RGPD - Règlement Général de la Protection des Données

CONTEXTE

RGPD, EVOLUTION NORMATIVE EN MATIERE DE PROTECTION DES DONNEES / DATA PROTECTION

> l'attente du législateur : une démonstration de bonne foi & d'efficacité à priori

- Applicable depuis mai 2018, le RGPD a pour objectif de **responsabiliser les acteurs** autour de la notion centrale de *Data Protection* (protection des données).
- Les entreprises doivent faire preuve de ***compliance*** (conformité) : il est attendu qu'elles se placent d'elles-mêmes en conformité avec la réglementation européenne et locale, sous peine de se voir infliger de lourdes sanctions administratives.
- Le RGPD introduit une nouvelle méthodologie qui révolutionne le système probatoire en matière de protection des données à caractère personnel : l'***accountability*** (responsabilité) est l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.
- Ainsi, le responsable de traitement comme le sous-traitant doivent être en mesure de **démontrer leur conformité**, à tout moment et par tous moyens.

ETAT D'AVANCEMENT DU DOSSIER AU SEIN DE MUST INFORMATIQUE

> la politique de Must : 6 points prioritaires mis en action

- **Désigner un DPO** (Data Protection Officer) conforte l'entreprise dans le principe de « Data Gouvernance ».
  Sa mission est d'assurer une mise en conformité de l'activité en considérant les risques (sanctions pénales / sanctions Cnil, de défiance ou publicité néfaste).
  Son rôle est celui de conseiller le responsable de traitement et servir d'interface auprès des sous-traitants.

- **Documenter sa sécurité** par la mise en place d'un **référentiel de sécurité** est la traduction concrète de l'**engagement de l'entreprise** pour sa mise en conformité.
  Cette documentation sert d'élément de preuve à la démonstration de l'opérationnalité de mesures techniques et organisationnelles au sein de l'entreprise.
  *Le référentiel sécurité est composé du **Registre des traitements**, du **Registre des sous-traitants** et du **Plan d'action issu du PIA**.*

05 55 48 49 50 - PARC D'ACTIVITÉS OCEALIM - 2 BIS RUE LOUIS BLÉRIOT 87270 COUZEIX

RGPD - Règlement Général de la Protection des Données

- **Exprimer la volonté du dirigeant et motiver l'adhésion du personnel** est l'accélérateur d'une évolution des pratiques en profondeur.
  La compliance est un principe d'organisation et de développement interne et externe de l'entreprise : cette approche consistant à bien faire dès l'émergence d'un projet, le montrer simplement et rapidement valorise les échanges générant une nouvelle forme de cohésion des salariés et des collaborateurs.
  Simultanément, l'engagement des dirigeants est un socle initial qui doit être connu et reconnu. Le personnel est donc sensibilisé par des sessions d'informations et de formations ciblées et pertinentes.

- **Adopter une démarche ''*Privacy by Design*''** est le pendant technique de cette logique : il s'agit de penser l'outil dès les premières étapes de conception en intégrant d'office les contraintes liées à la protection des données – ''***Privacy by default***''**-** et d'inciter ainsi une utilisation et des pratiques conformes aux attendus.
  Suivant une logique de responsabilisation, chaque acteur doit s'assurer de la **conformité des traitements** qu'il envisage de mettre en œuvre. Cela implique la mise en place de **mesures organisationnelles et techniques** spécifiques et d'**associer le DPO** à chaque stade de conception d'un nouveau service.

  Dispositifs de pseudonymisation ou de chiffrement*, application du* ***principe de minimisation des données*** *(seules les données nécessaires à la finalité doivent être collectées) devront également être mis en œuvre en vertu de ce principe général.*

- **Anticiper les risques** et **auditer ses traitements** pour **garantir une conformité effective et une opérationnalité concluante.**
  L'évaluation des risques par un travail de **documentation** et d'**audit** permet de **cartographier les traitements** afin d'élaborer un registre des activités de traitement, mais également d'identifier et de hiérarchiser les risques pesant sur ces traitements.
  Le document de formalisation de l'analyse des risques est identifié comme le **PIA -** *Privacy Impact Assessment*.
  Le DPO aidé d'autres intervenants peut accompagner la démarche par une description objectivée des opérations de traitements et des risques inhérents.

- **Sécuriser ses relations avec les partenaires sous-traitants** renforce la politique interne. Les bons programmes de compliance contribuent à préserver une image positive de l'entreprise soucieuse de la sécurité de son personnel et de ses clients. La mise en place et la **communication de la politique de sécurité** est un facteur de confiance pour les clients, les partenaires et les fournisseurs car l'entreprise montre comment elle s'investit pour limiter les risques auxquels elle est exposée.
  La sécurisation de ces relations se traduit aussi par la mise en place des ***Data Protection Agreements*** – DPA –qui clarifient les **obligations respectives** de chacune des parties au traitement par la **formalisation contractuelle**.

05 55 48 49 50 - PARC D'ACTIVITÉS OCEALIM - 2 BIS RUE LOUIS BLÉRIOT 87270 COUZEIX

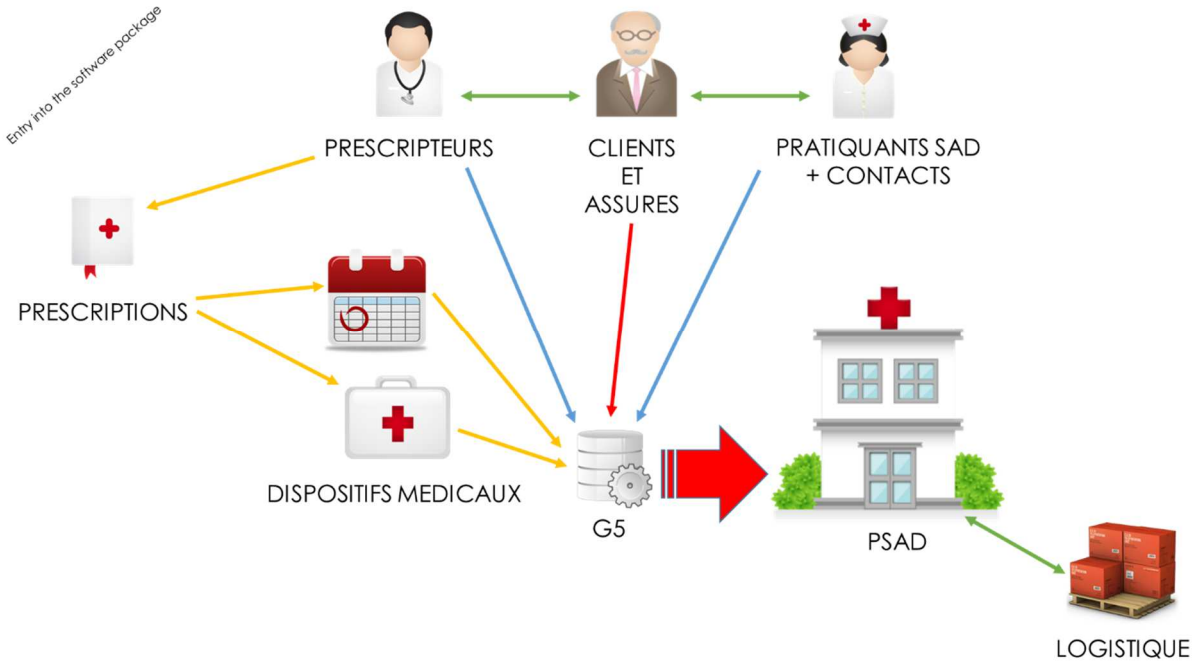
RGPD - Règlement Général de la Protection des Données

MUST, EDITEUR G5 & Qrieu

> Qualifier & Cartographier pour identifier et pondérer les risques à un niveau acceptable,
> Contrôler le flux de data, l'utilisation, l'archivage, la suppression et la portabilité des DCP **dans les règles de l'art**.

CARTOGRAPHIE DES DCP (G5 / Qrieu)

- Une **donnée à caractère personnel** est toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation (NIR), n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).
- Une **donnée sensible** (*sensitive data*) est une information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou l'orientation sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.



- ***Nous avons identifié la provenance, la destination et le flux des données et fixé le critère majeur d'identification du risque selon la nature de ces données :***

en vert pas de DCP,

en bleu peu de DCP ou DCP à caractère peu sensible ou contrôlé,

en orange DCP présentes ou risque existant,

en rouge DCP à caractère sensible et ou risque élevé

RGPD - Règlement Général de la Protection des Données

Nous mettons en place des **mesures de pondérations** permettant de porter le **risque résiduel à un niveau acceptable**.

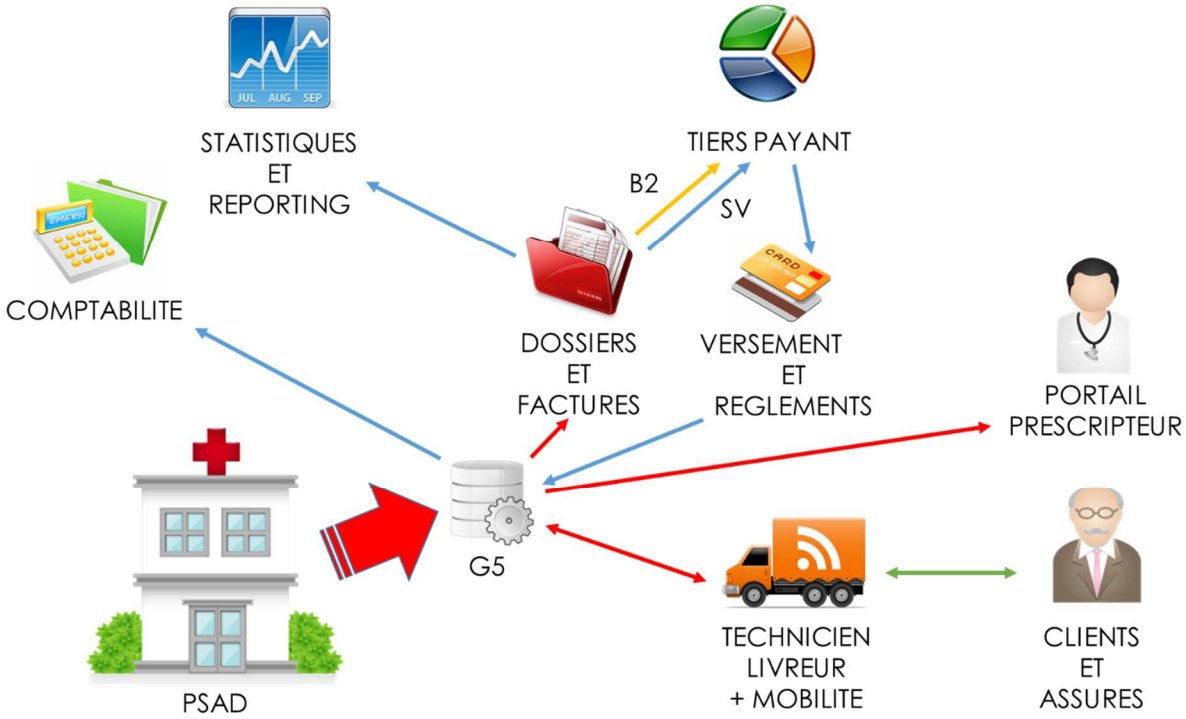
- Ces mesures sont classées en 3 axes principaux :

. **Axe juridique**
Conformité réglementaire au regard des salariés MUST, partenaires et sous-traitants, *notamment :*
respect des temps d'archivage légaux, mention de confidentialité dans les contrats …

. **Axe organisationnel**
Procédures internes afin d'éviter les abus d'usage des DCP

. **Axe logique**
La protection informatique de la solution MUST se décline sur deux thèmes :

- Protection des données dans les fonctions du logiciel et dans le flux des données exportées,
  Protection des données entrantes et sortantes du logiciel via les différents canaux informatiques.



ROAD MAP DU SERVICE DEVELOPPEMENT : ACTIONS A MENER SEQUENCEES EN 3 PHASES

2ème semestre 2018
Anonymisation des sauvegardes récupérées chez les clients
Mot de passe obligatoire sur les comptes utilisateurs G5
Gestion des mots de passe dans la G5
Possibilité d'extraire les données liées à un contact ou un patient
Identification des champs libres comme DCP
Communication chiffrée des échanges avec le serveur
Recommandations pour chiffrer les supports (Mobilité)

1er semestre 2019
Archivage / purge
Gestion des signatures
Export et visualisation de certains types de documents
Mobilité : mise en veille automatique
Connexions multiples simultanées
Sécurisation de l'intranet
Prise d'appel entrant MUST : purge de la base des ITV au-delà de 5 ans

2ème semestre 2018
Demande de consentement
Sécurisation de l'intranet MUST et suivi des modifications
Personnalisation des mots de passe du compte admin des BDD
Accès à l'intranet depuis le PRM

05 55 48 49 50 - PARC D'ACTIVITÉS OCEALIM - 2 BIS RUE LOUIS BLÉRIOT 87270 COUZEIX

RGPD - Règlement Général de la Protection des Données

ROAD MAP DU S&R (HEBERGEMENT G5) - ACTIONS A MENER SEQUENCEES EN 3 TEMPS : 2ème semestre 2018, 1er semestre 2019, 2ème semestre 2019

En vue de la protection des risques concernant les DCP, il est prévu de mettre en place une politique de sécurité logique et une maintenance accrue sur le périmètre de notre département service et réseaux.

→ Quelques exemples

- Sécurisation de l'hébergement par la mise en place d'un VPN
- Gestion renforcée des logins aux différents soft utilitaires et mise en place d'un espace de stockage sécurisé des mots de passe (VAULT)
- En interne une restriction d'accès aux DCP en fonction des besoins et du niveau d'accréditation

RGPD - Règlement Général de la Protection des Données

MUST Sous-Traitant : focus sur le Service Support [Hotline] & l'Hébergement

> une responsabilité partagée avec obligation de performance avérée

Dans le cadre délimité de la gestion des DCP et sur les périmètres d'activités du service support de hotline et du service d'hébergement, Must est en position de sous-traitant.

Dans ce contexte, **les clients peuvent réaliser des audits de notre activité** afin de vérifier la réalité de notre performance en matière de sécurité des données.
Comme pour les autres périmètres d'activité, nous devons mettre à jour nos contrats de prestations : il nous faut ici mentionner cette possibilité d'audit ainsi que vos modalités d'intervention sur site.

Le tableau ci-dessous propose un focus sur les singularités de nos responsabilités mutuelles selon le sens de la relation de sous-traitance.

MUST PRESTATAIRE	MUST SOUS-TRAITANT	
EN TANT QU'EDITEUR G5 / QRIEU	SERVICE SUPPORT : HOTLINE	HEBERGEMENT

- Notre **DPO** est dès à présent l'interlocuteur privilégié de nos clients qui peuvent désigner un référent RGPD au sein de leurs services.
- **« Data processing agreement »** : nous devons réviser nos contrats de prestations, *mentionner la relation de sous-traitance et les obligations respectives.*

Dans le cadre du RGPD nous pouvons réaliser des audits de l'activité de nos clients et vérifier la conformité de leurs actions visant à protéger les DCP via la solution G5 / Qrieu.
Dans ce cadre, la documentation obligatoire doit être présentée.

Les clients peuvent réaliser des audits de notre activité
- **Notre DPO devra alors présenter le Registre de traitements des sous-traitants et le PIA.**
- **Les mesures correctives et d'amélioration portées au PIA ferons l'objet d'un recueil de bonnes pratiques.**
- **Un recueil des procédures du progiciel permettant la portabilité, la suppression, la rectification et l'archivage des données sera à votre disposition.**

- Notre **Référent sécurité informatique** complète la mission du DPO.
- **En situation d'audit, il présente la cartographie des traitements**
- **Le DPO présente le PIA**
- **Le Responsable du traitement vous présente la politique de sécurité informatique de MUST et sa mise en œuvre à travers la Roadmap.**

05 55 48 49 50 - PARC D'ACTIVITÉS OCEALIM - 2 BIS RUE LOUIS BLÉRIOT 87270 COUZEIX

RGPD - Règlement Général de la Protection des Données

DROITS DES PERSONNES & OBLIGATIONS INCOMBANT AUX RESPONSABLES DE TRAITEMENT

La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

- de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
- de la finalité poursuivie par le traitement auquel les données sont destinées ;
- du caractère obligatoire ou facultatif des réponses ;
- des conséquences éventuelles, à son égard, d'un défaut de réponse ;
- des destinataires ou catégories de destinataires des données ;
- des droits dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ;
- le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;
- de la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

POUR CONCLURE

> un élan international, projet ambitieux, qui nous entraîne ensemble vers le haut aux prix d'efforts réels mais éclaire la mentalité de nos activités et surtout simplifie (-era bientôt!) nos quotidiens de travail.

A l'échelle de nos structures, certes l'investissement sur ce dossier du RGPD est significatif, principalement en mobilisation d'esprit et en temps homme.

De notre point de vue, c'est un stade de professionnalisation dont il a été intéressant de s'emparer.

Nous serons à vos côtés pour vous transmettre les moyens opérationnels susceptibles de transformer cette envie d'aller de l'avant en agissements opérationnels.

05 55 48 49 50 - PARC D'ACTIVITÉS OCEALIM - 2 BIS RUE LOUIS BLÉRIOT 87270 COUZEIX