Cybersécurité et Développement

Le RGPD

I-Introduction:RGPD ?

Le **R**ègle**G**énéral sur la **P**rotection des **D**onnées (RGPD), officiellement appelé règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

Les principaux objectifs du RGPD sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement. Ces principes pourront être appliqués grâce à l'augmentation du pouvoir des autorités de contrôle.

La Commission nationale de l'informatique et des libertés (CNIL) est l'autorité qui veille à ce que le RGPD soit respecter en France.

II-Le RGPD en 9 points

Point numéro 1 : respecter l'esprit du RGPD

Pour respecter et comprendre le RGPD, l'important est de comprendre **l'esprit du RGPD** : respectez vos utilisateurs, soyez transparents, entourez-vous de partenaires qui respectent le RGPD et sécurisez votre infrastructure pour limiter au maximum les risques concernant les données de vos utilisateurs.

On vous donnera plus d'exemples par la suite mais pour respecter le RGPD vous devez faire preuve de bon sens et d'honnêteté :

- N'envoyez pas d'emails non sollicités ;
- Ne revendez pas les données de vos utilisateurs sans qu'ils aient clairement accepté ;
- Expliquez clairement l'utilisation faites des données que vous récoltez ;
- Ne récoltez que les données nécessaires au fonctionnement de votre entreprise ;
- N'usez pas des dark pattern (fourberie permettant d'amener au consentement plus facilement) ;
- Mettez les données de vos utilisateurs en sécurité.
- Si votre entreprise appartient à un secteur très réglementé (la banque, la santé, la politique), METTEZ LES DONNÉES DE VOS UTILISATEURS EN SÉCURITÉ.

Point numéro 2 : organiser le traitement de la donnée

Ce point vous servira autant à respecter le RGPD qu'à répondre efficacement à vos utilisateurs dès qu'ils auront une question.

Pour bien organiser le traitement de la donnée, voici quelques conseils :

- **Nommez un responsable de la donnée ou un DPO** (délégué à la protection des données) au sein de votre entreprise. Pour une grande entreprise aux besoins complexes, ce dernier devra avoir des compétences juridiques et techniques, pour les plus petites structures, il s'agit plus d'avoir un responsable qui aura une connaissance de tous les sujets liés à la protection des données et qui pourra mettre en place les actions nécessaires si besoin.
- **Cartographiez les données que vous récoltez**. Vous devez connaître précisément les données que vous avez en votre possession et sur quelle catégorie de personnes (utilisateurs, salariés, partenaires).
- **Définissez les objectifs de la collecte de données** ;
- **Définissez la sensibilité des données collectées**, certaines données comme celles de santé, informatiques ou financières sont plus sensibles que d'autres.

Vous n'organiserez pas la donnée de la même manière si vous êtes à la tête d'une banque ou d'un petit e-commerce mais nous vous conseillons de vous poser régulièrement pour faire le point sur la gestion des données de vos utilisateurs et le respect du RGPD.

Point numéro 3 : répondre à vos utilisateurs

Les internautes (oui on utilise encore ce mot-là en 2022) ont pris conscience de l'utilisation faite de leurs données personnelles. **Vous êtes obligé de leur répondre sur ce sujet** et d'accéder aux demandes suivantes :

- La suppression de toutes les données utilisateurs en votre possession ;
- La communication de toutes les données utilisateurs en votre possession ;
- Le non-traitement de vos données.

On en revient à notre DPO du point numéro 2. Avoir quelqu'un en interne en charge de répondre aux demandes utilisateurs qui seront plus ou moins régulières en fonction de votre secteur d'activité vous permettra de gagner du temps et de **répondre plus efficacement**.

Point numéro 4 : s'entourer des bons partenaires

Le RGPD, la CNIL et la police de la data ne vous obligent pas seulement à respecter le RGPD, vos partenaires doivent aussi le respecter.

Vous ne pouvez pas vous défausser sur un partenaire en cas de non-respect du RGPD. C'est en partie pour cette raison que tous les logiciels BtoB que nous analysons mettent en avant la "sûreté de leur solution", le "respect de la protection des données utilisateurs" et du RGPD en règle générale (même si certains disent toujours RPGD au lieu d'RGPD).

Cela peut paraître anecdotique mais si un de vos partenaires ne respecte pas le RGPD, il se pourrait que la CNIL vous embête. Encore plus contraignant, il se pourrait que vous deviez changer en urgence de partenaire.

Point numéro 5 : sécuriser la donnée

Quelle que soit la donnée que vous récoltez et le traitement que vous en faites. **Vous avez l'obligation de sécuriser l'endroit ou les endroits où elles sont stockées**.

La sécurité peut passer par le chiffrement de la donnée, la limitation de l'accès à la donnée en interne ou des prestataires externes spécialisés mais l'objectif reste le même : les données doivent être protégées pour qu'elles ne soient pas utilisées à mauvais escient, volées ou revendues.

Point numéro 6 : obtenir le consentement éclairé

Le RGPD définit ce qu'est le consentement : **il doit être libre, spécifique, éclairé et univoque**. Pour une fois dans cet article, vous n'échapperez pas à quelques définitions.

- **Le consentement libre** signifie que l'utilisateur ne doit pas être ni contraint ni influencé de communiquer ses données personnelles. L'utilisateur doit avoir un choix réel sans subir de conséquences négatives en cas de refus.
- **Le consentement spécifique** signifie que pour chaque nouvelle demande, vous devez obtenir à nouveau le consentement. Par exemple, la communication d'un email pour une inscription ne vous empêchera pas de redemander le consentement pour l'envoi d'une newsletter même si vous avez déjà l'email de la personne.
- **Le consentement éclairé** signifie que l'utilisateur doit pouvoir comprendre facilement l'utilisation qui sera faite de ses données et ce qu'implique son consentement.
- **Le consentement univoque** signifie que l'utilisateur clairement indiqué qu'il est d'accord. Par exemple, la poursuite de la navigation sur un site ne signifie pas "accord". Le consentement doit être donné par un acte positif clair.

Pour respecter le RGPD, oubliez toutes les fourberies des cases précochées, des emails envoyés sans accord ou des petits caractères cachés pour ne pas dire comment la donnée est utilisée.

Point numéro 7 : récolter uniquement la donnée utile

Cela paraît évident mais **vous ne devez récolter que les données nécessaires et pertinentes à l'utilisation de votre produit ou de votre service**.

Pour illustrer ce point, on remercie la CNIL qui nous offre de bons exemples :

- Les informations sur la situation professionnelle de l'entourage d'un candidat n'sont pas pertinent dans un fichier de recrutement ;
- Le numéro de sécurité social n'est pas utile pour l'inscription à l'école.

Point numéro 8 : donner le choix à vos utilisateurs concernant les cookies et les traceurs

Le RGPD connaît de nouvelles évolutions régulièrement. C'est le cas en 2021 concernant les cookies et autres traceurs. On continue dans notre démarche de ne pas vous em****** avec des définitions, **on part du principe que vous savez ce qu'est un cookie ou un traceur**. Depuis 2021, les règles ont changé.

- L'utilisateur doit être clairement informé de la finalité du dépôt de cookies ou traceurs ;
- Il doit pouvoir activer ou désactiver les différents types de cookies, il peut en accepter certains et en refuser d'autres ;
- Le refus doit être aussi facile que l'acceptation ;
- L'interface d'acceptation ou de refus des cookies doit être lisible.

Point numéro 9 : faire une veille régulière

Le RGPD et les lois sur la protection des données évoluent régulièrement. **Nul n'est censé ignorer la loi** comme me disait mon professeur de droit constitutionnel à une époque et vous devrez régulièrement adapter vos pratiques aux évolutions légales.

Encore mieux, regardez régulièrement la manière dont vous pouvez améliorer la gestion de vos données utilisateurs. Par exemple, nous avons profité des vacances d'août et de votre absence pour remettre à plat cette partie chez Tool Advisor et on a quelques chantiers en attente :

- Définir le temps nécessaires de conservation des données des entrepreneurs que nous accompagnons dans leur choix de logiciels ;
- Faire un prêt bancaire ou faire péter notre PEL pour installer un outil de gestion du consentement alors que nous sommes des agneaux de la donnée ;
- Enrichir nos mentions légales.

III-La mise en place du RGPD dans l'entreprise

Étape 1 : **DÉSIGNER UN PILOTE (Résponsable)**

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- **d'informer et de conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- **de contrôler le respect du règlement** et du droit national en matière de protection des données ;

•**de conseiller l'organisme** sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;

•**de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci.

Pour vous accompagner dans la mise en place des nouvelles obligations imposées par le règlement européen, le délégué doit notamment :

•**s'informer** sur le contenu des nouvelles obligations ;

•**sensibiliser** les décideurs sur l'impact de ces nouvelles règles ;

•**réaliser l'inventaire** des traitements de données de votre organisme ;

•**concevoir** des actions de sensibilisation ;

•**piloter** la conformité en continu.

Étape 2 : CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

Pour être en capacité de mesurer l'impact du règlement sur l' activité et de répondre à cette exigence, on devrait au préalable recenser précisément :

•Les différents traitements de données personnelles,

•Les catégories de données personnelles traitées ;

•Les objectifs poursuivis par les opérations de traitements de données ;

•Les acteurs (internes ou externes) qui traitent ces données. Vous devrez notamment clairement identifier les prestataires sous-traitants afin d'actualiser les clauses de confidentialité ;

•Les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Étape 3 : PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

Assurez-vous que **seules les données strictement nécessaires** à la poursuite de vos objectifs sont collectées et traitées.

1.**Identifiez la base juridique** sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)

2.**Révisez** vos **mentions d'information** afin qu'elles soient conformes aux exigences du règlement (articles 12, 13 et 14 du règlement)

3.Vérifiez que vos **sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.

4.Prévoyez les modalités d'exercice des **droits des personnes** concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)

5.Vérifiez les **mesures de sécurité** mises en place.

Étape 4 : **Gérer les risques**

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD).

Étape 5 : **ORGANISER LES PROCESSUS INTERNES**

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

Étape 6 : **DOCUMENTER LA CONFORMITÉ**

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

IV-Sources

https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on#:~:text=Le%20sigle%20RGPD%20signifie%20%C2%AB%20R%C3%A8glement,territoire%20de%20l'Union%20europ%C3%A9enne.

https://tool-advisor.fr/blog/rgpd-pour-les-nuls/

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes