Christophe Nouhau – DPO

« Règlement Général sur la Protection des Données (RGPD) »

RGPD

MEDEF - Premier réseau d'entrepreneurs de France

7bis Rue du Général Cerez, 87000 Limoges

Tél : 05.55.12.15.01

https://www.medeflimousin.fr/fr/

OBJECTIFS DE CET ATELIER MEDEF

- La réglementation (la loi) sur la protection des données personnelles

- Qu'est ce qu'implique cette loi dans ma structure (société, association, collectivité, autres…).

- D'accord, mais on fait quoi maintenant et comment ? (pragmatisme et priorisation)

MEDEF
LIMOUSIN

RGPD

RGPD : Historique et Rappels

Comprendre les nouveaux droits des personnes (la loi) – RGPD c'est quoi ?

CNIL : Loi n°78-17 du 6 janvier 78 relative à l'informatique, aux fichiers et aux libertés

RGPD : Nouveaux droits pour les PC : 25 mai 2018

Le RGPD (Règlement Général sur la Protection des Données) :

ou (GDPR) *General Data Protection Regulation* en anglais.
C'est le texte de référence européen en matière de protection des données personnelles qui vise à protéger le droit à la vie privée

La réforme de la protection des données poursuit trois objectifs :

1.Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;

2.Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;

3.Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

Comprendre les nouveaux droits des personnes (la loi) – Qui est concerné ?

Tous les professionnels :

- Ceux de l'internet bien sûr
- Ceux du secteur marchand
- Ceux du secteur public
- Ceux du secteur associatif

Tout en respectant le droit des états membres

Le RGPD s'applique quand :

- Une organisation traite des données personnelles
- Un résident de l'UE est directement visé par un traitement de données

Responsabilité de la structure « responsable de traitements » ET de ses sous-traitants

Données sensibles
C’est quoi ?

Données sensibles :

Information concernant l’origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l’appartenance syndicale, **la santé** ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu’avec le consentement **explicite** des personnes ou :

- Nécessaires à l’exécution des obligations en droit du travail et social
- Nécessaires à la sauvegarde des intérêts vitaux de la personne
- Traitées pour la gestion des membres d’un organisme à but non lucratif
- Manifestement rendues publiques par la PC

Quelques exceptions : constatation, exercice ou défense d’un droit en justice / motifs d’intérêt public (IP) importants / fins médicales / santé publique…

« Traitement à grande échelle » C’est quoi ?

Grande échelle :

Les traitements à grande échelle sont des traitements "qui visent à traiter un volume considérable de données à caractère personnel, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé, pour les droits et libertés des personnes concernées, en particulier lorsque, du fait de ces opérations, il est plus difficile pour ces personnes d'exercer leurs droits.".

NON	OUI
Traitement, par un médecin exerçant à titre individuel, des données de ses patients.	Traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités.

Obligations qui incombent aux organismes

6 Principes :

- *Licéité, Loyauté, transparence*
- *Limitation des finalités*
- *Minimisation des données*
- *Exactitude des données*
- *Limitation de la conservation*
- *Intégrité et confidentialité*

➔ *Le* responsable du traitement est en mesure de **démontrer** le respect de ces principes

➔ *Grande échelle = DPD + PIA (analyse d'impact)*

DPO
Data Protection Officer

pia analyse d'impact sur la protection des données privacy impact assessment

Les droits de la PC :

- *Droit d'accès*
- *Droit de rectification*
- *Droit à l'effacement (« oubli »)*
- *Limitation du traitement*
- *Droit d'opposition*
- *Droit à la portabilité*
- *DIA (décision Individuelle Automatisée / hors données médicales dans certaines conditions)*

➔ *La PC (personne concernée) doit être informée*

Risques en cas de non-conformité

Le règlement RGPD prévoit deux niveaux de sanction, pour les entreprises, en cas de non-respect :

- Des amendes administratives pourront s'appliquer pour un montant allant de 10 à 20 000 000 €
- ou bien 2 à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent.

L'hôpital de Barreiro a écopé d'une amende de 400 000 euros en raison de sa politique d'accès aux bases de données des patients.

La CNIL avait prévenu dès avril 2018. Le 21 janvier 2019, elle passe à l'acte. Sanction de 50 millions d'euros à Google.

Comprendre ce que cela implique en termes d'obligations

Mise en conformité RGPD

Il n'y a (pour l'instant) pas de « tampon » RGPD conforme…

Un paradoxe, car nous devons pouvoir démontrer notre démarche de mise en conformité et le respect de la loi.

LE REGISTRE EN PRATIQUE

La CNIL nous propose plusieurs moyens pour faire un registre… Il existe des logiciels spécialisés comme power GDPR (et bien d'autres).

registre-traitement Societe-Exemple.rtf
registre-traitement Societe-Exemple.xlsx

Vous pouvez créer votre propre modèle s'il répond aux prérogatives des réponses attendues par la loi.

Remarque : Attention aussi aux entreprises qui vous certifient qu'avec un outil de RGPD électronique, une GED ou coffre-fort électronique vos allez être certifiés RGPD !

LE REGISTRE EN PRATIQUE

L'article 30 du RGPD prévoit des obligations spécifiques pour le registre du responsable de traitement de données personnelles et pour le registre du sous-traitant. Si votre organisme agit à la fois en tant que sous-traitant et responsable de traitement, votre registre doit donc clairement distinguer les deux catégories d'activités.

En pratique, dans cette hypothèse, la CNIL vous recommande de tenir 2 registres :

- Un pour les traitements de données personnelles dont vous êtes vous-même responsable
- Un autre pour les traitements que vous opérez, en tant que sous-traitant, pour le compte de vos clients

Pensez aussi à

Informez les personnes concernées :
Si vous avez un site avec une « fiche contact » servez vous en pour permettre à la personne concernée d'échanger avec vous.
Mettez à jour **vos mentions légales (**https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228**)**
Mettez à jour **vos politiques de confidentialité**
Pensez à mettre à jour votre **charte informatique** (très pratique pour informer les salariés)
Préparez des **courriers de réponses** aux différentes sollicitations (notamment clients) et **faire attention aux arnaques !!!**

Ayez un process de **déclaration des violations de données.**

Priorisez les actions

Documentez (preuves)

ARNAQUES

Logiciels qui vont vous certifier !

Les escroqueries liées aux personnes qui vous demandent de modifier, supprimer, récupérer leurs informations personnelles – Exigez un justificatif d'identité

Les « clients » qui « profitent » du RGPD pour vous proposer des modifications de contrat pour répondre au RGPD.

6. [redacted] est responsable et accepte d'indemniser, de garder indemnisé, de garantir la responsabilité et, à la demande d'[redacted], de défendre [redacted] et ses administrateurs, employés, actionnaires et agents de tout dommage, responsabilité, dépense, réclamation, amende, ainsi que les pertes de tout type, y compris sans limiter les honoraires d'avocat raisonnables, résultant ou liées à tout ou partie du manquement du Service de santé (ou de ses employés ou sous-traitants) au respect de la vie privée et à la protection des données obligations en vertu du présent Contrat, y compris en cas de violation des données à caractère personnel.

ARNAQUES

Institution Européenne de la règlementation générale à la protection des données

Pas d'adresse de l'émetteur

CONTROLE RGPD

000003031 - DD87.0014

PROXIMIT
24 AVENUE DU PRESIDENT WILSON
87700 AIXE SUR VIENNE

Seule la CNIL est habilitée à contrôler.

Vos Références

Bulletin d'information du 22/03/2019
Région : Nouvelle-Aquitaine
Décret N° 2018-687 du 01 aout 2018
Numéro d'identifiant : RG-135012003031
Date limite de déclaration : 05/04/2019

REMARQUE : Des sociétés spécialisées (Proximit entre autres) proposent des services à leurs clients pour les accompagner juridiquement et techniquement mais ce ne sont pas des organismes de contrôle

Objet : Mise en conformité RGPD

Tél : 09 74 59 [redacted]
E-mail : contact@rgpd-registre.online

Madame, Monsieur,

La date du 25 Mai 2018 pour attester de la mise aux normes à la protection des données personnelles au sein de votre établissement (R.G.P.D) a été dépassée.

Nous vous rappelons qu'à compter de cette date, les entreprises qui n'auront pas régularisé leur situation quant au nouveau règlement RGPD 2016/679 sur la protection des données, quelle que soit leur activité ou taille, sont passibles de sanctions pénales et financières pouvant s'élever jusqu'à 4% du Chiffre d'Affaire annuel de la société.

Pour information, le propriétaire ou l'exploitant d'un établissement traitant des données personnelles (Il peut donc s'agir du nom, prénom, de l'adresse physique ou d'une adresse e-mail mais aussi du numéro de sécurité sociale...) qui ne répond pas aux exigences de la législation sur le RGPD définies par la directive (UE) 2016/680 en date du 25 mai 2018, doit élaborer obligatoirement un rapport et une mise en place des protections des données avec documents justificatifs à l'appui en cas de contrôle.

Vous êtes invités à vous mettre en conformité sans délai.

Un service de traitement RGPD dédié à cette circonstance est disponible :

- Par téléphone : 09 74 59 [redacted]
- Du lundi au jeudi de 9h00 à 18h00 sans interruption et le vendredi de 9h à 16h00.

Sylvain Blanchet
Gestionnaire RGPD

Un numéro (surement surtaxé) et ensuite une démarche abusive commerciale !!!

RAPPEL DE LA LOI

Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions pénales
(Chapitre VIII, article 83, alinéa 5)
Les violations des dispositions suivantes font l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000 000 € ou 4 % du chiffre d'affaire annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Règlement Général de Protection des Données 2016/679 (RGPD) – sanctions civiles
(Chapitre VIII, article 79 alinéa 1)
Sans préjudice de tout recours administratif ou extra judiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectuées en violation du présent règlement. Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. (Modifié par Loi n°2004-801 du 6 août 2004)

Le RGPD c’est simple

Si vous collectez des données, **informez la PC**

Donnez-lui les moyens de **savoir et d’intervenir**

Donnez-vous les moyens de **lui répondre** et de **répondre à la loi**

Accompagner vos sous-traitants (instructions)

N’en faites pas trop – **registre** / **analyse des risques** / **priorités** / **documentation**

proximit
IT services

MEDEF
LIMOUSIN

AUDIT, CONSEILS TECHNIQUES ET JURIDIQUES - RGPD

INFOGÉRANCE

SERVICES HÉBERGÉS

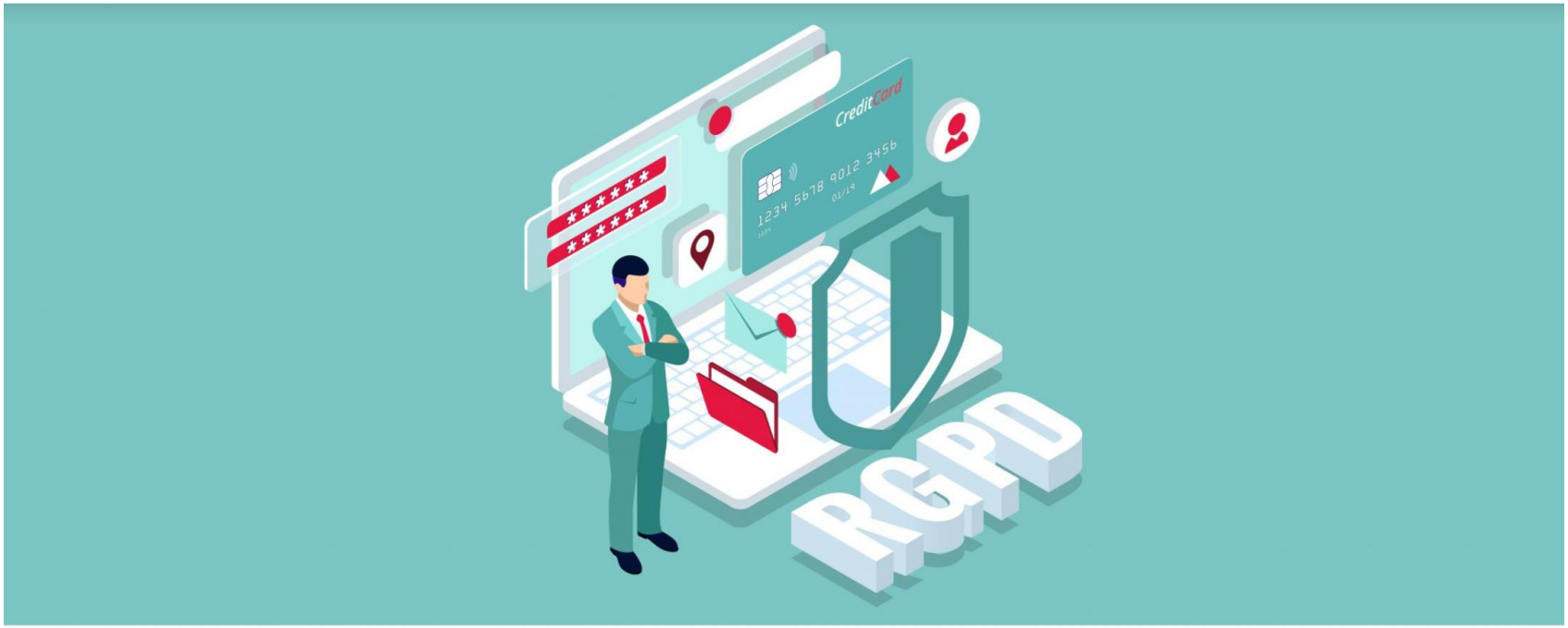
SÉCURITÉ DES SYSTÈMES D'INFORMATIONS

proximit
IT services

MEDEF
LIMOUSIN

proximit IT services notre métier, vous permettre de vous consacrer au vôtre

Accueil | Expertises | Produits & solutions | Actualités | Clients



← Retour

ACCUEIL / PRODUITS & SOLUTIONS / ACCOMPAGNEMENT RGPD

ACCOMPAGNEMENT RGPD

UN ACCOMPAGNEMENT SIMPLE, ADAPTÉ, MINIMISANT LA SOLLICITATION DE VOS ÉQUIPES, ET CONFORME AUX ATTENTES DE LA CNIL

R G P D

MERCI

Christophe NOUHAU
Directeur IT services - DPO
email : christophe.nouhau@proximit.fr
[fixe] +33 (0)5 87 02 01 00
[mob] +33 (0)6 45 71 69 49
24 avenue du Président Wilson - 87700 Aixe sur Vienne
www.proximit.fr

https://www.proximit-itservices.fr/