Comment se préparer au GDPR

Il a dernièrement beaucoup été question de la nouvelle législation européenne sur le règlement général de la protection des données, ou GDPR (General Data Protection Regulation). Ce nouveau règlement régit **la manière dont les données à caractère personnel des citoyens européens doivent être traitées, quelle que soit la nationalité de l'organisation traitera ces dernières.**

Le GDPR établit des lignes directrices spécifiques pour la collecte, la gestion et l'utilisation des données qui s'appliquent à tous les résidents de l'UE et à toutes les sociétés opérant dans l'UE. Le non-respect de cette nouvelle loi peut entraîner de lourdes amendes.

Ce guide vous aidera à comprendre la nouvelle loi et ce qu'elle signifie pour la façon dont votre organisation recueille, stocke et utilise les données. Il abordera certaines des définitions légales autour du GDPR, vous proposera des outils pour évaluer la conformité actuelle de votre organisation au GDPR et vous présentera les étapes à suivre pour rester ou devenir conforme.

FFW

Contactez FFW

Pour vous préparer au GDPR, vous devez comprendre quelles données votre organisation sera amenée à collecter, traiter ou stocker et comment votre système se doit d'être configuré afin de respecter les droits des utilisateurs.

Quelle que soit la taille de votre entreprise ou de votre organisation, FFW se tient à votre disposition pour vous soutenir et vous conseiller dans vos démarches de conformité au GDPR. Contactez-nous dès aujourd'hui.

Pour en savoir plus :

ffwagency.com **facebook** **twitter** **linked in**

Qu'est-ce que le GDPR ?

En 2016, l'Union Européenne (UE) a approuvé un règlement général sur la protection des données à caractère personnel des citoyens européens.

La loi vise à assurer **"la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation de ces données".**

Que cela signifie-t-il pour vous ou votre organisation ?

En termes simples, le GDPR est une nouvelle loi qui protège les données des citoyens européens. Il existe entre autres deux types de législation dans l'UE :

Les directives
qui instaurent une obligation de résultat tout en laissant les Etats membres libres quant aux moyens d'y parvenir.

Les règlements
qui sont immédiatement et uniformément applicables dans les Etats membres.

Le GDPR étant un règlement, il est applicable dès son entrée en vigueur et devient une loi dans tous les États membres de l'UE. Axé sur la protection des données à caractère personnel, il s'applique à toute organisation qui collecte, stocke ou exploite les données d'un citoyen de l'UE, même si cette organisation est basée en dehors de l'UE.

Si vous consultez le GDPR, vous rencontrez l'expression **"Règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel".** Cette nomenclature est importante car elle inclut plusieurs distinctions juridiques dont les organisations doivent tenir compte :

Une **personne physique** est un être humain auquel on a attribué la jouissance de droits.

Les **données personnelles** sont toutes les informations relatives à une personne physique identifiée ou identifiable. Il peut s'agir de leur nom, de leur numéro d'identification, des données de localisation, d'un identificateur en ligne ou de tout autre facteur physionomique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

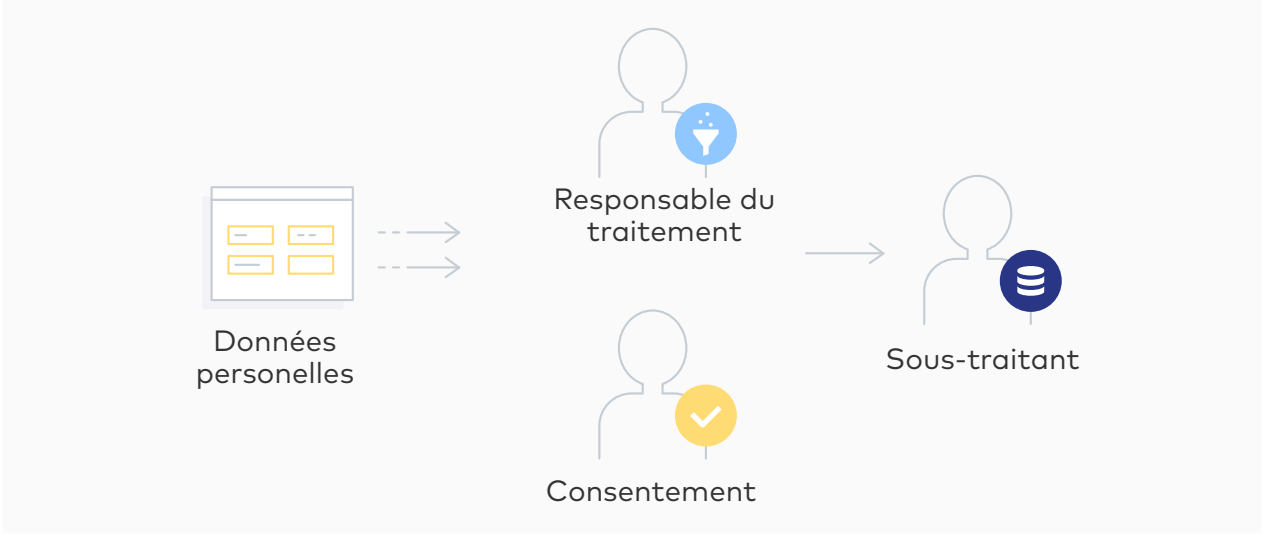
Traitement désigne toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel. Cela comprend la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou toute autre forme de mise à disposition, ainsi que l'effacement ou la destruction de ces données.

Comprendre le champ d'application "données personnelles" et "traitement" peut aider les organisations à mieux comprendre l'ampleur de ce règlement **qui entrera en vigueur le 25 mai 2018.**

Les organisations exerçant des activités au sein de l'EU devront obligatoirement se conformer au GDPR, toute infraction entrainant des amendes graduées pouvant aller, pour les plus lourdes, **jusqu'à 10 millions d'euros ou 2% du chiffre d'affaire annuel global.** Les amendes seront également très lourdes pour les entreprises, services ou organismes devant répondre de la violation de données à caractère personnel (comme récemment Talk Talk, qui s'était fait subtiliser 170 000 de ces données). Pour les infractions très lourdes, ces chiffres peuvent doubler.

Qui doit se conformer au GDPR ?

La réponse est simple : tout le monde. Si votre organisation dispose des données d'un citoyen de l'UE quelque part dans vos systèmes, vous devez alors vous assurer que vous êtes conforme. Il y a quelques définitions primordiales à comprendre lorsque l'on se prépare à se conformer à la norme GDPR.



Responsable du traitement

Responsable du traitement est l'organisation ou la personne "responsable" des données. Officiellement, le responsable du traitement détermine les finalités et les moyens du traitement des données à caractère personnel.

Un responsable peut être une personne physique ou morale, une autorité publique, une agence ou un organisme agissant seul ou conjointement avec d'autres.

Ainsi, lorsque vous avez téléchargé ce guide de FFW, vous nous avez donné votre nom, votre courriel et peut-être quelques informations sur votre employeur. Cela fait de nous le responsable du traitement des données que nous avons collectées lorsque vous avez rempli le formulaire de téléchargement sur notre site Web.

Consentement

Il incombe au responsable du traitement de traiter les données de manière licite, loyale et transparente. La licéité du traitement ne peut être garantie que si la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques. Le consentement doit être donné librement et donner une indication précise, compréhensible et non ambiguë des souhaits de la personne concernée. Ici, la loi est très claire sur ce qui constitue le consentement : les utilisateurs doivent faire une déclaration compréhensible et formulée en des termes clairs et simples pour affirmer que leurs données peuvent être utilisées.

Les lignes directrices entourant le consentement signifient qu'il doit y avoir un avis de confidentialité clair pour les utilisateurs lorsqu'ils saisissent leurs données. L'avis doit indiquer très clairement pourquoi le consentement est demandé et ce qu'il adviendra de ces données. De plus, les gens doivent toujours opter pour l'adhésion plutôt que pour la non-participation. Des libellés compliqués et des options pré-choisies seraient considérés comme une violation des règles de consentement. En tant que responsable du traitement, vous devrez être clair sur le fait que vous demandez la permission d'utiliser les données des visiteurs/ utilisateurs d'un site et sur la raison de votre demande.

Sous-traitant

Le sous-traitant est l'organisation ou la personne qui manipule, stocke ou détruit les données. Comme dans le cas d'un responsable du traitement, un sous-traitant peut-être une personne physique ou morale, une autorité publique, une agence ou un autre organisme. Un sous-traitant peut gérer des informations pour le compte ou à la demande d'un responsable du traitement.

Nous pouvons ici aussi prendre notre cas pour illustrer cette situation. Certains des services de FFW peuvent inclure le stockage et la récupération des données pour le compte de nos clients sur leurs propres clients. Cela fait de nous un sous-traitant pour une organisation tierce même si nous ne tirons aucun bénéfice personnel ou organisationnel ni ne traitons les données collectées.

Le but du GDPR est la protection de la vie privée

Le GDPR est très clair quant au fait que les organisations devront être capables et prêtes à prouver leur respect des exigences de la loi. Il s'agit d'une approche proactive et non pas réactive : Si quelqu'un vous contacte pour s'assurer que vous êtes conforme au GDPR, vous devrez être en mesure de démontrer dans l'instant que votre organisation est conforme aux règlements du GDPR.

Selon le GDPR, toutes les données....

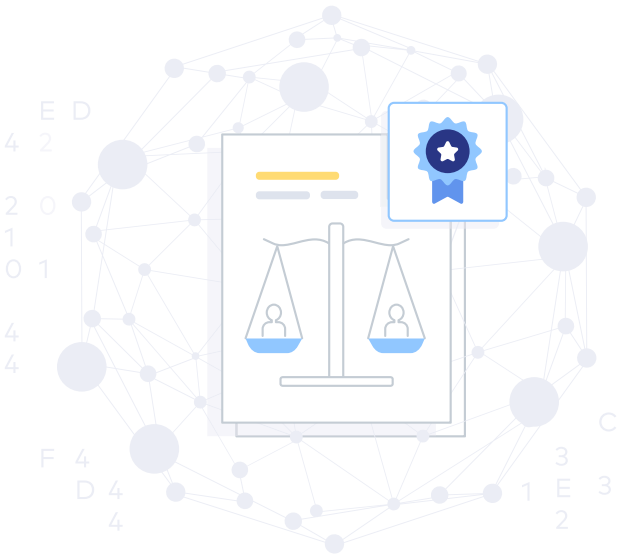
1. Doivent être traitées de manière légale, équitable et transparente.
2. Doivent être collectées à des fins précises, explicites et légitimes.
3. Doivent être tenu à jour.
4. Doivent être limité à ce qui est nécessaire.
5. Ne devraient pas permettre l'identification des personnes plus longtemps que nécessaire.
6. Doivent être traité de manière à garantir une sécurité appropriée.

Une fois appliqués, ces principes peuvent se résumer à l'idée suivante :

Les données doivent être collectées avec le consentement explicite de l'utilisateur et tous les utilisateurs doivent savoir exactement à quoi serviront leurs données. La collecte et la conservation des données ne doivent se limiter qu'à ce que votre organisation a absolument besoin de savoir sur un utilisateur. Votre organisation doit être en mesure de démontrer qu'une demande de consentement a été présentée clairement et que les données ne sont pas vendues, modifiées ou utilisées de manière abusive. Les systèmes ne devraient pas s'appuyer sur des données désuètes ou vieilles de plusieurs années à des fins commerciales ou de marketing et si les utilisateurs souhaitent mettre à jour leurs données ou retirer leur consentement, ils devraient pouvoir le faire facilement.

Enfin et surtout, les données doivent être conservées en lieu sûr et traitées de manière à protéger les personnes auxquelles elles appartiennent.

Comprendre vos droits et les droits de vos utilisateurs



Les règles du GDPR ont été conçues autour des droits des citoyens européens sur leurs données personnelles. Elles sont :

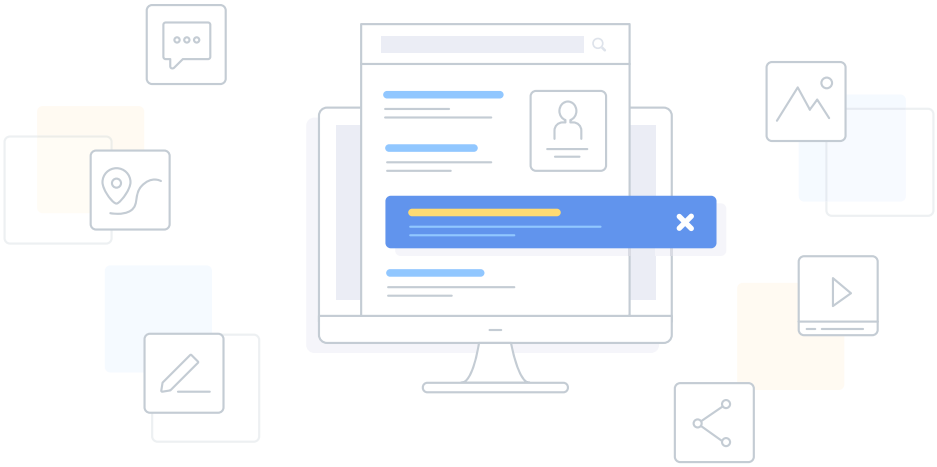
- Le droit d'être informé ;
- Le droit d'accès ;
- Le droit de rectification ;
- Le droit à l'effacement (droit à l'oubli) ;
- Le droit de restreindre le traitement ;
- Le droit à la portabilité des données ;
- Le droit de s'opposer ;
- Le droit de ne pas faire l'objet d'une prise de décision automatisée, y compris le profilage

En plus de veiller à ce que votre organisation respecte les règles relatives à la collecte, au stockage et au traitement des données en toute sécurité, vous devrez également vous assurer que vous disposez de systèmes qui permettent aux citoyens européens d'exercer leurs droits en ce qui concerne leurs données. **Vous devrez vous assurer d'avoir des processus, des procédures et une formation au sein de votre équipe afin que les utilisateurs puissent exercer leurs droits.**

En outre, toutes les formes de communication devraient être concises et facilement accessibles. Utilisez un langage clair et simple, même sur les documents juridiques - vous pourrez éventuellement être amené à les modifier afin de les rendre accessibles au grand public.

Un exemple de construction d'un cadre pour les droits sur les données

Pour savoir comment s'assurer que votre système est conforme, il suffit de regarder le cas de Google. En mai 2015, la Cour de justice de l'UE a statué que les moteurs de recherche sont responsables du contenu qu'ils désignent et qu'ils doivent de fait se conformer à la législation de l'UE en matière de protection de la vie privée. Plus précisément, Google a été prié de respecter le droit à l'oubli.



Selon Reuters, "les sociétés Internet peuvent être incitées à supprimer des informations personnelles non pertinentes ou excessives dans les résultats des moteurs de recherche... La Cour de justice de l'Union européenne (CJCE) a confirmé la plainte d'un citoyen espagnol qui s'opposait au fait que le résultat de la recherche de son nom dans Google mené vers des liens d'un article de journal de 1998 sur la reprise de possession de son domicile." En vertu de cette décision, toute personnalité non publique "devrait pouvoir effacer ses traces numériques de l'Internet".

Pour respecter le droit des utilisateurs à l'oubli, Google a créé un cadre pour supprimer les résultats de recherche de l'index communautaire et a créé un processus permettant aux utilisateurs de demander que leurs informations soient supprimées.

Il s'agit là d'un exemple clair de la manière dont une très grande organisation a mis en place des processus et des procédures permettant aux personnes d'exercer leurs droits. Si quelqu'un peut supprimer ses informations de Google, il devrait également être en mesure de pouvoir supprimer ses informations de vos systèmes.

Mettre en œuvre un plan de préparation en 8 étapes pour GDPR

La première étape de préparation au nouveau GDPR consiste à évaluer vos politiques et procédures existantes. Quelles données recueillez-vous et pourquoi ? Ces données sont-elles sécurisées ? Les utilisateurs peuvent-ils effacer leurs données de vos systèmes ? Établissez des processus, des procédures et assurez la formation du personnel afin que votre organisation soit en mesure de traiter avec des personnes qui voudront simplement exercer leurs droits.

Au-delà de cet aspect, il y a quelques éléments clés que vous devez faire pour préparer votre organisation :

1. Sensibiliser les gens

Veillez à ce que les décideurs et les personnes clés de votre organisation soient conscients que la loi actuelle va être remplacée par le GDPR. Ils doivent comprendre l'impact que cela aura probablement et vous devez avoir leur adhésion pour apporter les changements nécessaires à vos systèmes...

2. Effectuer un audit de vos informations

Documentez les données personnelles que vous détenez, d'où elles proviennent et avec qui vous les partagez. Dans le cadre de cette démarche, vous devrez éventuellement revoir vos avis de confidentialité actuels et mettre en place un plan pour apporter les changements nécessaires. Vérifiez également les procédures que vous avez mises en place pour vous assurer que les citoyens européens peuvent exercer leurs droits sur votre site. Il devrait être simple pour les utilisateurs de fournir, mettre à jour ou supprimer leurs données personnelles des systèmes de votre organisation.

3. Mettre en place un plan de traitement des demandes d'accès

Si vous recevez une demande d'accès de la part d'une personne ou d'un organisme officiel qui doit vérifier la conformité de votre organisation ou de vos procédures, vous devrez réagir. Assurez-vous de créer ou de mettre à jour les procédures que vous avez mises en place pour fournir les données et planifiez la façon dont vous traiterez ces demandes, le cas échéant.

4. Vérifier le fondement légal du traitement

Vérifiez et comprenez comment vous et votre organisation traitez les données, pour quelles raisons, et assurez-vous que vos utilisateurs donnent leur consentement explicite. Avant que le GDPR n'entre en vigueur, assurez-vous que vous traitez les données légalement, que vous disposez de documents à l'appui et que vous avez mis à jour votre avis de confidentialité pour l'expliquer.

5. Vérifiez vos systèmes quant aux utilisateurs mineurs

Il s'agit d'une étape très importante que certaines organisations peuvent négliger. Selon la façon dont vous recueillez les données, vous devrez peut-être mettre en place des systèmes pour vérifier l'âge de la personne et obtenir le consentement des parents ou du tuteur pour les enfants dont vous pourriez recueillir les données.

6. Élaborer un plan pour les violations de données

Aucune organisation ne souhaite que ses données soient compromises. Néanmoins, vous devez d'abord vous assurer que vos données sont aussi sécurisées que possible pour ensuite mettre en place des procédures et des systèmes pour détecter, signaler et enquêter sur une éventuelle violation de données personnelles. Pour vous assurer que vos systèmes sont conformes aux règles de protection, familiarisez-vous avec les dernières directives du groupe de travail « Article 29 » sur la protection des données. Planifiez entre autres comment mettre en œuvre les évaluations des facteurs relatifs à la vie privée dans votre organisation.

7. Responsables de la protection des données

Désignez quelqu'un (au sein de votre organisation ou d'une entité juridique) pour prendre la responsabilité du respect de la protection des données. Évaluez sa place et son rôle au sein de votre structure.

8. Comprendre les directives internationales

Si votre organisation opère dans plus d'un État membre, déterminez l'autorité de contrôle responsable de la protection des données. Peut-être ne savez-vous pas où commencer ? En décembre 2016, le Groupe de travail « Article 29 » ("WP29") a publié un Guide pour l'identification d'une autorité de surveillance (NB: En anglais uniquement) afin d'aider les organisations à prendre cette décision. Pour faciliter le processus d'identification d'une autorité de contrôle, vous devez surtout savoir où votre organisation prend des décisions concernant les activités de traitement.

Désignez un représentant

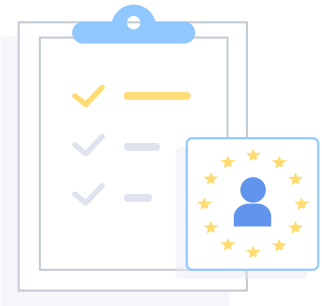
Les organisations qui ne sont pas établies dans l'UE mais qui opèrent dans l'UE, ou qui traitent les données de personnes vivant dans un état membre de l'UE, doivent trouver un/e représentant/e au sein de l'UE.

Selon l'article 4 du GDPR :
"Toute personne physique ou morale résidant dans l'un des États membres peut être désignée comme représentant/e dans l'Union d'une société non basée dans l'UE."

Il incombe au/ à la représentant/e de fournir tous les renseignements demandés qui peuvent être requis par une autorité de surveillance.

Une fois qu'un/e représentant/e a été identifié/e, vous devez le/la désigner par écrit comme représentant/e de votre organisation. Il/Elle représente le/la responsable du traitement ou le sous-traitant en ce qui concerne leurs obligations respectives au titre de GDPR.

Quelques remarques sur les représentants :



- Un/e représentant/e doit être établi/e dans l'un des États membres de l'UE où se trouvent les personnes concernées par les données.
- Il est de votre responsabilité de désigner un/e représentant/e sans préjudice des poursuites judiciaires qui pourraient être intentées contre votre entreprise.
- Un/e représentant/e fera l'objet de toute procédure d'exécution forcée en cas de non-respect par la société. Cela signifie que votre entreprise et votre représentant pourraient être assujettis à des pénalités si vous ne respectez pas la loi.

À mesure que la date d'entrée en vigueur du GDPR approche, de nombreux prestataires de services apparaissent dans l'UE pour les organisations qui doivent désigner des représentants.

Prochaines étapes

Pour vous préparer au GDPR, vous devez comprendre quelles données créez-vous, où et comment les traitez et les stockez-vous et enfin comment votre organisation et vos systèmes respectent les droits des utilisateurs.

Nous vous recommandons de commencer par identifier comment les données personnelles circulent sur votre site.

Une fois les données que vous utilisez et la façon dont vous les utilisez identifiées, vous pouvez commencer à créer des systèmes pour garantir la protection de la vie privée de vos utilisateurs et mettre en place des processus permettant à ces derniers d'accéder à leurs données, de les mettre à jour ou de les supprimer.

Si vous avez besoin d'aide pour vous conformer aux nouvelles réglementations du GDPR, contactez FFW. Nous proposons une Boite à Outils de Conformité au GDPR qui analyse votre présence numérique pour identifier les problèmes potentiels de conformité et vous fournir les recommandations nécessaires pour y remédier.

Nos experts GDPR sont dès maintenant à votre disposition pour s'assurer de la conformité de vos systèmes et de vos procédures de traitement des données à caractère personnel.