SEQUENCE 6

APPLICATIONS RGPD

🕮 Mise en situation n°1.

Monsieur Forget réside à Lyon et il a commandé, il y a plus de 10 ans maintenant, des produits sur le site marchand d'une société implantée en Californie. A chaque début de mois, Monsieur Forget reçoit sur sa messagerie électronique des offres commerciales de cette société. Ne souhaitant plus être importuné, Monsieur Forget se demande s'il peut demander la suppression de son compte à ladite société.

Question 1. Vérifier si le Monsieur Forget a le droit d'effectuer cette demande.

Question 2. Indiquer le recours dont il dispose en cas de refus de la société.

🕮 Mise en situation n°2.

Une association vient de créer une bibliothèque dans une petite commune normande. Elle possède un fonds de 400 ouvrages pour l'essentiel achetés d'occasion ou donnés, et s'est équipée d'outils informatiques pour la gestion des ouvrages et des lecteurs.
Le président de l'association vous demande votre aide quant à la mise en place de cette activité de prêt afin d'être en conformité avec le RGPD.

La secrétaire de l'association a commencé à élaborer un tableau relatif au prêt de livres par la bibliothèque afin de recenser les données qui seront collectées dans les bases de données.

Quelles données traitons-nous?	*Pourquoi traitons-nous ces données ?*	*Jusqu'à quand conservons-nous ces données ?*
Identité du lecteur : nom et prénom Ses cordonnées : adresse postale, num. tél., email Sa situation familiale : marié, veuf, célibataire Son activité : étudiant, salarié, retraité … Son niveau d'étude Son adhésion ou non à un parti politique	Pour identifier le lecteur et conclure le contrat de prêt Pour faire respecter le contrat de prêt Pour l'informer des actions menées par l'association	Aucune limite de temps
Liste des livres empruntés avec le titre du livre, le nom de l'auteur, le nom de l'éditeur et la date de parution	Pour établir le contrat de prêt Pour proposer de nouveaux livres	Pendant 3 ans après le retour du dernier livre emprunté
Date du prêt, état du livre, nombre de jour de retard, pénalités	Pour récupérer les livres Pour appliquer les sanctions/pénalités	Pendant 10 ans

Question 1. Montrer que l'association est bien concernée par le RGPD.

Question 2. Indiquer si toutes les données qui vont être saisies constituent des données à caractère personnel.

Question 3. Préciser qui sera considéré comme le « responsable de traitement des données ».

Question 4. Indiquer le nom donné à ce tableau, et préciser son (ses) destinataire(s).

Question 5. Analyser les informations figurant dans ce tableau : données traitées / finalités / durée de conservation et donner quelques recommandations à l'association pour être davantage en conformité avec le RGPD.

- *Concernant les données* :
- *Concernant les finalités* :
- *Concernant les durées de conservation :*

Préconisations :

Enfin, le président de l'association s'interroge sur la nécessité de désigner un D.P.O..

Question 6. Rappeler le rôle du D.P.O. et vérifier si sa désignation est obligatoire dans le cas de cette organisation.

🕮 Mise en situation n°3 avec documentation

La pharmacie LAFAYETTE, située dans le centre-ville de Tours, héberge ses données auprès de la société PROG INFO, dont le siège social se situe à Poitiers. Cette société informatique est spécialisée depuis 2 ans dans l'hébergement de données de santé. Elle dispose de datacenters dont certains sont implantés hors UE. Sa clientèle est constituée notamment de médecins, pharmaciens, kinésithérapeutes, laboratoires d'analyses.
Pour exercer cette activité, elle détient la certification HDS (Hébergeur de Données de Santé).

Question 1. Faire quelques recherches pour présenter la norme ISO 27001, dont le respect est nécessaire pour l'obtention de la certification HDS.

Madame LAMARIN, habitant au centre-ville de Tours, est cliente de cette pharmacie. Ayant appris que la pharmacie a délégué l'hébergement des données à un tiers, craint pour ses données. Elle craint plus précisément une violation de ses données.

Question 2. Repérer la particularité des données relatives à Mme LAMARIN traitées par la pharmacie, et en déduire les conséquences juridiques pour la pharmacie en termes de traitement de ces données.

Question 3. Qualifier juridiquement, au regard du RGPD, la pharmacie LAFAYETTE et la société PROG INFO.

- *Pharmacie LAFAYETTE qualifiée de ???*
  - Justification :
- *Société PROG INFO qualifiée de ???*
  - Justification :

Question 4. Préciser ce qu'est une « violation de données » au sens du RGPD.

Question 5. Présenter les obligations qui pèsent sur la pharmacie et sur la société PROG INFO *(distinguer les deux acteurs)* **en cas de violation des données personnelles de Mme Lamarin.**

- *Obligations de la pharmacie LAFAYETTE* :
- *Obligations de la société PROG INFO* :

Question 6. Distinguer les sanctions encourues en cas de non-respect de ces obligations.

Par crainte pour ses données, Madame LAMARIN décide finalement de changer de pharmacie.

Question 7. Vérifier si Madame LAMARIN peut demander le transfert de ses données personnelles vers la nouvelle pharmacie.

Document 1. La certification HDS et la norme ISO 27001

Les données personnelles de santé sont des données sensibles. Leur accès est juridiquement encadré pour protéger les droits des personnes. L'hébergement de ces données doit en conséquence être réalisé dans des conditions de sécurité adaptées à leur criticité. La réglementation définit les modalités et les conditions attendues.

Depuis le 1er avril 2018, la certification Hébergeur de Données de Santé (HDS) est obligatoire pour toute organisation publique ou privée qui héberge des données de santé de citoyens français. Elle vient remplacer la demande d'obtention d'agrément effectuée auprès du ministère français de la santé. Un certificat, valable 3 ans et renouvelable indéfiniment, est ainsi délivré à l'organisation qui en fait la demande, dès lors qu'au travers des audits effectués sur site, il est attesté le bon respect de normes notamment la norme ISO 27001.

Document 2. Guide du sous-traitant publié par la CNIL

https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

🕮 Mise en situation n°4 avec documentation

Sébastien est un internaute français qui utilise régulièrement les services de différents moteurs de recherche dans le cadre professionnel et personnel (Google, Qwant, Bing).
Un jour, il s'est aperçu que, lorsqu'il saisissait ses nom et prénom sur le moteur de recherche de GOOGLE, des propos injurieux et diffamatoires étaient publiés à son égard sur un blog : *«Sébastien est une personne qui n'est pas digne de confiance. C'est un tricheur, un voleur* ».
Etant actuellement en phase de recherche d'emploi, il s'interroge sur les moyens dont il dispose pour obtenir la suppression de cette publication en ligne.

Il décide d'effectuer une démarche auprès de la société Google.

Question 1. Qualifier la démarche effectuée auprès de la société Google.

Question 2. Vérifier si cette démarche est recevable.

Question 3. Préciser les recours dont dispose Sébastien et les sanctions encourues par la société Google si elle refuse d'accéder à sa demande.

Question 4. Montrer les limites de cette démarche.

DOCUMENT 1 – Une palette de droits pour mieux exercer le droit à l'oubli.

Pour exercer plus facilement son droit à l'oubli sur internet, un internaute dispose de plusieurs moyens : utiliser son droit à l'effacement, son droit d'opposition à la publication de ses données à caractère personnel sur un site ou bien encore son droit au déréférencement.
Le déréférencement permet de faire supprimer un ou plusieurs résultats fournis par un moteur de recherche à l'issue d'une requête effectuée à partir de l'identité (nom et prénom) d'une personne. Pour cela, l'internaute concerné doit adresser au moteur de recherche, par le biais de son formulaire en ligne, une demande motivée de déréférencement d'un contenu le concernant s'affichant dans la liste de résultats du moteur de recherche.
Toutefois, cette suppression ne conduit pas à effacer l'information sur le site internet source : le contenu original reste inchangé et est toujours accessible, en utilisant d'autres critères de recherche ou en allant directement sur le site à l'origine de la diffusion. Pour supprimer l'information sur le site source, il faut privilégier une demande d'effacement auprès du responsable du site.

La CNIL a dressé 13 critères devant servir à déterminer si un contenu doit ou non être déréférencé :

1- *Les résultats de recherche sont-ils relatifs à une personne physique ?*
Seules les personnes physiques peuvent exercer ce droit.
2- *S'agit-il d'une personne publique ? Le plaignant joue-t-il un rôle dans la vie publique ?*
Plus la personne a une activité publique, plus la liberté d'information prime.
3- *Les données sont-elles exactes et mises à jour ?*
Les infos inexactes ou trompeuses doivent être déréférencées.
4- *Les données sont-elles pertinentes et/ou excessives?*
Si elles touchent à la vie privée, si elles sont diffamatoires, injurieuses, calomnieuses, etc., si elles reflètent une opinion personnelle plutôt qu'un fait vérifié, alors le déréférencement peut apparaître justifié.
5- *L'information est-elle sensible* ?
Cela concerne les données d'origine raciale, ethnique, opinions politiques, convictions religieuses ou philosophiques, l'appartenance syndicale, les informations liées à la santé ou à la vie sexuelle. Par principe, la diffusion de ce type de données aura un impact plus important sur la vie privée des personnes que celle d'autres informations plus ordinaires. Par conséquent, leur déréférencement peut être justifié.
6- *Le traitement de l'information cause-t-il un préjudice au plaignant ?*
Les données ont-elles un impact négatif disproportionné sur sa vie privée ?
Il n'y a pas d'obligation pour les personnes de démontrer qu'elles subissent un préjudice et cela ne peut pas être une condition du déréférencement. Toutefois, l'existence d'un préjudice pour la personne constitue un facteur important en faveur du déréférencement.
[…]

Source : www.cnil.fr

DOCUMENT 2 – La Cnil belge inflige une amende record de 600 000 euros à Google.

L'autorité protectrice des données (APD) en Belgique - l'équivalent de la CNIL en France - a imposé le 14 juillet 2020 une amende de 600 000 euros à Google Belgium pour non-respect du droit à l'oubli. Il s'agit de la plus lourde sanction imposée par l'APD à ce jour.
"*Cette décision est historique pour la protection des données personnelles en Belgique, non seulement de par le montant de la sanction, mais aussi parce qu'elle assure que la protection complète et efficace du citoyen soit maintenue dans des dossiers liés à des grands groupes internationaux comme Google, dont la structure est très complexe* ».

Le plaignant demandait à l'entreprise américaine de supprimer certains résultats de recherche liés à son nom dans le moteur de recherche. Une partie des pages litigieuses concernait un éventuel étiquetage politique et une seconde était relative à une plainte pour harcèlement à son encontre, déclarée non fondée il y a de nombreuses années. La situation était particulièrement délicate car le plaignant fait partie de la vie publique belge. Mais, malgré les circonstances, Google a refusé de déréférencer ces pages visées.
L'autorité a donné raison à Google sur les pages concernant l'étiquetage politique. "*Le maintien de leur référencement était nécessaire à l'intérêt public,* mais sur le volet harcèlement, elle estime que la firme technologique aurait dû donner suite à la demande de suppression "*Vu que les faits n'ont pas été établis, sont anciens, et susceptibles d'avoir de sérieuses répercussions pour le plaignant, les droits et intérêts de la personne concernée doivent prévaloir*.
En plus de l'amende record, l'APD ordonne à Google de cesser les référencements des pages concernées dans l'Espace Economique Européen. […]

Source : www.usine-digitale.fr - juillet 2020