SPOT IT

YOUR SECURITY & NETWORK LAYER

RGPD DANS LE RÉSEAU DES PHARMACIENS : LA PHARMACIE

Recommandations vers le Règlement Général Européen de Protection de Données

Table des matières

1 RECOMMANDATIONS

Dans cette section, nous abordons d'abord des recommandations par thème sur la manière de traiter des données à caractère personnel dans des situations spécifiques. Ensuite nous proposons des documents afin de répondre aux ercommandations proposées dans la rubrique précédente.

Conjointement à ces recommandations, nous mentionnons, dans la mesure du possible, la source de l'interprétation des recommandations et où vous pouvez trouver plus d'informations sur un sujet spécifique, si nécessaire.

1.1 Recommandations spécifiques pour les pharmacies

1.1.1 ENREGISTREMENT DE NOUVEAUX PATIENTS

1.1.1.1 TRAITEMENT MINIMUM DES DONNÉES (ARTICLE 5.1C DU RGPD)

Au moment de l'enregistrement d'un nouveau patient, il est nécessaire d'enregistrer un nombre de données à caractère personnel, basées notamment sur le chapitre 7 du AR du 21 janvier 2009, à savoir :

- Nom, prénom du prescripteur;
- Nom, prénom du patient;
- Numéro d'identification à la sécurité sociale (NISS) ;
- Date de naissance (faisant partie du numéro NISS) ; ces données sont nécessaires pour le remboursement de certains médicaments, comme par exemple les vaccins. Cette nécessité trouve son origine dans les obligations légales de l'AR du 10 août 2005.

A côté de ces éléments légalement obligatoires, des données personnelles supplémentaires sont enregistrées :

- L'adresse du patient, qui peut être recueillie si le patient y a marqué son accord ;
- L'e-mail et le numéro de téléphone, qui peut être recueillis si le patient y a marqué son accord ;
- La photo du patient qui peut être receuillie si le patient y a marqué son accord, ou dans le cas où le pharmacien enregistre la photo pour s'assurer de l'identification correcte du patient. Cette correcte identification vaut uniquement comme intérêt légitime si un but plus important que celui de la simple identification est lié, par exemple pour éviter un abus en vérifiant si c'est la bonne personne qui vient chercher le médicament.

Des données supplémentaires peuvent uniquement être recueillies si elles sont pertinentes dans le cadre de l'obligation de minimalisation des données.

Dans le cadre de la délivrance des médicaments qui ne sont pas soumis à prescription et de la délivrance d'autres produits parapharmaceutiques, on peut enregistrer uniquement les données que si le patient y a marqué son accord. Cette collecte doit être limitée au minimum et le patient doit être informé du fait que les données demandées ne sont pas fournies obligatoirement.

1.1.1.2 DÉLAI DE CONSERVATION (ARTICLE 5.1 – E) RGPD)

Les données à caractère personnel ne sont jamais supprimées du système informatique. Il existe une obligation légale au niveau de la conservation des données dans un but pharmaceutique. Ces données doivent être conservées dans la pharmacie pour un délai de 10 ans au minimum. Après ces données peuvent être conservées encore 20 ans et après 30 ans, les données doivent être détruites. Pour donner une suite correcte à ces délais de conservation, une procédure sur la conservation et la supression doit être rédigée. Cette procédure doit préciser quels sont les délais de conservation légaux, de quelle manière les données seront conservées, qui est responsable pour la suppression des données et comment ceci sera effectué.

La procédure peut éventuellement être intégrée dans le Code de Conduite Sectoriel.

Il est également avisé de vérifier si le système informatique peut automatiquement indiquer quelles données sont enregistrées dans le système depuis 30 ans.

Une alternative serait d'anonymiser automatiquement les données après un délai de 30 ans.

Recommandation : activer l'anonymisation automatisée ou avoir un écran pop-up pour la suppression des données ainsi qu'intégrer les modalités de suppression dans une procédure ou le Code de Conduite Secotriel.

1.1.1.3 EXACTITUDE ET QUALITÉ DES DONNÉES (ARTICLE 5.1- d) ET 16 RGPD)

L'enregistrement des données s'effectue par la lecture de la carte d'identité avec un lecteur de carte eID afin de pouvoir garantir l'exactitude et la qualité des données à caractère personnel. L'enregistrement de la carte d'identité ne se fait qu'une seule fois lors de la première visite. Le nombre d'enregistrement de la carte d'identité dépend d'une pharmacie à l'autre.

Enregistrer la carte d'identité est une mesure proactive du pharmacien lui permettant de garantir que les données d'assurabilité sont à jour. Il est souhaitable de reparcourir cette procédure tous les 6 mois. Le patient peut bien entendu toujours demander de rectifier les données qui le concernent. Dans ce cas, le pharmacien peut à nouveau enregistrer les données de manière manuelle ou en utilisant un lecteur de carte eID.

Recommandation : vérifier avec les maisons de soft s'il est possible de définir un rappel automatique après un délais de 6 mois pour relecture d'enregistrement de la carte d'identité.

1.1.2 LIVRAISON DE PRODUITS A DES TIERS

Le pharmacien reçoit régulièrement la demande de délivrer des médicaments à un tiers. Ceci peut être un membre de la famille, un proche, un prestataire des soins à domicile, un voisin ou un autre tiers.

Dans ces cas, il faut pouvoir démontrer le **consentement ou le mandat** du patient/concerné avant que le pharmacien puisse délivrer les médicaments à un tiers. Ceci afin de pouvoir garantir qu'il existe une base légitime pour le traitement des données dans le cadre de l'article 6 RGPD.

Recommandation : prévoir que l'on peut démontrer que le consentement ou le mandat du patient/concerné ont été obtenus avant la délivrance des médicaments par un tiers.

1.1.3 PARTICIPATION À DES ÉTUDES SCIENTIFIQUES

Les patients peuvent participer à des études scientifiques. Le patient donne sa permission au pharmacien par son« **consentement éclairé** », mais le pharmacien désidentifieles données avant de les transférer à des tiers. Cela implique que le pharmacien attribue un code au patient, ce code est communiqué au tiers et le pharmacien est capable de lier le code aux données du patient.

En cas de transfert de données à des tiers dans le cadre d'études scientifiques, les points d'attention doivent être respectés :

- Si les parties tierces demandent les initiales et la date de naissance, il convient devoir s'il n'existe pas une autre possibilité permettant d'avoir des informations équivalentes. Transférer ces données peut compromettre l'anonymité des données.
- Les documents de consentement doivent être vérifiés conformément aux conditions *de* de transparence et informations à fournir comme reprises dans les articles 12-14.

En transférant les données à des parties tiers pour des études scientifiques, les recommandations suivantes sont d'application :

1. Informer le patient si les données seront transférées sous un format non-anonyme;
2. Reprendre cette information dans le formulaire de consentement ou dans la déclaration de protection des données avant la signature du formulaire;
3. Inscrire les garanties nécessaires dans un contrat avec la partie que s'occupe de l'étude scientifique. Ce contrat doit être conclu avant que le transfert des données ne soit effectué;
4. Le consentement éclairé doit être conservé dans la pharmacie de manière sécurisé, c.à.d. dans une armoire fermée ou un espace clos.

1.2 IT et sécurité[1]

1.2.1 MOTS DE PASSE

En démarrant le système informatique, la pratique en pharmacie démontreque cela se résume à entrer son nom d'utilisateur et un mot de passe, sauf si on utilise un badge. Si on se sert d'un badge pour se connecter, il est néanmoins nécessaire d'entrer un mot de passe en combinaison avec le badge pour lancer certains modules (p.ex. la caisse).

En pratique, il ne semble pas y avoir de restrictions sur la qualité des mots de passe et il ne faut jamais choisir un nouveau mot de passe ; dans certains cas un mot de passe n'est pas nécessaire pour redémarrer.

Recommandation : rédiger une politique des mots de passe au niveau du secteur (possibilité de l'intégrer dans la Code de Conduite Sectoriel). En rédigeant la politique des mots de passe, il faut accorder une attention particulière aux éléments suivants :

- Utilisation obligatoire d'un nom d'utilisateur et mot de passe pour démarrer le système informatique et cela afin d'éviter que des personnes non-autorisées ne puisse avoir accès au système;
- Utilisation obligatoire des nom d'utilisateurs / comptes individuels pour garantir la traçabilité des manipulations;
- En choisissant un mot de passe, il faut imposer qu'un mot de passe fort soit établi (au moins 8 caractères, dont au moins 1 majuscule, au moins 1 minuscule, 1 chiffre et 1 caractère spécial) ;

Recommandation : conseiller l'utilisation de phrases en mot de passe et non de mots de passe simples ;

- Forcer les utilisateurs à choisir un nouveau mot de passe tous les 90 jours (tous les 3 mois) ;
- Ne choisissez pas de mots de passe qui sont faciles à deviner comme votre nom ou date de naissance ;
- Imposer qu'un mot de passe ancien ne puisse pas être utilisé à nouveau ;
- Un mot de passe est personnel, ne pas le partager avec quelqu'un d'autre, et cela même avec une personne du service technique (IT).

1.2.2 ACCÈS DIGITAL

Dans le système informatique il y a plusieurs modules et il est possible d'assigner différents rôles. Dans certaines pharmacies, on distingue le compte de l'administrateur de celui d'un utilisateur normal. Cependant, cette distinction n'est pas appliquée partout et par conséquence tout le monde a les mêmes droits.

Recommandation : pour déterminer les personnes et leurs droits respectifs dans une application, il est nécessaire d'introduire un système de rôles selon le principe du moindre privilège.

Afin d'arriver à un niveau de sécurité élevé l'on préfère une combinaison de possibilités différentes :

- Limiter l'accès aux modules différents dans le système informatique aux personnes qui en ont vraiment besoin pour exercer leur travail. Ceci est possible en couplant l'accès au compte ou en utilisant un système de badge couplé à l'accès à un badge appartenant à une seule personne ;
- Faites toujours la distinction entre des comptes d'administrateur et des comptes normaux ;
- Rédiger une politique d'accès qui est basée sur des rôles ;
- Limiter les possibilités d'exporter les données ;
- Masquer si possibles les données;
- Rédiger une politique décrivant les champs libres de l'application qu'il est permis d'utiliser afin d'éviter qu'on utilise ces champs pour stocker des données à caractère personnel ;
- Imposez un time-out automatique de la session après p.ex. 30 minutes d'inactivité et imposer de réactiver son accès p.ex. lorsqu'une session dure plus de 8 heures afin d'éviter des accès non souhaités;
- Imposer le verrouillage de l'écran automatiquement après p.ex. 15 minutes d'inactivité.

[1] PIA Knowledge bases, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

1.2.3 TRAÇABILITÉ DES DONNÉES DU PATIENT

Par « traçabilité », nous entendons, en cas de perte de données, la possibilité de démontrer quand, comment et par qui le problème a été initié et quelles étapes s'en sont suivies. Dans le secteur des pharmacies, actuellement la traçabilité est peu garantie. Dans certaines pharmacies un système de badge pour se logger dans le système informatique existe mais dans la pratique ce système de badge n'est que peu appliqué systématiquement. Ce système garantit pourtant une forme de traçabilité.

Si la bonne utilisation de ce système est remise en question, en tout cas ce système est plus efficace qu'un système nécessitant de se reconnecter au système à chaque fois. Il appartient au pharmacien de choisir les mesures de sécurité qu'il souhaite mettre en place puisqu'il est libre de déterminer le niveau de sécurité il souhaite atteindre.

Recommandation : mettre en place un système de badge comme mesure de sécurité et une solution pour la traçabilité

1.2.4 DOCUMENTS PHYSIQUES

Dans la pharmacie, il y a pas mal de documents physiques présents qui contiennent des données à caractère personnel (p.ex. des prescriptions, des schémas de médication, des contrats, des attestations, des mandats, etc.).

Recommandation : les documents doivent être gardés dans une armoire fermée ou un espace clos qui n'est pas accessible pour des personnes non-autorisées. Dans le cas où on travaille avec un système d'archivage, les mêmes mesures de sécurité doivent être d'application pour les archives. Les clés des armoires ou des archives doivent être conservées dans un endroit séparé et ne doivent pas rester sur la serrure.

1.2.5 POLITIQUE DU BUREAU PROPRE

L'introduction d'une politique du bureau propre n'est pas obligatoire, mais est cependant fortement conseillée. Une telle politique peut être directement liée à l'obligation de devoir garder des documents physiques dans une armoire fermée ou un espace clos. Par l'introduction d'une politique du bureau propre, on réduit les chances de fraudes et pertes de données parce que les documents seront ainsi moins accessibles.

Recommandation : rédigez une politique du bureau propre au niveau du secteur, implémentez-le et exercez des contrôles fréquents.

Une politique du bureau propre contient au moins les éléments suivants :

- Installez des armoires fermables ou un espace sécurisé pour garder les documents et informez vos collaborateurs de l'endroit où l'on peut retrouver et garder les documents ;
- Evitez des documents sur papier et, si possibles, digitalisez les documents;
- Evitez d'imprimer les documents ;
- Obligez l'emploi d'un destructeur de papiers ou l'emploi d'une corbeille à papier fermée (destrabox) ;
- Verrouillez toujours le poste de travail en se levant et quittant l'espace pour éviter que des personnes non autorisées puissent voir des données à caractère personnel;
- Eteignez toujours le poste de travail en fin de journée ;
- Veillez à la fin de la journée à ce que tous les documents soient conservés de manière sécurisée ;
- Exercez des contrôles fréquents afin de garantir que la politique est suivie.

1.2.6 SHADOW-IT

Shadow-IT (parfois Rogue-IT) est un terme utilisé pour désigner des systèmes d'information et de communication réalisés et mis en œuvre au sein d'organisations sans approbation de la direction des systèmes d'informations. Certains pharmaciens utilisent la conservation en ligne (cloud ou nuage informatique) pour diverses raisons, y compris la conservation des contrats. Dans les cas où on ne l'utilise pas, il est possible de stocker des documents dans le cloud en utilisant des applications comme Dropbox et ou entre autre Onedrive personnelle. Ces méthodes de stockage posent des risques de sécurité.

Recommandation : introduisez une politique sectorielle concernant le choix de stockage en ligne et l'emploi autorisé. Ceci peut p.ex. être Office 365 avec OneDrive.

Essayez de réduire les risques inhérents au stockage en ligne en :

- Faire un choix autour du fournisseur préféré de cloud. Cela peut être par exemple Office 365, y compris OneDrive ;
- Composer une liste des types de documents peuvant ou non être stockés en ligne ;
- Eviter de stocker des documents non-permis sur des serveurs en ligne en bloquant le téléchargement de ces documents au niveau du firewall ;
- Encrypter tous les documents qui contiennent des données à caractère personnel et qui sont stockés en ligne.

1.2.7 BACKUPS

Les backups des données doivent également être au maximum sécurisés. La sécurisation est possible par des mesures techniques d'un côté, mais également en sécurisant physiquement les backups.

Il faut aussi se pencher sur le délai de conservation des données des backup. Si les données à caractère personnel sont reprises dans les fichiers backup, il n'est pas permis de conserver ces fichiers plus longtemps que nécessaire et il convient de veiller à ce que ces données soient à jour. Lorsque cela est possible, il est préférable d'écraser ces données après un délai de 30 jours vu que de cette manière, les modifications suivants les demandes des patients/personnes concernées (dans le cadre des articles 12-20 GRPD) sont reprises dans les données en backup.

Recommandation : encryptez les données en prenant les backups comme partie du procédé de backup si la méthode utilisée pour le backup le permet. Le logiciel de backup Veeam prend en charge le cryptage. Si les fichiers backup sont stockés sur des disques externes, il faut les protéger en les conservant dans une armoire fermée ou un endroit clos. Les clés des armoires ou des archives doivent être conservées dans un endroit séparé et ne doivent pas rester sur la serrure.

Recommandation : déterminez le délai de conservation des fichiers backup et écrasez-les après une période de 30 à 90 jours au maximum.

1.2.8 UTILISATION DE E-MAILS

L'utilisation d'e-mail pour la communication entre les prestataires de soins est largement répandue. De cette façon, lors de problème avec les plateformes de eHealth, RSW, Abrumet ou Vitalink, les schémas de médication peuvent être envoyés par e-mail. Il peut également s'agir d'informations sur l'usage abusif de médicaments (fausses prescriptions), des préparations magistrales, des résultats du labo, des vols par certains patients, etc. L'utilisation d'e-mail est largement répandue, mais est sujet à des risques comme l'interception de la communication, infection de virus et autres risques qui posent un problème pour la sécurité.

Bien qu'il soit impossible d'éliminier entièrement l'utilisation d'e-mail étant donné les risques, il va de soi qu'il faut l'éviter autant que possible.

Un autre risque en utilisant les e-mail est le choix par le pharmacien de l'application pour l'envoi de mails (GMAIL, Yahoo, Outlook, etc.). Il existe des différences dans le niveau de sécurité et le risque de perte des données peut augmenter en fonction de ce choix. Ces différences se situent au niveau technique (chiffrage, filtres pour spam- et ransomware), mais aussi au niveau géographique le RGPD demande de s'interroger sur le lieu de conservation des données.

Si le choix du fournisseur s'est porté sur GMAIL, il faut réfléchir à changer de fournisseur comme Outlook ou Exchange. Outlook offre la possibilité de chiffrer les mails par défaut par moyen de TLS (Transport Layer Security). Si on utilise Office 365, cela est possible via l'extension gratuite « Azure Information Protection » ce qui permet chiffrer automatiquement le trafic des courriels.

A côté du chiffrement du trafic des e-mails, il est possible d'imposer des règles « Data Loss Prevention (DLP) ». Les règles DLP sont utilisées pour indiquer quel type de documents peuvent être envoyés en externe et quel type de documents doivent être interceptés parce qu'ils posent un risque de perte de données.

Recommandation : limitez l'utilisation d'e-mails pour l'envoi des données à caractère personnel ou confidentiel et utilisez des plateformes comme Vitalink et eHealth.

Essayez de réduire les risques inhérents au trafic d'e-mails en :

- Choisir une application d'e-mails sécurisée ;
  Conseil : déployer Office 365
- Appliquer« Secure e-mail » pour chiffrer les e-mails et le trafic ;
- Eviter l'usage des boîtes aux lettres « groupe ». Appliquez une séparation stricte entre la boîte aux lettres personnelle et la boîte aux lettres utilisée en groupe et n'utilisez la boîte aux lettres en groupe que par exemple pour la facturation.

Remarque : des recommandations additionnelles concernant le choix d'une plateforme d'e-mails externe ont été reprises dans la section 1.3.2.3 de ce document.

1.2.9 USAGE DU TÉLÉPHONE ET DES FAX

Lors de l'échange d'informations à caractère confidentiel ou secret, notamment lors d'appels téléphoniques, il y a lieu de s'assurer qu'une personne non autorisée à cet effet ne puisse pas suivre la conversation.

Recommandation : il faut s'assurer que les conversations téléphoniques ne puissent pas être suivies par des personnes non autorisées.

Afin d'éviter que les données soient échangées de manière incorrecte, les numéros de fax et les adresses e-mails externes ne peuvent être repris que s'ils proviennent de listes officielles ou ont été directement données par le destinataire.

Avant d'envoyer un fax contenant des données confidentielles, il faut en informer le destinataire. Après la transmission, la réception du fax doit être confirmée par téléphone. L'expéditeur veille également à ce que l'accusé de réception soit retiré du télécopieur.

1.2.10 ORDINATEURS ET SERVEURS LOCAUX

Chaque pharmacien dispose d'un poste de travail pour les traitements quotidiens. Celui-ci peut être un desktop ou un laptop. De plus, des serveurs sont également prévus permettant la conservation des données.

Recommandation : assurez-vous que ces appareils soient munis de mesures adéquates de sécurité permettant de protéger les données qui s'y trouvent[2].

En déterminant un niveau de sécurité adéquat, pensez aux éléments suivants :

- Rédigez - si ce n'est pas encore fait – une politique décrivant l'usage adéquat des ordinateurs (IT Security policy) ainsi que les mesures à prendre pour sécuriser et maintenir la sécurité des ordinateurs. Si cette politique est déjà écrite, la version actuelle peut être soumise à une révision.
- Installez les dernières mise-à-jours des logiciels de sécurité (*) ;
- Installez un logiciel Antivirus et -malware et mettez régulièrement les définitions de virus à jour (*) ;
- Imposez une politique de mot de passe fort[3] (*) ;
- Assurez-vous ,lors de l'installation d'un logiciel, que le système vous demande de vous connecter avec un utilisateur ayant les droits d'administrateur ;
- Chaque ordinateur a la possibilité de connecter des outils externes (Tools). Il est conseillé de restreindre l'utilisation des clés USB. Il est possible de limiter l'utilisation des outils pour le stockage de masse sans bloquer la fonctionnalité d'une souris ou d'un clavier.
- Evitez le vol de ces appareils en les gardant dans une armoire fermée quand ils ne sont pas utilisés ou de les verrouiller avec une serrure ;
- Chiffrez le disque dur pour s'assurer que les données sont illisibles en cas de vol ou de perte (*)
  Recommandation : Activer Microsoft BitLocker via Active Directory
- Prévoyez des procédures pour la destruction sécurisée des appareils et disques durs en fin de vie (*) ;
- Appliquez un loggin sur l'ensemble afin de pouvoir poursuivre chaque notification possible du logiciel, de la sécurisation ou du système et assurez-vous que personne ne peut modifier les fichiers log (*) ;
- **Recommandation : fournir un syslog chiffré SSL/TLS (Cisco)**

[2] PIA Knowledge bases, CNIL, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf, section 19.1
[3] PIA Knowledge bases, CNIL, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf, section 8.4

- Stockez les fichiers log à un endroit qui n'est accessible que pour des personnes autorisées et analysez régulièrement les événements loggés (*) ;
- **Recommandation : mise en œuvre de la gestion des événements de sécurité et d'information (Security and Information Event Management - SIEM) - Rapid7**
- La connexion externe sur ces machines doit s'effectuer par un canal sécurisé (VPN) (*).

Les suggestions indiquées avec un (*) sont considérées comme le minimum à prévoir pour atteindre un niveau de sécurité acceptable. Un bon nombre de ces mesures sont déjà d'application chez certains pharmaciens, mais ne sont pas encore d'application dans l'ensemble du secteur.

1.2.11 RÉSEAU

Le réseau forme la base du bon fonctionnement des ordinateurs. Chaque utilisateur a accès au réseau ainsi qu'aux données disponibles sur le réseau.

Recommandation : soyez certain qu'aucun ordinateur non-géré ou non-sécurisé peut se connecter sur le réseau et les données.

Prenez les mesures suivantes :

- Rédigez une politique qui décrit l'usage justifié du réseau ainsi que les mesures à prendre pour sécuriser et maintenir la sécurité du réseau ;
- Installez une solution firewall pour protéger tout le trafic venant et allant vers l'internet (*) ;
- Segmentez ou isolez les ordinateurs qui contiennent des données à caractère personnel ;
- Ne permettez aucune connexion non-sécurisée. N'utilisez que des connexions codées (HTTPS, SFTP, SSL) (*) ;
- Implémentez des règles « Data loss prevention » pour éviter des pertes de données ;
- Sécurisez les connexions sans fil (*) ;
- Utilisez des logging et monitoring pour détecter des pertes de données ou des situations non-sécurisées et pour en être averti automatiquement.

Les suggestions indiquées avec un (*) sont considérées comme le minimum à prévoir pour atteindre un niveau de sécurité acceptable. Un bon nombre de ces mesures sont déjà d'application chez certains pharmaciens, mais ne sont pas encore d'application dans l'ensemble du secteur.

1.2.12 CONSERVATION DIGITALE DE DONNÉES

Les données sont conservées sur différents systèmes informatiques et applications.

Recommandation : soyez certain que la conservation de données est suffisamment sécurisé.

Prenez les mesures suivantes :

- Rédigez une politique qui décrit la conservation sécurisée de données;
- Centralisez la conservation de données afin de ne devoir sécuriser que cette source ;
- Limitez la conservation de données sur des appareils non-sécurisés en installant une solution « Data Loss Prevention » ;
- Implémentez le chiffrage pour sécuriser la source (*) ;
- Vérifiez la possibilité de chiffrer des fichiers et les bases de données pour éviter la divulgation non-autorisée de données ;
- Vérifiez la possibilité d'implémenter une solution « Digital Rights Management » qui peut limiter le traitement de données non-autorisé par voie de restriction en matière d'utilisation (usage, conservation, envoie, impression) ;
- Implémentez un système de conservation sécurisée en fonction du partage de fichiers (*) ;
- Evitez de transmettre des documents et utilisez des liens vers les documents concernés qui se trouvent sur un endroit de conservation partagée.

Les suggestions indiquées avec un (*) sont considérées comme le minimum à prévoir pour atteindre un niveau de sécurité acceptable. Un bon nombre de ces mesures sont déjà d'application chez certains pharmaciens, mais ne sont pas encore d'application dans l'ensemble du secteur.

1.2.13 IMPRIMANTES

Les pharmaciens ont besoin d'une imprimante pour imprimer les preuves d'achat. De plus, il y a plusieurs logiciels qui permettent d'exporter et imprimer des rapports et des documents. Si personne ne prend ces documents, il est possible que les documents disparaissent ou soient accessibles pour des personnes non-autorisées. Dans ce cas, on parle d'une perte de données potentielle.

Recommandation : limitez les impressions au minium et veillez à ce que la personne qui a imprimé un document vienne tout de suite chercher son document.

Ci-dessous vous trouverez un aperçu des mesures à prendre pour augmenter le niveau de sécurité :

- Rédigez une politique sur l'utilisation autorisée des imprimantes, dans laquelle il est bien spécifié qu'on n'imprime que les documents nécessaires et qu'on doit toujours immédiatement ramasser les documents imprimés ;
- Du point de vue technique, « Secure Printing » peut réduire ce risque. Quand l'option est activée, une tâche d'impression ne peut être lancée qu'après avoir introduit un code pin sur l'imprimante. Il existe aussi des systèmes de badge ;
- Des imprimantes récentes ont suffisamment de mémoire pour correctement imprimer des documents substantiels. Cette mémoire contient également l'historique de ce qui a été imprimé et cet historique peut également être utilisé abusivement. En chiffrant ou vidant automatiquement cette mémoire, ce risque peut être diminué ;
- Verrouillez l'accès aux personnes non-autorisées dans le menu de configuration des imprimantes et modifiez le mot de passe par défaut de l'imprimante réseau ;
- Faites appel à une société spécialisée pour la destruction des imprimantes qui ne sont plus en service afin d'éviter que des données puissent être retirées de la mémoire de l'imprimante.

1.2.14 SUPPORT

Lors d'une intervention du service ou support IT sur le matériel ou un logiciel, il est possible que des données à caractère personnel soient visibles. L'intervention peut se faire sur place ou à distance en prenant le contrôle de l'écran (TeamViewer)

Recommandation : respectez les dispositions légales en nommant une tierce partie qui pourra avoir accès aux données à caractère personnel traitées.

- Concluez un contrat de sous traitance dans le cadre d'article 28(3) RGPD ;
- Concluez un accord de non-divulgation pour garantir la confidentialité ;
- Evitez de partager des données à caractère personnel si ce n'est pas nécessaire ;
- Soyez certain qu'une personne accompagnante soit toujours présente durant les activités de support.

1.2.15 SUPPRESSION / DESTRUCTION SÉCURISÉ DES DOCUMENTS

Tous les documents contenant des données à caractère personnel doivent être détruits d'une façon sécurisée.

Recommandation : utilisez un destructeur de papiers ou déposez les documents dans une corbeille à papier fermée (destrabox), qui sera collectée régulièrement par une firme spécialisée en destruction de documents.

Ce service est fourni par différents fournisseurs, mais est aussi offerts par certaines associations professionnelles. Si on fait appel à un fournisseur, la collecte et la destruction doivent être considérées comme un traitement, ce qui implique qu'un contrat de sous-traitance doit être conclu avec ce fournisseur.

1.2.16 SUPPRESSION / DESTRUCTION SECURISÉE DE DONNÉES INFORMATIQUES

Dans le cadre de la stratégie de conservation de données, il est nécessaire de rédiger une politique sur la suppression / destruction des données informatiques.

Supprimer des données en les jetant dans la corbeille (DEL, SHIFT. Suppr.) et après vider la corbeille n'est pas suffisant.Formater le disque dur n'est pas suffisant pour complètement supprimer des données.

Ecraser des données est une bonne méthode pour supprimer / détruire des données.

Même lorsque les supports informatiques sont détruits, ce n'est pas suffisant. Ce problème peut être résolu en achetant un logiciel pour supprimer / détruire des données ou pour démagnétiser le support d'information.

Contactez toujours une société spécialisée qui peut démontrer qu'elle dispose des licenses pour supprimer / détruire des données informatiques.

Recommandation : rédigez des procédures sur la suppression / destruction des données sur des supports informatiques. Pensez à des PC's, des laptops, des serveurs, des photocopieuses, des imprimantes, des télécopieurs, des PDA's (assistant éléctronique de poche), des téléphones, des ordiphones, des clés USB et des caméras digitales.

- Déterminez ce que vous voulez faire avec des appareils de traitement de l'information hors d'usage : les donner à un tiers ?, les vendre ?, les détruire et récycler ?;
- Le choix de la méthode de suppression variera en fonction du choix de ce que vous voulez faire de ces appareils hors d'usage. (écraser, suppression par un logiciel ou démagnétiser) ;
- Si le support informatique sera ré-utilisé par un tiers, il faut être absolument certain que toutes les données soient vraiment bien détruites ;
- Toujours demandez la preuve de la destruction des données.

1.3 Recommandations concernant les cartes de fidelité & Bulletins d'information.

En organisant et en exerçant des activités de marketing, il faut prêter une attention spéciale au traitement des données à caractère personnel qui y sont liées. Dans cette section, nous faisons des recommandations en fonction du type d'activités de marketing et proposons des recommandations afin de les aligner avec les obligations du RGPD.

1.3.1 CARTES DE FIDELITÉ

L'offre de cartes de fidélité ne peut se faire qu'à condition qu'une base de traitement légitime soit disponible. Dans la plupart des cas, il s'agit du consentement obtenu de la personne concernée et, dans des cas exceptionnels, d'un accord si des conditions générales sont liées à l'obtention d'une carte de fidélité (art. 6.1a-b RGPD). Ce consentement doit être donné par le client de manière informée et les conditions stipulées àl'article 7 du RGPD doivent être remplies[4]).

Dans le contexte des obligations déontologiques pour les pharmaciens, des limites sont fixées qui seront respectées. [5]

Les données à caractère personnel qui sont demandées au client lors de la création d'une carte de fidélité doivent se limiter à l'information pertinente et minimale (article 5.1c RGPD). Sur base d'une carte de fidélité on ne peut pas dresser un profil du client, sauf consentement explicite, spécifique et informé du client, qui estindépendante du consentement pour la création de la carte de fidélité (article 22 RGPD).

Si une carte de fidélité est créée pour le client, le patient/la personne concernée doit être préalablement informé de manière complète sur les traitements et les modalités qui y seront associées. Cette information peut se faire au moyen d'un document pour la demande d'une carte de fidélité ou une Déclaration de

[4] Ces conditions sont les suivantes : (1) Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant. (2) Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.(3) La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement. (4) Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

[5] Art. 112-133 Code des doctrines de devoir pharmaceutiques DR du 10 novembre 1967

Confidentialité. Si la création d'une carte de fidélité est possible via le website, cette information doit également être mise à disposition d'une manière identique.

Veuillez remarquer que la demande d'une carte de fidélité ne contient pas de consentement automatique pour la réception de mails de marketing. Ces éléments doivent être considérés comme séparés.

1.3.2 E-MAILS

Une distinction doit être faite entre les e-mails de marketing et les e-mails d'information. Des e-mails d'information sont des e-mails qui sont envoyés par le pharmacien au client concernant des produits achetés, commandés et/ou livrés, les nouvelles heures d'ouverture de la pharmacie, cartes de fidélité venant à l'échéance et les preuves d'achat.

Dans le cas des e-mails de marketing, l'intention est d'informer le client sur les nouveaux produits de l'assortiment ou sur le marché, sur les ristournes des cosmétiques ou d'autres produits, sur les soirées d'information qui seront organisées (par exemple arrêter de fumer et workshops de make-up), sur des évènements (par exemple dix ans d'existence, nouvelle ouverture après restauration et autres). Il peut s'agir également d'e-mails de promotion.

1.3.2.1 LES E-MAILS D'INFORMATION

Les e-mails d'information informent le client sur les produits achetés, commandés et/ou livrés, les nouvelles heures d'ouverture de la pharmacie, des cartes de fidélité venant à l'échéance ou les preuves d'achat. Ces e-mails peuvent être motivés d'une part dans le cadre de l'exécution d'un accord et d'autre part par **l'intérêt légitime**.

Les mails d'information qui se rapportent aux produits achetés, commandés et/ou livrés, peuvent être considérés comme ressortant de la base de traitement légitime **"exécution d'un accord** « (article 6.1 du RGPD). Toutefois il est préférable de demander le média le plus approprié par lequel le patient/la personne concernée veut être contacté. Les patients/personnes concernées doivent toujours avoir la possibilité de décider de la manière par laquelle ils veulent être contactés.

Les e-mails d'information concernant les heures d'ouverture ou d'autres choses pratiques, peuvent être motivés par « **l'intérêt légitime** » (article 6.1- f) du RGPD). Lors d'un contrôle pour déterminer si l'e-mail est fondé sur un "intérêt légitime", les questions suivantes doivent être posées :

- Est-ce que le client attend que ses données soient traitées par le pharmacien ?
- Une influence négative sur le patient/la personne concernée peut-elle être exclue ?
- Est-ce que le traitement des données est dans l'intérêt du patient/la personne concernée ?
- Existe-t-il un rapport de puissance entre le patient/la personne concernée et le pharmacien ?
- Existe-t-il un trafic bidirectionnel entre le patient/la personne concernée et le pharmacien ?
- Est-ce qu'une information raisonnable est donnée sur le traitement et est-ce qu'on mentionne spécifiquement les finalités du traitement ?
- l'information a-t-elle été obtenue directement par le pharmacien auprès du patient/la personne concernée ou a-t-elle été collectée indirectement ?
- y a-t-il intrusion ou incorrection ?
- Est-ce que le traitement de données est nécessaire/proportionnel pour atteindre le but du traitement des données ?
- N'y a-t-il pas d'autre mesure possible pour atteindre le même but ?

Il faut toujours mesurer l'intérêt du pharmacien et la confidentialité du patient/de la personne concernée.

Dans le cadre du devoir d'information de l'article 12-14 du RGPD, le patient/la personne concernée doit être informé lors de la collecte des données à caractère personnel que ces données peuvent être utilisées dans le cadre d'e- mails d'information et/ou s'il y a question de transmission de données à caractère personnel à des tiers (par exemple mailproviders).

1.3.2.2 e-MAILS DE MARKETING/BULLETINS D'INFORMATION ETC.

Dans le cas des e-mails de marketing, l'intention est d'informer le client sur les produits qui sont nouveaux dans l'assortiment ou sur le marché, sur les ristournes sur les cosmeticques ou d'autres produits, sur les soirées d'information qui seront organisées et d'autres mails de promotion. Si le pharmacien veut envoyer de tels mails aux patients/personnes concernées, il doit préalablement demander son consentement avant de pouvoir les lui envoyer. Ce consentement doit se faire de manière éclairée. Ceci implique que le patient/la personne concernée soit au courant des traitements qui seront faits avec ses données à caractère personnel. Cette information sera incluse dans la Déclaration de Confidentialité.

La collecte des consentements, peut se faire de différentes façons, ou chaque fois qu'il faut se conformer à l'obligation d'information visée aux articles 12-14, à savoir :

- Ajouter une case à cocher « pour accord » sur le document à remplir lorsque le patient communique ses données à caractère personnel (avec référence/livraison de la Déclaration de Confidentialité) ;
- Ajout d'une case à cocher « pour accord » avec un formulaire online de contact /formulaire de commande (avec référence à la Déclaration de Confidentialité) ;
- Ajout d'une case à cocher « pour accord » avec le formulaire de demande online/de papier pour une carte de fidélité (avec référence/livraison de la Déclaration de Confidentialité) ;
- Lien de connexion sur le site web où le patient/la personne concernée peut s'inscrire pour les e-mails de marketing (avec référence à la Déclaration de Confidentialité) ;
- Un lien inclus dans un e-mail d'information où le patient/la personne concernée est renvoyée vers une page où il peut s'inscrire pour recevoir également des e-mails de marketing.

Le consentement doit répondre aux conditions prévues à l'article 7 du RGPD, c'est à dire qu'il doit s'agir d'un consentement libre, spécifique, éclairée et univoque ("opt-in") - acte positif clair de la personne concernée. Ce qui signifie que dans la pratique, il doit être question d'un règlement "opt-in". L'usage de cases cochées à l'avance, l'inscription automatique et le consentement tacite ne sont par exemple pas compatibles avec les conditions imposées par le RGPD.

Dans le contexte de l'obligation de responsabilité, selon l'article 5.2 et 7.1 (RGPD), le pharmacien doit veiller à ce que le consentement puisse être prouvé. Les possibilités mentionnées ci-dessus d''enregistrement du consentement permettent ainsi au pharmacien de fournir cette preuve.

En ce qui concerne les clients actuels, il faut vérifier s'ils ont donné ubn consentement valable répondant aux conditions imposées par l'article 7 du RGPD. Si c'est le cas, leur consentement pourra être conservé.Si ce n'est pas le cas, un nouveau consentement sera requis.

Finalement le système doit permettre que le patient/la personne concernée puisse à tout moment retirer son consentement (article 7.3 du RGPD). Dans la pratique on appelle cela le système du « opt-out », cette possibilité doit être mentionnée dans chaque mailing.

Dans le cas d'e-mails de marketing, en plus du droit de retrait, un droit absolu d'opposition doit être prévu, permettant au client de demander à tout moment que ses données à caractère personnel ne soient plus traitées àdes fins de marketing (article 21 du RGPD).

1.3.2.3 USAGE D'UNE PLATE-FORME DE COURRIER ÉLECTRONIQUE EXTERNE

Si le pharmacien fait usage d'une plate-forme de courrier électronique externe (par exemple mailchimp, hubspot, yourmailinglistprovider), le contrat avec ces entreprises doit être vérifié dans le contexte de l'obligation de rédiger un contrat de sous-traitance comme prévu à l'article 28 - 3) RGPD.

Certaines plate-formes de courrier électronique telles que mailchimp proposent pour cela leur propre contrat de traitement des données, nous invitons le pharmacien à vérifier les conditions proposées avant de marquer son accord..

Si les serveurs de la plate-forme de courrier électronique externe se trouvent en dehors de la Zone Economique Européenne, des mesures de sécurité supplémentaires pour protéger les données à caractère personnel doivent être prises, comme imposé aux articles 44 à 50 RGPD.

1.4 Recommandations concernant les images de camera

1.4.1 Formalites légales concernant la surveillance par caméra

L'AR du 8 mai 2018 relatif aux déclarations d'installation et d'utilisation de caméras de surveillance et au registre d'activités de traitement d'images de caméras de surveillance, impose de déclarer les caméras de surveillance auprès de la du SPF Intérieur via un guichet électronique centralisé ..

La déclaration auprès de la Commission de la protection de la vie privée est remplacée par un nouveau e-guichet du SPF Intérieur. Les déclarations existantes dans le registre actuel de la Commission de la protection de la vie privée ne sont pas automatiquement reprises dans le nouveau système. Cela veut dire que les pharmaciens, qui utilisent une surveillance par caméra, devront remplir à nouveau les formalités de déclaration.
Lorsqu'une déclaration avait été faite auprès de la Commission de la protection de la vie privée, un délai supplémentaire est accordé jusqu'au 25 mai 2020. La déclaration doit s'accompagner d'un registre qui indique chaque traitement des images de caméras qui ont eu lieu.

De plus, chaque pharmacien qui utilise les caméras de surveillance, doit afficher le pyctogramme légal. Cet affichage est obligatoire et sert à informer les gens de l'usage de caméra de surveillance.

Recommandation: Préalablement à l'installation de caméra de surveillance nous vous conseillons de faire une analyse d'impact relative à la protection des données afin de vérifier la finalité, la proportionnalité et de la nécessité.

1.4.2 Période de conservation (article 5.1- e) RGPD)

Dans le contexte de la protection des données, la période de conservation des images prises par la caméra doit être déterminée. Les images sont prises si des incidents se produisent. Le sentiment général est que de tels incidents se détectent dans un délai de 30 jours et par conséquent, les imagesseront visionnées dans ce délai.

En ce qui concerne les caméras de surveillance, une période de 30 jours peut être considérée comme un délai pertinent pour atteindre la finalité visée. La caméra de surveillance est réglée de telle manière que les images disparaissent automatiquement après un délai de 30 jours.

La période de conservation doit être liée à la finalité visée et non pas à la capacité du disque dur utilisé.

Le pharmacien peut – en fonction du système utilisé (le fournisseur de la caméra de surveillance) décider de régler la période de conservation ou effacer manuellement ou automatiquement les images après un délai de 30 jours. Si le pharmacien fait appel à un fournisseur externe, il faudra rédiger un contrat de sous-traitance.

1.4.3 Protection des images (article 32 RGPD)

Les images de caméra doivent être conservées de manière sécurisée dans un délai de 30 jours. La protection peut être installée par le fournisseur ou par le pharmacien même. Les images peuvent être protégées d'une part en limitant l'accès aux images et d'autre part en cryptant les disques durs. Les sauvegardes qui sont faites, doivent être sécurisées de la même manière que les disques durs.

1.5 Droits de la personne concernée (article 12-20 RGPD)

Dans le contexte du RGDP, chaque individu, dont les données sont traitées par un responsable de traitement et/ou un sous-traitant, possède des droits déterminés concernant ses données à caractère personnel. Il s'agit du droit d'être informé, du droit d'accès, du droit de rectification et d'effacement (droit à l'oubli), , le droit à la limitation du traitement, le droit à la portabilité, le droit d'opposition et le droit de ne pas être soumis à une décision automatique à laquelle des effets juridiques sont liés.

Le patient/la personne concernée soumet en principe sa demande au pharmacien, mais peut également envoyer sa demande au sous-traitant. Dans ce dernier cas, le contrat entre le pharmacien et le sous-traitant détermine les modalités du suivi de la demande.

Lors de toute demande, l responsable du traitement, à savoir le pharmacien,:

- Répondre à la demande, à moins que le pharmacien ne soit pas en mesure d'identifier correctement le patient/la personne concernée.

- Dans un délai d'un mois après réception d'une demande donner une réponse. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes, pour autant que le patient/la personne concernée en soit informé ainsi que des motifs du report ;

- Les demandes peuvent être répondues par voie électronique ou par tout autre moyen de communication si le patient/la personne concernée en fait la demande.

1.5.1 DROIT À L'INFORMATION (ARTICLE 12-14 RGPD)

Le pharmacien doit de manière pro-active informer le patient/la personne concernée dont les données à caractère personnel sont collectées sur le traitement de ses données à caractère personnel. Ce droit peut être exercé au moyen de la mise à disposition d'une Déclaration de Confidentialité, pour autant que le pharmacien ne viole pas son secret professionnel. Outre le secret professionnel des limites au droit d'information sont fixées dans le cas où la la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés Si le traitement est prescrit par la législation, le patient/la personne concernée est censé savoir ce qui se passe avec ses données.

1.5.2 DROIT DE REGARD DE LA PERSONNE CONCERNÉE (ARTICLE 15 RGPD)

Le patient/la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations sur ce traitement. En combinaison avec ce droit d'accès, le pharmacien fournit l'information nécessaire concernant ce traitement renvoit vers la Déclaration de Confidentialité.

La réponse à cette demande se fait endéans les 30 jours selon le RGPD, veuillez toutefois remarquer que la réglementation belge impose un délai plus court de 15 jour pour ce droit d'accès.

Lorsque la demande est soumise électroniquement, l'information est également transmise sous forme électronique. Une possibilité est de permettre l'accès en ligne aux données à caractère personnel. Si la demande est verbale, le pharmacien doit vérifier l'identité du patient/de la personne concernée. Après vérification de l'identité, le pharmacien doit fournir au patient/la personne concernée une copie de toutes les données personnelles. Ce droit est exercé gratuitement.

1.5.3 DROIT DE RECTIFICATION/CORRECTION (ARTICLE 16 RGPD)

Le patient/la personne concernée a le droit d'obtenir la rectification de ses données à caractère personnel si les données sont inexactes ou incomplètes. Ce changement doit être exécuté gratuitement et sans délai. La demande de rectification doit être transmise par le pharmacien à des tiers en charge du traitement de données à caractère personnel dans le contexte des soins pharmaceutiques

La (re)lecture de la carte eID peut apporter une vérification et correctionimmédiate..

1.5.4 DROIT D'EFFACEMENT DE DONNÉES/DROIT À L'OUBLI (ARTICLE 17 RGPD)

Le patient/la personne concernée a le droit droit d'obtenir du responsable du traitement, le pharmacien, l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le pharmacien a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais,. Toutefois le pharmacien ne doit pas dans tous les cas répondre à la demande du patient/la personne concernée, il existe des exceptions valables :

Le pharmacien ne doit pas répondre à la demande :

- Si le pharmacien respecte une obligation légale qui requiert le traitement et la conservation des données à caractère personnel;

- Si les données à caractères personnel sont toujours nécessaires dans le contexte du (suivi) des soins pharmaceutiques et si l'intérêt légitime du pharmacien prime sur l'intérêt du patient/la personne concernée ;
- Lorsque le traitement par le pharmacien est justifié par des motifs d'intérêt public dans le domaine de la santé publique

Le RGPD indique que les données à caractère personnel doivent quand-même être supprimées dans les cas suivants:

- Les données à caractère personnel ne sont plus pertinentes/nécessaires ;
- Le patient/la personne concernée a retiré son consentement et il n'y a pas d'autre base de traitement ;
- Les données à caractère personnel ne sont pas basées sur un intérêt légitime;
- Les données à caractère personnel ne peuvent plus être conservées sur base d'une obligation légale.
- L'autorité de protection de données examine actuellement la question de savoir comment répondre à une demande du droit à l'oubli. Le conseil qui sera fourni concernant cette demande servira comme base de jugement au droit à l'oubli.

1.5.5 DROIT À LA LIMITATION DU TRAITEMENT (ARTICLE 18 RGPD)

Si le patient/la personne concernée le souhaite, il/elle peut toujours demander au pharmacien un droit à la limitation du traitement. Ceci implique que le pharmacien n'est plus autorisé à traiter les données personelles du patient/de la personne concernée. Le pharmacien doit exercer cette demande dans un délai raisonnable et obligatoirement si :

- L'exactitude des données à caractère personnel est contestée par lepatient/la personne concernée, pendant une durée permettant au pharmacien de vérifier l'exactitude des données à caractère personne. Les données à caractère personnel qui ont été désignées comme correctes par le patient/la personne concernée peuvent,entre-temps, être traitées ;
- Le traitement est illicite, mais le patient/la personne concernée s'oppose à ce que ses données soient effacées ;
- Les données à caractère personnel ne sont plus nécessaires pour les finalités, mais celles-ci sont encore nécessaires la constatation, l'exercice ou la défense de droits en justice;
- Le patient/la personne concernée s'est opposé au traitement ultérieur de ces données personnelles par le pharmacien.

Pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le pharmacien prévalent sur ceux du patient/de la personne concernéele pharmacien peut toujours décider de continuer le traitement des données à caractère personnel.

Si l'intérêt légitime du pharmacien ne prévaut pas à l'intérêt du patient/la personne concernée, le traitement des données à caractère personnel peut malgré tout être continué si l'une des conditions suivantes est remplie :

- Le patient/la personne concernée a donné son consentement ;
- Les données à caractère personnel sont nécessaires pour une action en justice ;
- Le traitement est nécessaire pour la protection des droits d'une autre personne ;
- S'il y a un intérêt public pour le traitement.

Lors d'une limitation du traitement, le pharmacien informe tous les tiers concernés qui reçoivent les données à caractère personnel (comme les offices de tarification, association professionnelle, APB, Farmaflux, comptable, secrétariat social, entreprises de leasing), de. Sont donc concernés, les tiers qui reçoivent les données à caractère personnel du pharmacien.

1.5.6 DROIT À LA PORTABILITÉ DES DONNÉES(ARTICLE 20 RGPD)

Le patient/ la personne concernée a le droit de demander au pharmacien de transférer les données personelles reçues à un autre pharmacien. Cela doit être fait dans un format structuré, couramment utilisé et lisible par l'appareil.

Le pharmacien doit respecter le droit à la portabilité :

- Si le traitement est fondé sur le consentement[6] :
    - La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.
    - La personne concernée a donné son consentement explicite au traitement de catégories particulières de données à caractère personnel pour une ou plusieurs finalités spécifiques.
- soit le traitement est fondé sur un contrat entre le patient/la personne concernée[7]:
    - lorsque le traitement est nécessaire à l'exécution d'un contrat auquel le patient/la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande du patient/la personne concernée.
- soit sur base de de traitement nécessaire (mission d'intérêt public)
- Le traitement est effectué à l'aide de procédés automatisés.

Toutes les données personnelles collectées doivent être transférées à la pharmacie concernée. Pour respecter ce droit, il est important que le pharmacien sauvegarde les données personnelles d'une manière qui permette de respecter cette possibilité de la portabilité. Cette portabilité est liée à l'obligation de protéger les données par la conception[8]. Protection des données dès la conception implique que, au début de la collection des données personnelles des mesures techniques et organisationnelles sont appliquées pour garantir que les données sont traitées avec prudence. Il peut s'agir pseudonymisation, chiffrement, définition les périodes de conservation, la minimisation des données.

1.5.7 Droit d'opposition (article 21 RGPD)

Chaque patient/personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur, le consentement et intérêt justifié légitime.

Le pharmacien arrête le traitement, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés du patient/de la personne concernée.

Dans ce cas, le pharmacien ne doit pas supprimer automatiquement les données.

1.6 Services auxiliaires

1.6.1 Ressources Humaines

Lors du traitement de données à caractère personnel dans le contexte de ressources humaines, le pharmacien doit prendre en compte les éléments suivants :

- Outre la technologie utilisée, la protection des données à caractère personnel doit être observée ;
- Les communications électroniques jouissent de la même protection que les autres communications ;
- Le consentement est une base légale difficile à gérer dans une relation employeur-employé, à moins que l'employé puisse refuser sans subir une conséquence négative ;
- L'intérêt légitime peut être invoqué, si les principes de proportionnalité et subsidiarité sont respectés, c'est-à dire-que les mesures soient proportionnelles aux finalités et qu'il n'y a pas d'autre possibilité moins intrusives concernant la confidentialité de l'employé ;
- Les employés doivent être informés concernant la supervision de leurs activités, tel que le contrôle de lutilisation d'internet ;
- Un transfert international de données n'est possible que si un même niveau de sécurité des données à caractère personnel est prévu.

Aucune distinction n'est faite ici entre le personnel qui est employé sous un contrat de travail et d'autres travailleurs (par exemple les pharmaciens indépendants, travaillant dans la pharmacie d'un autre pharmacien).

[6] Article 6, 1, a), jt. Article 9, 2, a) Règlement général sur la protection des données.
[7] Article 6, 1, b) Règlement général sur la protection des données.
[8] Article 25 Règlement général sur la protection des données.

1.6.1.1 BASES LÉGALES DE TRAITEMENT (ART. 6 RGPD)

Dans le contexte de ressources humaines, il existe plusieurs bases de traitement. Il peut s'agir soit d'obligations légales, soit d'obligations contractuelles, soit d'intérêts légitimes de l'employeur ou encore du consentement. Toutefois cette dernière base, le consentement, est très difficile à gérer dans le contexte de ressources humaines.

Pour être valable, le consentement doit se donner volontairement. Dans le contexte d'une relation employeur-employé, c'est-à-dire une relation patron-travailleur, il existe un certain déséquilibre, on parle d'une certaine "pression" sur ce consentement, où le consentement volontaire peut être remis en question. Cependant un tel consentement peut être accepté si un employé/travailleur peut décider de ne pas donner ce consentement sans donné lieu à des conséquences négatives en son chef. De même,la possibilité de retirer le consentement doit être prévue. Exemple : publier des photos du personnel sur le site internet. Pour cela l'accord doit être demandé à l'employé/travailleur et cette possibilité de refuser ne doit pas avoir de conséquences négatives.

Dans le cas où l'intérêt légitime est utilisé, comme base de traitement légal, une évaluation de la proportionnalité doit être réalisée ainsi qu'une évaluation de la nécessité et qu'aucune mesure moins intrusive ne puisse atteindre le même but. Cette évaluation implique de vérifier que la mesure prise est la mesure la moins intrusive possible, pour atteindre la finalité désirée, en d'autres termes, malgré le fait que les intérêts de employeur/patron puissent prévaloir, il faut veiller à ce que l'intérêt de l'employé-travailleur lors du traitement de ses données à caractère personnel ne soit pas remis en question inutilement ou abusivement.

1.6.1.2 RECRUTEMENT.

Lors de la phase de recrutement, les données à caractère personnel de candidats et de possibles candidats sont collectées. Plusieurs medias sont utilisés pour cela. Toutefois les différents medias exigent une enquête sur la base de traitement légale et les modalités de traitement.

Nous vous avons présentés les points les plus importants sur ce sujet. Cependant, si vous avez encore des questions,nous vous invitons à consulter le site internet de l'Autorité de la protection des données répond à beaucoup de questions.

1.6.1.2.1 Candidature spontanée/candidature sur base d'un post vacant

Lors d'une candidature spontanée ou une candidature sur base d'un poste vacant l'employeur/patron obtient des données à caractère personnel (principalement) au moyen d'un CV. L'envoi du CV est considéré comme un consentement pour le traitement de cette candidature, mais il est important que le candidat soit mis au courant du traitement de ses données. Nous vous invitons à utiliser la Déclaration de Confidentialité pour les candidats, dans laquelle les modalités de traitement d'une candidature sont précisées.

La Déclaration de Confidentialité des candidats peut être jointe à l'offre d'emploi et/ou à la page de contact relative au poste vacant (ou candidature spontanée) ou bien via un « just-in-time-notice » qui fait référence à la Déclaration de Confidentialité pour les candidats.

La Déclaration de Confidentialité peut également être présente sur le site web, si les candidatures peuvent directement être postées sur le site internet. Dans ce cas on peut référer via un lien "just-in-time-notice" à la Déclaration de Confidentialité du site internet. L'employeur informera dans la Déclaration de confidentialité sur la procédure/la gestion du traitement des candidatures.

1.6.1.2.2 Utilisation des médias sociaux durant le processus de recrutement[9]

Les médias sociaux sont de nos jours largement utilisés et les profils sur les médias sociaux sont souvent publics. Nombreux employeurs supposent qu'il s'agit d'information publique, vu que l'individu même l'a publié. Il faut faire une distinction entre les médias sociaux liés au travail et les médias sociaux orientés vers la vie privée. Seules les médias sociaux liés au travail peuvent en principe être pris en considération lors d'une procédure de recrutement, comme par exemple Linkedin.

[9] Opinion 2/2017 on data processing at work, Working Party article 29, http://ec.europa.eu/newsroom/document.cfm?doc_id=45631, Section 5.1

La collecte et le traitement de données à caractère personnel récoltées dans les média sociaux n'est permis que s'il y a un intérêt légitime et si ceette collecte et traitement sont nécessaires et pertinents pour l'exercice du poste vacant pour lequel une candidature est soumise. (art. 6.1f RGPD)

En aucun cas on ne peut attendre du candidat qu'il ajoute l'employeur comme "ami" sur un des médias sociaux utilisé, afin que celui-ci puisse avoir accès à l'information du profil sur le médium social utilisé.

1.6.1.3 EMPLOYÉS/TRAVAILLEURS

1.6.1.3.1.1 Supervision du comportement des employés/travailleurs[10]

Dans certains cas il peut être opportun de contrôler les activités des employés. Il peut s'agir de mesures qui permettent un contrôle de l'utilisation de l'ordinateur, voir même des mesures permettant un contrôle de l'utilisation de la voiture.

De telles activités de contrôle n'ont principalement pas de base légale, mais peuvent être installées à condition de respecter quelques exigences légales (voir les caméras de surveillance). De plus le *European Data Protection Board* (avant : Groupe de travail Article 29), conseille limiter le contrôle afin de permettre de garantir la confidentialité des employés/travailleurs. Il peut s'agir de limitations géographiques, de limitations liées au temps, de limitations liées aux données ou d'autres limitations qui visent à protéger la vie privée.

De plus il faut prendre en compte que, dans l'état actuel de la technologie, il y a beaucoup de ressources de contrôle disponibles. Ressources de contrôle qui ne sont pas toujours visibles pour l'employeur/travailleur. Ici on ne peut pas perdre de vue la transparence en ce qui concerne l'employé/travailleur comme personne concernée (article 5.1 – a) du RGPD - (licéité, loyauté, transparence).

1.6.1.3.2 Supervision de l'utilisation des ordinateurs/internet[11]

La surveillance de l'utilisation des ordinateurs et certains programmes peut pour des raisons de sécurité faire partie d'un intérêt légitime. Toutefois, dans chaque cas il faut une évaluation en ce qui concerne la proportionnalité, la nécessité et la subsidiarité. Ces conditions impliquent que la mesure doit être appropriée (proportionnelle) en ce qui concerne le but à atteindre, ainsi que nécessaire et qu'aucune mesure moins intrusive ne puisse atteindre le même but.

Si ces conditions sont remplies, l'employé-travailleur doit être mis au courant des mesures prises, ainsi que des modalités/paramètres de configuration qui sont pertinents pour garantir la transparence nécessaire (article 5.1 du RGPD).

Veuillez remarquer que dans beaucoup de cas il est préférable de favoriser la prévention que la détection. Par exemple dans le cas de surveillance du comportement de ,l'utilisation d'Internet, la préférence est de bloquer certains sites internet, plutôt que de surveiller le comportement.

Les conditions s'appliquent également aux mesures qui sont prises dans le contexte du travail à domicile. Dans le cadre du travail à domicile, des mesures peuvent être prises pour exercer une surveillance, mais les mesures ne peuvent être disproportionnées (comme par exemple c'est bien le cas avec l'usage du webcam à distance ou d'enregistrement de frappes)[12].

Pour plus d'information, voir également le FAQ de l'Autorité de protection des données concernant le contrôle de l'utilisation de l'ordinateur/internet au travail.

[10] Opinion 2/2017 on data processing at work, Working Party article 29, 29), http://ec.europa.eu/newsroom/document.cfm?doc_id=45631, Section 3.1
[11] Opinion 2/2017 on data processing at work, Working Party article 29, http://ec.europa.eu/newsroom/document.cfm?doc_id=45631, Section 5.3
[12] Opinion 2/2017 on data processing at work, Working Party article 29, http://ec.europa.eu/newsroom/document.cfm?doc_id=45631, Section 5.4.1

1.6.1.3.3 Surveillance des communications, trafic de la messagerie de l'employé/travailleur[13]

Le contrôle du trafic de la messagerie de l'employé/travailleur est souvent considéré comme nécessaire. Toutefois, ceci a un grand impact sur la vie privée de la personne concernée, étant donné que des messages privés peuvent également arriver dans la mailbox du travail.

Le principe de base stipule que l'employeur/patron ne peut pas avoir accès à la mailbox de l'employé/travailleur. Toutefois, en cas de départ inattendu ou absence prolongée, ceci peut conduire à des problèmes de continuité. Dans ce cas, il est possible qu'il y ait un intérêt légitime pour avoir quand même accès à la mailbox.

Cet accès est toutefois soumis à certaines conditions, à savoir[14]:

- Minimalisation de l'accès aux données à caractère personnel : ce qui implique que la consultation des données doit être limitée. Seul un accès à ce qui est nécessaire pour garantir la continuité est accepté.
- Droit d'information : les employés/travailleurs doivent être informés de cette possibilité en cas de départ inattendu ou de maladie prolongée et/ou d'autres situations.
- La période de conservation : en cas de départ, des règles doivent être respectées comme la durée de conservation des données. Cela signifie qu'il faut déterminer à l'avance quel terme sera utilisé pour garder la mailbox ouverte.

Si ces conditions sont remplies, on peut avoir un accès limité à la mailbox. En pratique, il est préférable d'installer une notification d'absence disant que l'employé/travailleur qui part,est absent ou ne travaille plus dans l'entreprise et en indiquant une adresse de courrier électronique ou numéro de téléphone ou la personne de contact peut se diriger pour un suivi ultérieur. Cette mesure est la moins intrusive, étant donné qu'il n'y a pas d'accès à la mailbox.

En pratique ce n'est pas toujours possible, c'est pourquoi dans certaines conditions l'accès au mailbox peut être autorisé. Veuillez remarquer que la transmission automatique est plus intrusive étant donné qu'il n'y a pas de sélection des données transmises.

Préventivement les employeurs/patrons peuvent recommander à leurs employés/travailleurs d'indiquer clairement leurs messages privés comme étant privés. Une telle indication signale qu'il s'agit de messages qui ne peuvent être ouverts, ce qui rend plus facile pour l'employeur/patron de faire la distinction entre privé et travail.

1.6.1.3.4 Bring Your Own Device (BYOD)[15]

L'utilisation croissante de ses propres appareils dans l'environnement du travail, apporte certains risques en ce qui concerne la protection des données de l'employeur, ainsi que la confidentialité des employés. Pour répondre à ces risques, il est recommandé d'utiliser les outils *"mobile device management(MDM)"* pour faire une distinction claire entre les données à caractère personnel et les données liées au travail. Ces outils rendent possible de supprimer le contenu de l'appareil à distance, s'ils se présentent des problèmes, comme perte ou vol.

Il y a beaucoup d'outils MDM en circulation, ou il faut toujours vérifier quelles fonctionnalités sont possibles et quelles fonctionnalités atteignent les finalités exactes. Il est donc recommandé d'effectuer une évaluation de protection de données, pour savoir quelles fonctionnalités sont nécessaires pour atteindre les finalités et quelles mesures permettent de répondre aux exigences fixées de proportionnalité et subsidiarité.

Les outils les plus connus sur le marché en ce moment sont Mobileron, Intune et 0365. Ces outils MDM ont leurs propres fonctionnalités, et il est nécessaire de toujours évaluer s'ils répondent aux exigences de proportionnalité, de nécessité et de subsidiarité.

---

[13] Recommandations cybersurveillance, Commission de la protection de la privée, https://www.privacycommission.be/sites/privacycommission/files/documents/2011-07-02-recommandations-cybersurveillance.pdf

[14] Access to eCommunications data when an employee is absent, European Data Protection Supervisor (EDPS), https://edps.europa.eu/data-protection/data-protection/reference-library/access-ecommunications-data-when-employee-absent_en

[15] Opinion 2/2017 on data processing at work, Working Party article 29, http://ec.europa.eu/newsroom/document.cfm?doc_id=45631, Section 5.4.2-5.4.3; Themes de vie privée "BYOD", Commission de la protection de la vie privée, https://www.privacycommission.be/fr/byod-fr.

Dans le contexte de BYOD, il est nécessaire que les employés aient le choix s'ils installent ou non un tel outil sur leur téléphone. Le choix peut être lié au choix si l'employé/travailleur veut recevoir/ou non sur son téléphone des données liées au travail. En tout cas, il ne peut y avoir des conséquences négatives associées au fait qu'un employé préfère ne pas recevoir d'information liée à l'entreprise sur son téléphone privée

Si l'employeur/patron opte pour attribuer des appareils liés au travail, l'emploi de MDM peut être rendu obligatoire. Toutefois, si l'utilisation privée est permise sur les appareils du travail, le MDM doit faire une distinction entre les données privées et les données liées au travail.

En tout cas s'il s'agit d'appareils du travail ou de BYOD, l'employé doit clairement être informé sur le traitement de ses données à caractère personnel. Cela est possible moyennant une Déclaration Confidentialité, mais aussi au moyen d'outils MDM qui fournissent des 'informations concernant l'opération.

1.6.1.3.5 Utilisation d'appareils « track 'n trace » dans la voiture.[16]

Les appareils *"Track 'n trace* sont utilisés pour vérifier où les voitures se trouvent et à quel moment. De tels appareils sont utilisés régulièrement comme outils, dans les voitures de société, mises à disposition par l'employeur/patron.

Les données qui sont collectées au moyen des appareils "track 'n trace" sont considérées comme des données personnelles. Pour pouvoir les traiter, il faut donc une base de traitement légale. Cette base de traitement légale dans certains cas est une obligation légale, mais repose souvent sur l'intérêt légitime. Ici à nouveau il convient de faire un test de proportionnalité, nécessité et subsidiarité. Des mesures permettant de limiter" l'intrusion" sont entre autres la possibilité de désactiver le système, de le limiter dans le temps ou dans l'espace.

En tout cas l'employé/travailleur doit être mis au courant de l'utilisation des appareils "track 'n trace", ainsi que des modalités/limitations installées afin de protéger sa vie privée.

1.6.1.3.5.1 Utilisation de média sociaux pour screening des employés/travailleurs[17]

L'utilisation de média sociaux pour le "screening" des (ex) employés/travailleurs, est permis seulement si un intérêt légitime peut être démontré pour cela et que l'on peut démontrer qu'il n'y a pas de mesures moins intrusives.

Par exemple un contrôle sur une clause de non-concurrence, en contrôlant Linkedin, peut être légitime en certains cas, à moins qu'il y ait d'autres mesures moins intrusives qui atteignent la même finalité.

Si un employé/travailleur doit utiliser les médias sociaux dans son cadre professionnel, il se peut que l'employeur veuille le contrôler. Ceci peut s'inscrire dans l'intérêt légitime, mais doit être jugé cas par cas et vérifier si l'ingérence dans la vie privée n'est pas disproportionnelle et si l'employé/travailleur a été informé clairement sur les contrôles[18].

1.6.2 FORMALITÉS FINANCIERES

1.6.2.1 PRINCIPES DE TRAITEMENT

Dans le contexte des formalités financières que doit remplir le pharmacien, il faut tenir compte du fait que les données personnelles sont traitées dans ce cadre.

Initialement il faut vérifier si la mention de données personnelles sur les factures peut être évitée. Dans certains cas on peut éviter d'indiquer une personne de contact sur la facture en adressant la facture seulement à une division de l'entreprise. Dans ce cas il est préférable de limiter à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) de l'article 5.1- c) (RGPD).

[16] Opinion 2/2017 on data processing at work, Working Party article 29, http://ec.europa.eu/newsroom/document.cfm?doc_id=45631, Section 5.7; Avis 12/2005 du 7 septembre 2005: Geolocalisation dans les voitures, https://www.privacycommission.be/sites/privacycommission/files/documents/avis_12_2005_0.pdf

[17] Opinion 2/2017 on data processing at work, Working Party article 29, http://ec.europa.eu/newsroom/document.cfm?doc_id=45631, Section 5.2

[18] Thèmes de vie privée "Réseaux sociaux sur le lieu de travail", Commission de la protection de la vie privée, https://www.privacycommission.be/fr/reseaux-sociaux-sur-le-lieu-de-travail

Dans les cas où ce n'est pas possible, les factures doivent être considérées comme des données personnelles et doivent être traitées avec la précaution nécessaire. Les documents papier doivent être conservés dans une armoire/coffre-fort/espace de manière qu'ils soient seulement accessibles pour les personnes qui ont besoin de l'accès. Les documents électroniques doivent se conserver sur un serveur sécurisé ou un outil sécurisé, où les droits d'accès sont ajustés. Si des documents financiers sont conservés, ils peuvent être archivés et ensuite être détruits. Les documents non pertinents doivent être détruits immédiatement.

Si l'on utilise des outils comptables, ils doivent être sécurisés au maximum. De préférence les droits d'accès sont définis et une politique de mot de passe est installée où une modification du mot de passe est exigée sur une base régulière. Si l'on utilise des outils externes et/ou bureaux de comptabilité les exigences du contrat de l'article 28(3) doivent être remplies.

1.6.2.2 PÉRIODE DE CONSERVATION (ARTICLE 5.1C DU RGPD)

Les documents comptables doivent se conserver durant une période déterminée sur base de différentes législations. Les périodes minimales de conservation que le législateur belge impose pour des documents comptables sont :

- Documents comptables: 7 années pour les documents qui peuvent servir de preuve à des tiers, à partir du 1 janvier de l'exercice suivant ;
- Registre du personnel: 5 années à partir du jour qui suit la fin du contrat de travail ;
- Contrat de travail: 5 années à partir du jour qui suit la fin du contrat de travail;
- Données personnelles: pas plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles furent obtenues ou seront traitées ultérieurement.
- Documents bancaires/ honoraires : 5 années.

Cette liste donne une indication de la durée de conservation applicable, mais est non limitative. Les durées de conservation peuvent dévier des durées de conservation légalement imposées, mais doivent être fixées et respectées. S'il y a des documents qui doivent se conserver plus longtemps parce qu'ils sont encore pertinents, ceci est possible à condition qu'il y ait une autre base de traitement légal, , une convention, un consentement ou un intérêt légitime (article 6 du RGPD).

2 DEFINITIONS UTILISEES

1. **RGPD**= Règlement Général de la Protection de Données, soit la version françaisedu règlement Européen "General Data Protection Regulation (GDPR) concernant la protection de personnes physiques en ce qui concerne le traitement de données à caractère personnel et la libre circulation de ces données dans l'Union Européenne.
2. **CNIL**: Commission Nationale de l'Informatique et des Libertés (CNIL), c'est-à-dire l'autorité Française de protection de données.
3. **Données à caractère personnel :** toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale(article 4 (1) RGPD).
4. **Destinataire**: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement; (article 4 (8) RGPD.
5. **Le patient/personne concernée** : nom générique pour toutes les personnes concernées dans le traitement par le pharmacien de données à caractère personnel. Il ne s'agit ici pas seulement du patient, mais aussi du représentant autorisé, les employés, travailleurs, personnes de contact et autres.
6. **Traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (article 4(2) RGPD).
7. **Responsable de traitement**: la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre; (article 4(7) RGPD)
8. **Le sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement; (article 4(8) AVG = RGPD) ;
9. **WP29**: "*working party article 29*", est un groupe de travail consultatif composé de représentants des autorités de protection de données. L'organe actuel sera, sous le RGPD) reformé à un "Comité de Protection de Données " dans le sens de l'article 64-65 (RGPD).