Audit GDPR

diatem
connecting everything

GDPR ?

Mai 2018

En mai 2018 entrera en vigueur la loi européenne de protection des données personnelles, la «General Data Protection Regulation» ou plus simplement : «GDPR».

Elle concerne toutes les entreprises, toutes les organisations et associations à partir du moment ou celles-ci répondent à ces deux problématiques :

Entreprise ou organisation domicilée sur le territoire européen

Collectant ou traitant des données personnelles

Quel impact ?

La loi impose de nombreuses obligations nouvelles aux organismes concernant le traitement des données personnelles. Les mesures à mettre en place sont diverses et concernent aussi bien les aspects purement technique de collecte, conservation et traitement, la gestion de la vie des données et de leur usage, mais plus largement la philosophie même des procédures au sein de l'entreprise.

La mise en place de la GDPR sera accompagnée de mesures de contrôle renforcés pouvant déboucher sur des injonctions de mise en conformité voire à des sanctions pécunières pouvant atteindre 4% du chiffre d'affaire mondial.

SOMMAIRE

1
LA GDPR EN DÉTAILS

“Qui, pourquoi, comment ? Les clés pour appréhender au mieux cette nouvelle réglementation.”

2
COMMENT COMMENCER ?

“La GDPR remet en perspective toute la politique de gestion de la donnée au sein de l’entreprise. Quelques étapes simples pour commencer à penser GDPR.”

3
LES APPORTS ET PRESTATIONS DE DIATEM

“Diatem peut être un partenaire de la continuité de votre stratégie GDPR sur le Web. Découvrez comment.”

LA GDPR en détails

Pour qui ?

Le règlement s'appliquera à tous les acteurs économiques, voire sociaux : les entreprises bien sûr, mais également les associations, administrations, collectivités locales et syndicats entreprises.

En effet, lorsque l'on parle de données personnelles, on inclut les informations des employés, clients, partenaires, prospects, que celles-ci se trouvent sur des ordinateurs, des terminaux mobiles ou des serveurs, dans des échanges emails ou dans la consignation des logs et du traçage, même non identifié, des visiteurs du site Internet de l'entreprise. Entre le caractère omniprésent des données numériques et la notion d'identification directe et indirecte, aucune société ne pourra y échapper.

De nouveaux devoirs...

En reposant sur le droit de chacun à la protection de ses données personnelles, le nouveau règlement impose des devoirs qui sont autant d'obligations aux entreprises. Celles-ci seront notamment tenues en principe de s'assurer du consentement éclairé et informé des individus quant à la collecte et au traitement de leurs données, consentement qu'elles devront pouvoir recueillir et prouver.

Elles veilleront à ce que seules les données nécessaires à la finalité en cause, et seulement pour celle-ci, soient collectées. Les données ne devront être conservées aussi longtemps que nécessaire et leur accès, leur modification, leur restitution jusqu'à leur effacement sur la demande des individus concernés, devront être garantis.

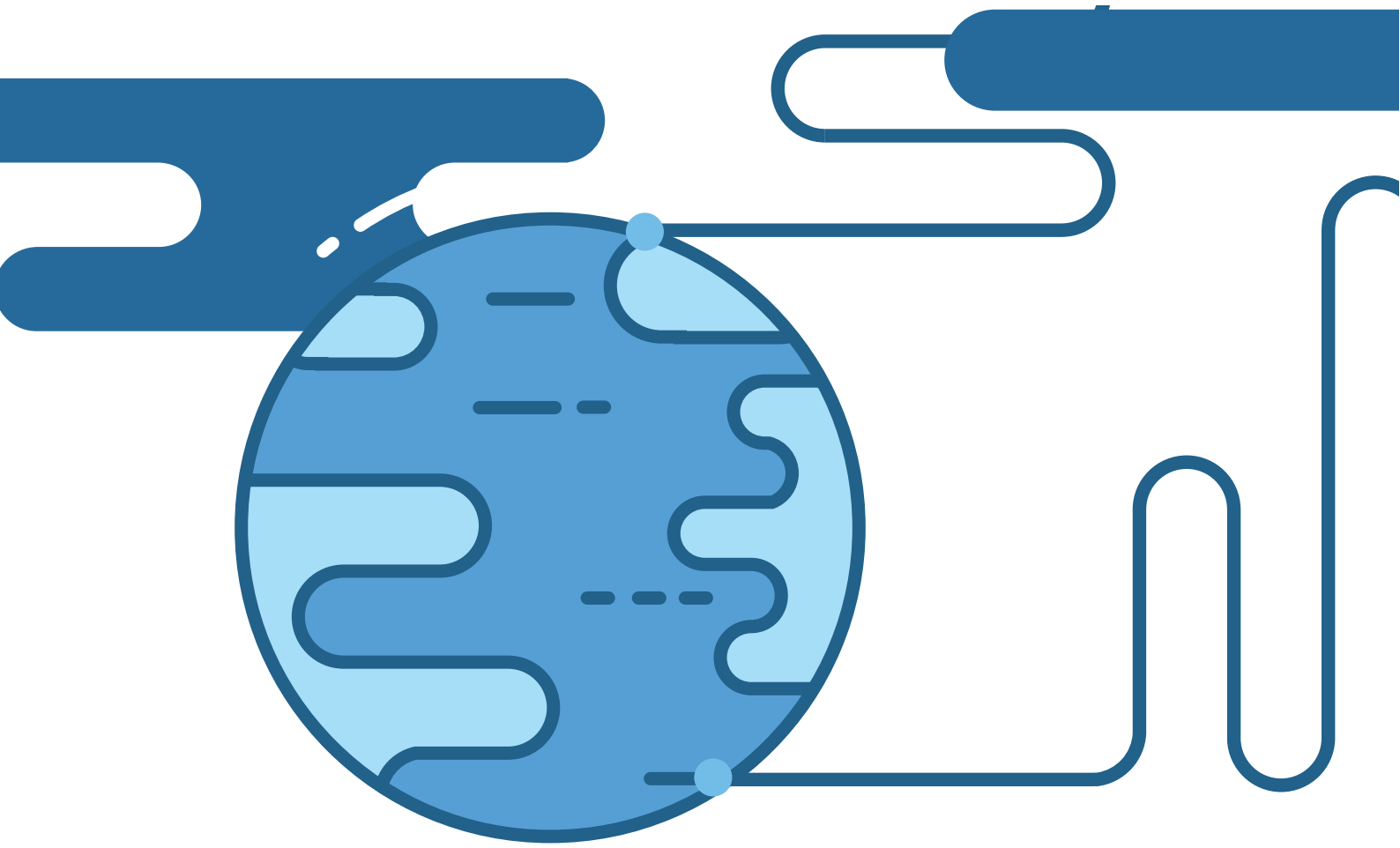
L'entreprise veillera également à ce que ces données soient à tout moment et en tous lieux sécurisées contre les risques de perte, de vol, de divulgation ou contre toute autre compromission. Si, malgré tout, un tel événement se produisait, alors l'entreprise en question devrait le notifier rapidement (idéalement sous 72 heures) à l'autorité compétente, la Cnil en France, et informer les personnes concernées en cas de risque réel d'atteinte à la protection de leur vie privée.

L'entreprise devra en outre documenter toutes les mesures et procédures utiles pour assurer à tout moment cette protection. Elle ne pourra transférer en dehors de l'Union Européenne ces données que selon un cadre strictement défini par le règlement et n'engager pour le traitement de ces données que des entreprises tierces offrant toutes les garanties nécessaires pour répondre à ces obligations. Enfin, à tout moment, elle devra pouvoir prouver aux autorités compétentes que tout est bien mis en oeuvre pour répondre à ces obligations.

...et des sanctions

Celles-ci peuvent aller jusqu'à 4 % du chiffre d'affaires annuel mondial ou 20 millions d'euros. Et c'est également l'entreprise qui devra indemniser toute personne lésée matériellement ou moralement par un traitement non-conforme de ses données, sans plafonnement. La nécessité d'une approche de cyber-résilience dans le traitement des données personnelles

Les obligations du GDPR supposent qu'une entreprise doit à tout moment savoir de quelles données elle dispose, leur localisation, l'objectif de leur collecte et leur mode de gestion, stockage, sécurisation, transfert et effacement. Au-delà de cette quasi omniscience, elle doit être en mesure de déceler si leur intégrité a été compromise et y remédier promptement, tout en consignant et notifiant l'événement.



Bénéfique à l'entreprise

Au-delà du traitement administratif du sujet, ces différentes obligations imposent à l'entreprise d'adopter une approche résolument cyber-résiliente, et donc d'intégrer la sécurité au coeur de son traitement des données, sous peine de sanctions bien plus élevées que l'investissement initialement nécessaire. Cette cyber-résilience suppose que l'entreprise se prépare à des cyber-attaques, dont la question n'est plus de savoir « si » mais « quand » elles se produiront. Ce processus de préparation doit être minutieux et planifié, avec une véritable évaluation et une cartographie des données et une analyse des incidents de sécurité.

Il permettra ainsi une détection plus rapide d'un risque avéré et une réponse plus efficace qui évitera le développement de l'attaque à davantage de systèmes et ainsi des préjudices supplémentaires. L'entreprise devra également veiller à se protéger contre ces attaques, ce qui implique bien entendu la mise en place et la mise à jour de technologies de protection, mais également une véritable formation, continue et renouvelée, des personnels impliqués. Les organisations devront donc suivre l'adage selon lequel « il vaut mieux prévenir que guérir », mais devront également tester régulièrement cette préparation afin de déterminer les failles potentielles et d'y remédier.

Cette gestion des risques étendue liée à la protection des données devra être partagée par et avec l'ensemble de l'entreprise, depuis les dirigeants en passant par les différents métiers et bien entendu jusqu'aux responsables de la sécurité des systèmes d'information.

Comment commencer ?

Vous l'avez compris, la couverture de la nouvelle règlementation est bien plus large qu'une simple modification des procédures de collectes des données et n'impacte pas uniquement des maillons spécifiques de l'entreprise mais doit bien être considérée comme une nouvelle manière d'appréhender la gestion de l'information au sein de l'entreprise, et ce de manière globale et transparente.

Afin de guider les entreprises dans ces changements considérables la CNIL propose une méthode en 6 étapes permettant de définir des jalons efficaces. Nous proposons de passer en revue rapidement ces 6 étapes afin de vous donner une grille rapide de compréhension de la marche à suivre globale :

Etape 1 : désigner un pilote

La GDPR introduit un rôle nouveau dans l'entreprise : le délégué à la protection des données. Le délégué à la protection des données aura pour rôle de piloter la gestion des données personnelles de votre structure. Il pourra aussi bien guider l'entreprise dans les nécessaires changements qu'elle devra opérer mais également d'assurer par la suite le respect des normes et la formation des salariés aux bonnes pratiques en la matière. La désignation d'un délégué à la protection des données n'est pas obligatoire mais est très fortement recommandé – ne serait-ce que parce qu'elle démontre de votre volonté de bien faire auprès des organismes de contrôle.

Etape 2 : cartographier les traitements de données personnelles

L'idée est ici de recenser précisément les différents processus de collecte, de stockage et de traitement de données personnelles. Pour chacun de ces traitements l'objectif sera de répondre à des questions précises touchant à la nature des données, aux risques encourus et aux mesures mises en place pour en assurer leur sécurité. Ce travail débouchera sur la réalisation d'un registre des traitements.

Etape 3 : Prioriser les actions à mener

L'étape 2 conduit naturellement à identifier les faiblesses du fonctionnement actuel et à rechercher des moyens à mettre en œuvre pour y palier et ainsi se mettre en conformité avec les obligations actuelles et à venir. Il s'agira ensuite de peser l'impact positif de chaque mesure afin de prioriser et planifier les actions correctives à mener.

Etape 4 : gérez les risques

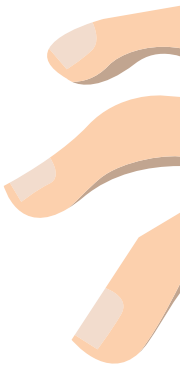
Si au cours de l'étape 2 vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques médians à élevés pour les droits et les libertés des personnes il vous faudra mener pour chacun de ces traitements une analyse d'impact sur la protection des données. (ou « PIA »)

Etape 5 : organiser les processus internes

La protection des données personnelles n'est pas qu'une affaire de technique mais également de formation des personnes aux bonnes pratiques. Il conviendra d'assurer cette formation, de suivre l'application des directives mais aussi de réagir conformément à la directive en cas de brèche dans les protections mise en place. (Information obligatoire des personnes)

Diatem vous propose son expertise relative à l'application des modification liées à la GDPR applicable aux outils Web. (site Internet, intranet, outil de mailing...)

Si nous ne pourrons pas nous substituer à une analyse globale de vos procédures de collecte et de traitement de données, car elle suppose une connaissance globale de votre entreprise que nous ne pouvons avoir, nous pourrons cependant vous conseiller et accompagner votre processus de conformité GDPR pour le Web.



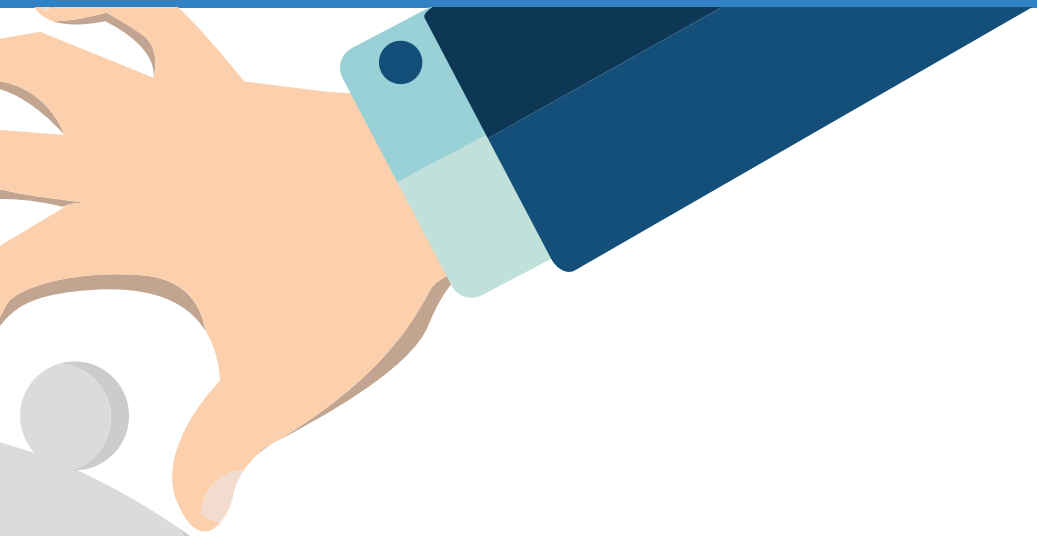
Audit

Nous vous proposons de réaliser un audit de votre solution Web afin de mettre en évidence :

- Les typologies de collecte et de traitement de données personnelles mises en œuvre
- Un schéma mettant en évidence les processus de collecte, stockage, traitement et éventuellement transmission des données
- Les processus en place permettant de se conformer aux impératif d'accès, modification et suppression des données personnelles
- Les anomalies majeures
- Identification des éventuelles données pouvant nécessiter la réalisation d'études d'impact de par leur caractère sensible ou leur portée.
- Les manquements et failles des mentions légales

Ceci permettant de déboucher sur un ensemble de préconisations et mesures correctives permettant de faciliter la mise en conformité de votre solution Web avec la politique globale de gestion des données mise en place au niveau de votre entreprise.

APPORTS & PRESTATIONS DIATEM



Mise en place des mesures correctives et documentation

En lien direct avec l'audit réalisé nous vous proposerons ensuite la mise en conformité via les actions suivantes :

- Mise en place des mesures correctives identifiées.
- Réalisation d'un registre des traitements spécifique aux opérations de collecte/stockage/traitement identifiés
- Analyses d'impact sur la sécurité des données pour les opérations de traitement les plus impactantes
- Documentation sur les mesures de protection et de sécurisation des données mise en place sur les infrastructures d'hébergement Diatem.
- Récapitulatif de l'audit réalisé et des mesures correctives mises en place.