, race...))

Disposez-vous de zones de commentaire ?	Non cette mesure n'a pas encore été mise en oeuvre. pas concerné
Ces zones de commentaires sont-elles encadrée afin qu'il ne puisse y avoir de dérive, ou d'insertion de données sensibles ?	

Protéger les locaux

- Restreindre les accès aux locaux (restreindre les accès aux locaux au moyens de portes verrouillées)

L'accès à vos locaux est-il restreint ?	Oui cette mesure a été mise en oeuvre. Oui avec digicode
---	---

- Installer des alarmes (installer des alarmes anti intrusion et les vérifier périodiquement)

Disposez-vous d'un système anti-intrusion ?	Oui cette mesure a été mise en oeuvre.
---	--

- Impression et destruction des supports

Disposez-vous d'un système de verrouillage par code ou badge sur votre copieur afin d'éviter que les données éditées soient consultables sur celui-ci?	Cette proposition est à l'étude et fera l'objet d'une prochaine action.
Détruisez-vous tous les documents comportant des données personnelles (papier, CD, carte bleue, ...) à l'aide d'un broyeur à coupe croisée?	Oui je dispose d'un broyeur à coupe croisée (norme DIN 66399 P4 ou supérieure).