LA LOI NOUVELLE INFORMATIQUE RGPD

QUESTIONNAIRE

Connaissez vous la nouvelle loi informatique prévue au 25 mai 2018, une étude estime que 30% des DSI n'auraient pas connaissance du GDPR (General Data Protection Régulation) ou RGPD (Règlement Général sur la Protection des Données en français, découvrez notre document et notre questionnaire afin de vous préparer à cette nouvelle loi,

AVANT TOUT : Avez-vous désignez un pilote de votre RGPD ?

RERPERTORIER : Possédez-vous un inventaire des contenus et conteneurs des données à caractère personnel ? – *Voir PAGE 4*

- ☐ Liste des fichiers stockés sur des postes locaux, les serveurs et les clouds.
- ☐ Liste des applications locales et sur le cloud.

EVALUER : Connaissez-vous les accès aux données à caractère personnel ? – *Voir PAGE 5*

- ☐ Type de contenu
- ☐ Type d'accès
- ☐ Risques
- ☐ Archivage

GERER : Avez-vous face aux données à caractère personnel, la capacité ? – *Voir PAGE 6*

- ☐ D'informer les personnes concernées
- ☐ De définir leur nature
- ☐ Leur limitation et leur effacement

SECURISER : Connaissez-vous le niveau de protection des données à caractère personnel ? - *Voir PAGE 7*

- ☐ Antivirus, antiransomware et cryptoguard.
- ☐ Analyseur détaillé d'attaque.
- ☐ Plan de Reprise d'Activité et archivage
- ☐ RTO et RPO

RECHERCHER : Savez-vous répondre aux droits existants des personnes physiques ? - *Voir PAGE 8*

- ☐ Droit d'accès aux données.
- ☐ Droit de copie ou de rectification
- ☐ Droit à l'oubli

REPONDRE : Avez-vous la capacité de répondre à la CNIL ? - *Voir PAGE 9*

- ☐ D'identifier la provenance de n'importe quelle donnée.
- ☐ Accéder à tous les endroits où se trouvent les données.
- ☐ Accéder à tous les mails de votre organisation.

INTRO

- Alors que sa mise en application est prévue au 25 mai 2018, une étude estime que 30% des DSI n'auraient pas connaissance du GDPR (General Data Protection Régulation) ou RGPD (Règlement Général sur la Protection des Données) pour les francophones.

- A leur décharge :un texte long de 200 pages, comportant 99 articles :rien que ça !

- Cette réglementation, qui conforte les grands principes de la Loi Informatique et Libertés, octroie de nouveaux droits aux personnes physiques sur leurs données à caractère personnel, comme le droit à l'oubli ou la portabilité des données, et impose de fait de nouvelles contraintes pour les entreprises et administrations... avec à la clé des sanctions dissuasives.

- Celles-ci pourront en effet atteindre jusqu'à 20 millions d'euros ou 4% du CA global (la somme la plus élevée étant retenue), sans compter le risque d'atteinte à l'image de la société que comporte une condamnation.

- Mais rassurez-vous, avant que l'on ne vous porte ce coup de grâce, qui concerne les infractions les plus graves, le texte prévoit une batterie de rappels à l'ordre, d'injonctions et d'amendes intermédiaires pondérées en fonction de la nature de la violation, de l'intention, des mesures prises pour atténuer celle-ci, du degré de coopération avec l'autorité locale (la CNIL en France).

- Si le règlement concerne bien évidemment l'organisation dans son ensemble, elle s'adresse tout particulièrement à vous, les directions des systèmes d'information, qui êtes responsables de la gestion des données et des relations avec les sous-traitants (éditeurs SaaS, hébergeurs, etc.).

- Le langage juridique n'étant pas toujours des plus accessibles, nous vous expliquons dans cet ebook les principaux tenants et aboutissants de ce règlement, simplement, et nous vous recommandons, en parallèle de vos mesures organisationnelles et commerciales, de prendre des mesures techniques pour vous conformer au mieux et rapidement à la nouvelle réglementation.

C'EST QUOI LA LOI RGPD

Quoi ?

- Le règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Donnée à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable. Cela concerne tous les interlocuteurs d'une entreprise qu'il s'agisse de ses salariés, clients ou encore partenaires et fournisseurs.
- Certaines données personnelles ont un statut particulier : les données sensibles qui sont par principe interdites de traitement sauf exceptions prévues par le règlement. Il s'agit des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, des données génétiques, biométriques, ou encore celles concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.
- Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés sur la donnée (collecte, enregistrement, organisation, structuration, conservation, modification, communication... jusqu'à sa destruction).
- Un traitement est licite dès lors qu'il répond à au moins une condition de l'article 6 : consentement de la personne physique, nécessité à l'application d'un contrat auquel la personne a souscrit, obligation légale, intérêts vitaux de la personne concernée ou d'une autre personne physique, nécessité d'ordre public.

Qui ?

Peut être partagée par voie contractuelle avec la notion de cotraitance. Les entreprises et les administrations, ainsi que leurs sous-traitants, effectuant un traitement de données à caractère personnel relatives à des ressortissants de l'Union européenne. La nouveauté du RGPD réside dans une responsabilisation accrue des sous-traitants, avec qui la responsabilité peut être partagée par voie contractuelle avec la notion de cotraitance,

Où ?

La territorialité s'étend désormais à l'international : les entreprises, responsables de traitement ou sous-traitants, hors de l'Union européenne sont concernées dès lors que le traitement s'applique à l'offre de biens ou de services s'adressant à des personnes dans l'U.E. ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'U.E.

En cas de traitement transfrontalier, le responsable de traitement peut définir quelle sera l'autorité locale référente (la CNIL en France) qui coopérera avec les autres autorités européennes. Cette notion de « guichet unique » s'adresse aussi aux personnes physiques qui souhaitent effectuer des réclamations : elles pourront passer par l'autorité locale de leur pays.

Quand ?

Après de longs mois de discussions et d'amendements, le texte a finalement été adopté le 14 avril 2016. Il remplacera en France la Loi Informatique et Libertés à compter du 25 mai 2018, sans passer par une transposition nationale. Néanmoins, des décrets définiront les points laissés à l'appréciation de chaque pays membre.

Comment ?

La mise en conformité passe par la mise en place de mesures organisationnelles et techniques. Le règlement rappelle l'importance des certifications notamment dans le choix des sous-traitants. Le responsable de traitement a la possibilité de se faire aider par l'autorité locale qui explicitera les bonnes pratiques en fonction de son secteur d'activité. Si la nomination d'un DPO (Data Protection Officer), qui remplacera la fonction du CIL actuel (Correspondant Informatique et Libertés), est encouragée, elle est obligatoire pour certaines organisations :

- les autorités ou les organismes publics ;
- les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.
- Son rôle est de centraliser et de coordonner en interne la gestion des traitements, notamment par de la sensibilisation. Il sera également le point de contact avec l'autorité locale pour remplir les formalités et coopérer en cas d'audit ou de litige.

RÉPERTORIER

ETAPE 1 – Gagner en visibilité

Pour préparer la mise en conformité, le point de départ est d'être en mesure d'identifier les données personnelles traitées par l'entreprise. Avec des données non-structurées dans 80% des cas, dispersées et généralement non sécurisées, la première difficulté est de faire face aux Dark Data. Gartner les définit comme «les données qui échappent à l'organisation de l'entreprise : ce qui n'est pas répertorié par l'entreprise mais par les salariés eux-mêmes qui 'cachent' ces données volontairement ou involontairement».

QUE DIT LA LOI ?

L'article 30 impose au responsable de traitement de produire un registre sur les traitements afin

de remplacer les formalités actuelles auprès de la CNIL. On parle alors d'«accountability».

Celui-ci demande de répertorier les traitements ainsi que leurs caractéristiques finalité,

catégories de données, destinataires, etc.

Les sous-traitants doivent également tenir, en plus de leur propre registre, un registre des traitements pour lesquels ils sont prestataires.

Mais s'il est important d'avoir une photo à un instant « t », le registre suppose d'auditer régulièrement le traitement des données et de mettre en place un monitoring pour effectuer des correctifs.

La gouvernance des données devient un enjeu de premier plan pour être conforme, avec la

nécessité de pouvoir documenter le pilotage et le monitoring de cette conformité.

ÉVALUER

ETAPE 2 – Exposer le risque

La deuxième mesure est de pouvoir évaluer le niveau de risque :qui a accès aux données ? Par qui sont-elles consultées ou au contraire depuis combien de temps n'ont-elles pas été consultées ? Où sont-elles stockées ? Sont-elles bien répliquées ? Comment sont-elles protégées... Toutes ces informations vont permettre d'évaluer le niveau d'exposition des données et le niveau de risque.

Une des nouveautés du règlement est de prévoir pour chaque traitement sensible une étude d'impact qui peut représenter entre 5 à 10 jours d'intervention par analyse, ce qui constitue une charge de travail considérable.

Etat des lieux

Vous devez réalisé un audit afin d'établir une cartographie de vos données structurées dans des bases de données de vos applications dans votre entreprise ou dans le cloud et de celles non structurées éparpillées dans des fichiers comme Excel stockées dans des dossiers utilisateurs ou dans des box comme OneDrive, Google Drive, Dropbox, ...

Pour chaque base de données, vous devez définir :

- Le type de contenu;
- L'utilisateur concerné ;
- Le risque lié à l'utilisateur ;
- Le risque lié à la ressource ;
- Le lieux de stockage;
- L'historisation de la donnée.

L'état des lieux, qui constitue un prérequis de la mise en conformité, doit être suivi d'un rapport de restitution préconisant des axes d'amélioration.

QUE DIT LA LOI ?

L'article 35 impose une analyse des risques avant traitement pour ceux susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Ce que l'on entend par traitement à risque concerne les collectes de données massives (Big Data), de données dites sensibles ou liées à des condamnations pénales, les traitements ayant pour finalité le profilage ou la surveillance systématique à grande échelle d'une zone accessible au public (vidéosurveillance).

Afin de préciser les traitements concernés, les autorités locales seront chargées d'en diffuser la liste.

Outre la description du traitement et l'évaluation de la nécessité et de la proportionnalité du traitement, l'étude doit prévoir:

- l'évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées ainsi que les garanties pour remédier aux risques en apportant la preuve du respect du règlement.

Si cette étude n'est pas systématique, elle suppose tout de même une « pré-étude d'impact » pour l'envisager ounon.

GÉRER

ETAPE 3 - Classifier et définir un cycle de vie

Les données non structurées sont souvent gérées directement par les employés eux-mêmes. Selon le Data Hoarding Report de Veritas, 43% ne savent pas quels fichiers doivent être conservés ou supprimés et 28 % pensent que la suppression de ces fichiers prend trop de temps.

Concernant les données à caractère personnel, les traitements doivent être licites, proportionnels et sécurisés tout au long de leur cycle de vie. Aussi des règles de gestion, de conservation et de rétention doivent être non seulement définies mais aussi appliquées de manière automatisée.

QUE DIT LA LOI ?

L'article 25 intègre deux nouveaux principes sur la gestion des données : la protection dès la conception et la protection par défaut.

Le « privacy by design » ou protection dès la conception consiste à prendre en compte toutes les questions relatives aux données personnelles dès la création d'un produit, d'un service ou d'une offre : la quantité de données, leurs natures, la limitation de durée de conservation, etc. Le responsable de traitement devra également anticiper la possibilité d'informer les personnes concernées, et prévoir des procédures, en cas de demande d'accès ou d'effacement de leurs données.

Le « privacy by default » ou protection par défaut consiste à prendre les mesures pour garantir que, par défaut :

- Seules les données nécessaires et pertinentes à la finalité du traitement sont traitées.
- Seules les personnes qui en ont raisonnablement besoin y ont accès.
- Les outils (tels que les CRM) doivent permettre l'effacement total des données si nécessaire.

SÉCURISER

ETAPE 4 - Sécuriser les données

Le règlement conforte les points « cyber sécurité » déjà soulignés dans la loi Informatique et Libertés en explicitant certaines recommandations telles que la pseudonymisation, l'anonymisation ou encore la cryptographie des données. Or, selon le Data Hoarding Report, 44% des données personnelles seraient non chiffrées et selon l'enquête Deloitte Enjeux Cyber 2016, seulement 7% des organisations françaises considèreraient la cyber sécurité comme un enjeu prioritaire. La vraie nouveauté dans le règlement réside dans la nécessité de pouvoir prouver de manière documentée ce qui a été fait pour sécuriser ces données et ce qui est prévu pour atténuer les risques en cas de compromission.

Définition de politiques de gestion

En fin d'audit, vous devrez délivrer un document de restitution intégrant :

- l'identification des données critiques avec leur niveau de protection et une analyse d'impact business (BIA) ;
- la classification des données ;
- la définition de règles de gestion du cycle de vie de la donnée associées à la classification (temps de conservation, stockage, sauvegarde, rétention...) ;
- la définition de politiques d'accès ;
- un plan d'actions à mener pour mieux gérer et sécuriser les données en concertation avec la direction générale, le juridique et le SI.

Cyber Sécurité

Vous devez mettre en place plus qu'un simple antivirus, mais un système de protection :

- Avant qu'il n'atteigne le système :
  - Sécurité du Web, Réputation des téléchargements, Contrôle du Web / Blocage des catégories d'URL, Contrôle des applications, Pare-feu client, Prévention des exploits du navigateur
- Avant qu'il ne s'exécute sur le système
  - Analyse comportementale en runtime / HIPS, Détection du trafic malveillant (MTD), CryptoGuard, Anti-ransomware
- Investigation et suppression
  - Suppression automatique des malwares, Synchronized Security Heartbeat, Analyse détaillée des attaques (Root Cause Analysis)

PRA

En cas de sinistre ou d'indisponibilité de votre site, vous devez prévoir un plan de reprise d'activité :

- Réplication de vos serveurs physiques ou virtuelles
- Sauvegarde avec rétention et archivage
- Ces deux points doivent être externalisés sur un deuxième site.

Pour définir le délai de réplication, de rétention et d'archivage, vous devez définir le RTO ou Recovery Time Objective qui désigne la durée maximale d'interruption admissible et le RPO ou Recovery Point Objective, qui désigne la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne.

QUE DIT LA LOI ?

L'article 32 explicite ce que le responsable du traitement et le sous-traitant peuvent mettre en œuvre comme mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté au risque :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Les articles 33 et 34 imposent au responsable de traitement de notifier à l'autorité locale la compromission de données personnelles dans les 72 heures qui suivent la détection. Le sous-traitant doit lui aussi pouvoir remonter cette information au responsable de traitement. Dans cette notification doit apparaitre la description la plus précise possible de la nature de la violation, de l'impact estimé et des mesures prévues pour atténuer ou éradiquer le risque. Si ce dernier s'avère toujours réel et/ou que l'autorité locale l'exige, le responsable de traitement devra notifier celui-ci à la personne concernée dans les meilleurs délais.

RECHERCHER

ETAPE 5 - Répondre aux requêtes des personnes physiques sur leurs données personnelles.

L'extension des droits aux personnes physiques suppose d'anticiper les demandes dès la conception d'un traitement, en prévoyant techniquement qu'il sera possible de retrouver toutes les données de la personne concernée, et de pouvoir effectuer des actions sur ces dernières (déplacer, supprimer, limiter).

Autour de ces droits, les obligations du responsable s'allongent :délai plus court pour répondre, liste d'informations à donner... d'où l'importance de se munir d'outils permettant une réactivité de réponse.

QUE DIT LA LOI ?

Les articles 15/16/17/18/20 consacrent les droits existants des personnes physiques sur leurs données personnelles : droit d'accès et demande de copie, droit de rectification. Et le règlement en crée de nouveaux : droit à la portabilité ainsi que le droit à l'oubli, c'est-à-dire à la suppression de ses données, et droit à la limitation de traitement lorsqu'il n'y a pas de raisons légitimes à son maintien... Ces demandes doivent être prises en compte dans le registre des traitements et surtout communiquées aux sous-traitants, ainsi qu'aux partenaires qui doivent également être en mesure de tracer les données.

RÉPONDRE

ETAPE 6 - Répondre aux demandes de la CNIL et fournir les preuves

Si besoin, le DPO (ou la personne chargée de la gestion des données personnelles) devra être en mesure de faciliter le travail d'enquête de la CNIL. En complément de la documentation produite sur les traitements, les emails, devenus la norme pour les communications internes et externes d'entreprise, sont souvent les seules preuves attestant d'échanges avec des partenaires, sous-traitants... Il est donc capital de rester propriétaire de ces derniers, même si la messagerie est basée dans le cloud, et surtout de pouvoir effectuer des recherches pertinentes et exhaustives.

Conformité : Recherche des données à caractère personnel

Le DPO doit à tout moment pouvoir fournir grâce à la tenue d'un registre des traitements (non exhaustif) :

- La description des données à caractère personnel.
- La pertinence de chaque donnée et de son traitement relatif.
- La liste des emplacements de stockage des données internes et externes à l'entreprise.
- La méthodologie qui permet d'accéder aux emplacements de stockage.
- La liste des sous-traitants gérant des données sous la responsabilité de l'entreprise.
- La liste des procédures et traitements relatives aux données à caractère personnel.
- La consignation et l'actualisation des consentements.

Litige : investigation étendue aux messageries et applications cloud

Qu'il s'agisse de retrouver des données personnelles ou des preuves présentes dans des emails, vous devez posséder un archivage des données et des mails avec possibilité de recherche globale.

Par exemple :

- Dans le cas CRM, le DPO doit pouvoir disposer du mot de passe général permettant d'accéder à toutes les informations, mails, mailing et traitement relatifs aux données à caractère personnel,
- Dans le cas d'un serveur de mails, le DPO doit pouvoir disposer du mot de passe général permettant de faire une recherche du type eDiscovery sur toutes les boites mails de l'entreprise.

Si des données à caractère personnel sont stockées dans des fichiers plats de type Excel, ces derniers devront être stockés sur un serveur dont le IDPO a un droit d'accès l'autorisant à faire une recherche sur tous les fichiers plats. Si certains sont protégés par mot de passe, ces derniers devront être notifiés dans le registre. Par contre des boites mails stockées dans des fichiers plats type .pst d'Outlook ne pourront pas faire l'objet de recherche globale.

QUE DIT LA LOI ?

L'article 58 rappelle les pouvoirs d'enquête dont dispose l'autorité locale, notamment ceux:

- d'ordonner au responsable du traitement et au sous-traitant de lui communiquer toute information dont elle a besoin pour l'accomplissement de sesmissions ;
- mener des enquêtes sous la forme d'audits sur la protection des données ;
- obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'accomplissement de ses missions.

RÉSUMÉ

- Le RGPD recouvre de multiples facettes, impliquant de nombreux acteurs tant en interne qu'en externe d'une organisation. Mais par la nature même de son sujet, (les données) l'angle technique représente un des chantiers les plus importants.
- Pour cela, **UNEETI**, entend vous accompagner pour vous mettre sur la voie de la conformité technique et vous propose son serveur 100% RGPD.
- Le règlement vise avant toute chose à inciter les entreprises à s'améliorer en continu,

Adopter cette démarche, c'est déjà être sur la bonne voie.

SOLUTION

Choisissez L'une
des offres Uneeti
100% RGPD
qui vous convient.

Pour plus d'informations
cliquez ICI

PC CLOUD
a partir de
69,90€/MOIS

Site : www.uneeti.com
Email : contact@uneeti.com
Tel : 01 69 52 84 93