

Quels sont les impacts du RGPD dans notre business ?

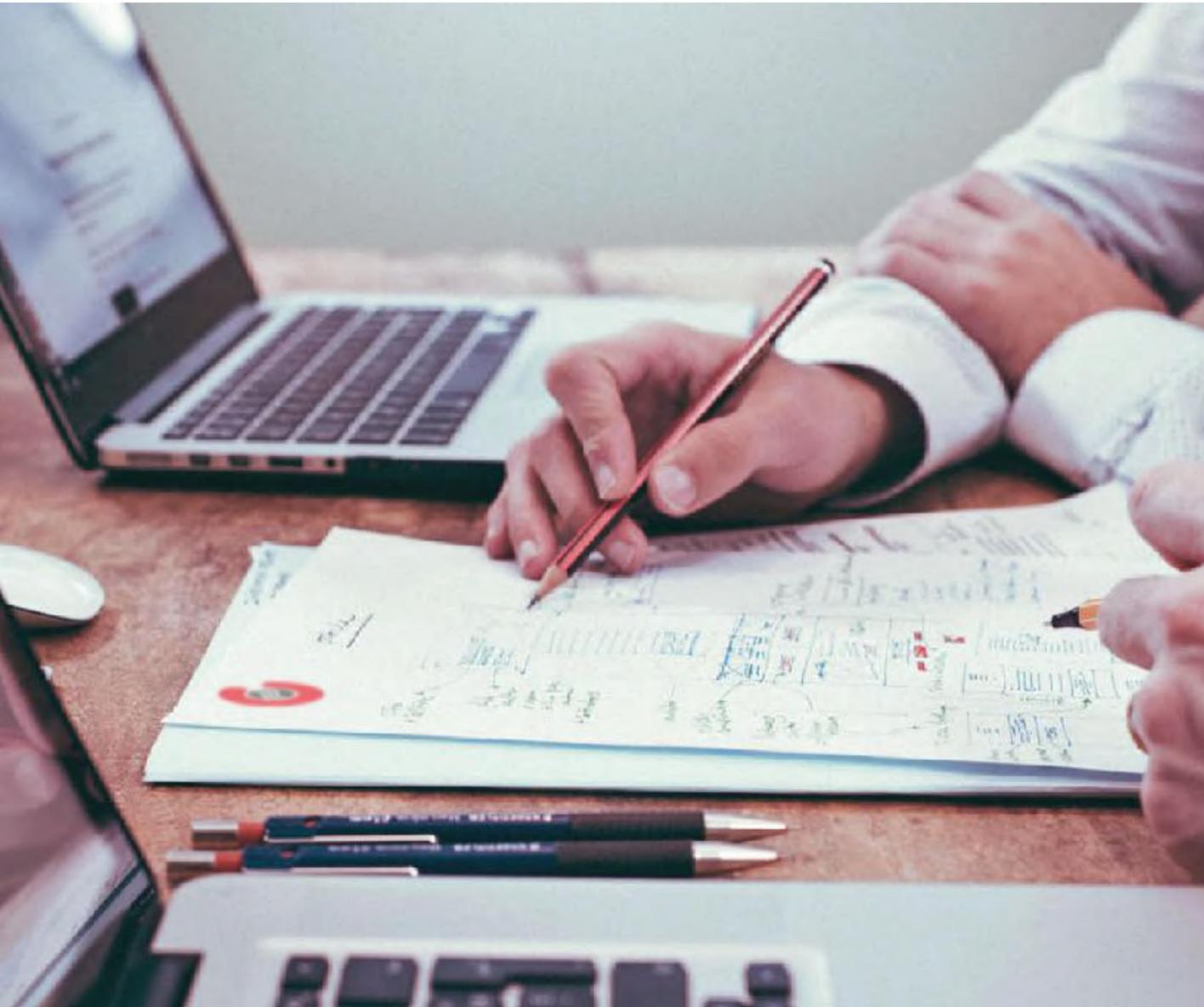
Alain Lacroix

Consultant et Directeur Associé



ALRIX
CONSULTING

ALRIX CONSULTING



Présent en Suisse et en France, Alrix Consulting est un cabinet indépendant de consultants experts dans le conseil en gestion d'infrastructures informatiques et technologies digitales

NOTRE MISSION



Mission :

- Accompagnement des entreprises dans l'organisation et la gestion de leur **Systeme d'Information (SI)**



Rôles :

- Consultants ponctuels
- Responsables informatiques à temps partiel pour les PME

A tablet computer is shown at an angle, displaying the European Union flag (a blue field with twelve yellow stars in a circle). A silver padlock is placed on the screen, symbolizing security and data protection. The background behind the tablet is a stylized map of Europe in blue and white. The text 'RGPD' is overlaid in the center in a large, white, sans-serif font.

RGPD

RGPD - QU'EST-CE C'EST ?

Règlement (UE) 2016/679 du Parlement européen et
du Conseil du 27 avril 2016



RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

GDPR en anglais (General Data Protection Regulation)

Entrée en vigueur le 25 mai 2018 !!

RGPD - QU'EST-CE C'EST ?

Règlement européen relatif à la protection des personnes physiques de l'union européenne à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

conformité
RGPD

Règlement Général de Protection des Données

RGPD S'APPLIQUE...

Le règlement s'applique dès le moment où une organisation, quelle qu'elle soit, **européenne ou non**, traite des **données personnelles** d'un résident européen.

Une donnée personnelle est :

"Toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement".

Et cela concerne les données papiers et numériques !!

Règlement Général de Protection des Données

RGPD - A SAVOIR...

A savoir que **la loi suisse sur la protection des données (LPD)** est actuellement en cours de révision de manière à s'aligner sur le règlement européen.

Règlement Général de Protection des Données

RGPD - L'OBJECTIF...

L'objectif est de donner aux résidents de l'union européenne plus de visibilité et de contrôle sur leurs données, à savoir....

- Quelles sont les données collectées ?
- Dans quel but ?
- Comment, combien de temps et où seront-elles stockées ?
- Comment informer les personnes concernées ?
- Comment les données seront-elles protégées ?
- Qui en aura accès ? A qui seront-elles transférées ?
- Comment les personnes pourront accéder, modifier ou supprimer leurs données ?

Règlement Général de Protection des Données

RGPD CONSISTE EN...

Pour être en conformité avec le RGPD, que faut-il faire ?

- **Désigner un responsable** du traitement des données (chef d'orchestre de la conformité), obligatoire dans certains cas.
- **Cartographier** vos traitements de données (catégories, flux, acteurs, traitement)
- **Gérer les risques** - Etude d'impact (PIA) dans le cas de données sensibles.
- **Actions de mise en conformité** (mentions, consentement, type de données, sous-traitants...)
- **Documenter** le tout afin de pouvoir démontrer que le traitement de données personnelles est conforme au règlement

Règlement Général de Protection des Données

RGPD - NOS DEVOIRS

Nous avons donc « **un devoir et l'obligation de rendre compte** »
(en anglais "**Accountability**")

Prouver par une documentation écrite, en cas de plainte ou de contrôle, sa **conformité au RGPD** et que l'on assure une protection des données en continu.

Important !!

Il est impératif d'**informer** les autorités et les personnes concernées (dans les 72 heures) **si leurs données personnelles ont été piratées** dans votre base.

Sous peine de sanctions importantes !

Règlement Général de Protection des Données

LE REGISTRE DES TRAITEMENTS

Certains organismes doivent également tenir un “registre des traitements”

- Toute entreprise ou administration qui emploie plus de **250 personnes.**

ou

- Si ce traitement porte sur des **données sensibles** ou sont susceptibles de présenter un grand risque pour les droits et libertés individuelles.

Règlement Général de Protection des Données

DONNÉES SENSIBLES

Qu'est-ce qu'une donnée sensible ?

- Origine raciale ou ethnique
- Opinion politique, philosophique, religieuse ou une appartenance syndicale
- Santé et orientation sexuelle
- Génétique et Biométrique
- Infractions ou condamnations pénales
- Régime alimentaire

Règlement Général de Protection des Données

LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

Dans le cadre du règlement, il vous faudra également désigner un délégué à la protection des données (appelé également DPO)....

- Si vous êtes un **organisme public**
- Si votre activité de base vous amène à réaliser un **suivi régulier** et systématique des personnes **ou** à traiter à **grande échelle des données** dites « **sensibles** »

Toutefois, dans tous les cas il est fortement recommandé de désigner une personne, disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen.

RGPD - INCIDENCE DANS LE MARKETING

A partir du **25 mai**, pour toute action marketing (emailing, formulaires de capture web, profilage...), un consentement...

...libre, spécifique, éclairé et univoque

sera obligatoire !

Règlement Général de Protection des Données

RGPD - INCIDENCE DANS LE MARKETING

En résumé l'utilisateur doit pouvoir :

- Savoir précisément comment ses données vont être utilisées
- Pouvoir consulter les politiques de confidentialité et Conditions Générales
- Possibilité de se désinscrire à tout moment ou modifier ses informations

Et le fournisseurs doit s'engager à :

- Recueillir le consentement de la personne
- Conserver la preuve du consentement
- Informer la personne concernée de ses droits
- Sécuriser le transfert des données personnelles

Règlement Général de Protection des Données

RGPD - MENTIONS DES COLLECTES

Quelques exemples de formulaires de capture sur les sites web

Règlement Général de Protection des Données

RGPD - MENTIONS DES COLLECTES

INSCRIVEZ-VOUS À NOTRE NEWSLETTER

Votre adresse mail

Valider

En renseignant votre adresse email, vous acceptez de recevoir chaque semaine nos derniers articles de blog par courrier électronique et vous prenez connaissance de notre [Politique de confidentialité](#).

Vous pouvez vous désinscrire à tout moment à l'aide des liens de désinscription ou en nous contactant à l'adresse xxx@company.com

 **CONFORME**

Formulaire conforme car 1 objectif

Règlement Général de Protection des Données

RGPD - MENTIONS DES COLLECTES

INSCRIVEZ-VOUS À NOTRE NEWSLETTER

Votre adresse mail

Valider

En renseignant votre adresse email, vous acceptez de recevoir chaque semaine **nos derniers articles de blog ainsi que des publicités de nos partenaires** et vous prenez connaissance de notre [Politique de confidentialité](#).

Vous pouvez vous désinscrire à tout moment à l'aide des liens de désinscription ou en nous contactant à l'adresse xxx@company.com



NON CONFORME

Formulaire non conforme car 2 objectifs

INSCRIVEZ-VOUS À NOTRE NEWSLETTER

Votre adresse mail

Valider

- Vous acceptez de recevoir nos derniers articles de blog par email
- Vous acceptez de recevoir des publicités de nos partenaires

Vous affirmé avoir pris connaissance de notre [Politique de confidentialité](#). Vous pouvez vous désinscrire à tout moment à l'aide des liens de désinscription ou en nous contactant à l'adresse xxx@company.com



CONFORME

cases à cocher nécessaires

RGPD - MENTIONS DES COLLECTES

VEUILLEZ RENSEIGNER VOS INFORMATIONS

Votre adresse mail

Valider

Vous acceptez de vous inscrire à notre newsletter



NON CONFORME

Pas de cases pré-cochées

VEUILLEZ RENSEIGNER VOS INFORMATIONS

Votre adresse mail

Valider

Cochez cette case pour refuser de recevoir des promotions par email



NON CONFORME

Ni de case pour refuser de recevoir

RGPD - A RETENIR

Ce qu'il faut retenir !

- Le consentement de l'internaute doit être demandé clairement ;
- Il doit être informé de l'usage (ou des usages) que vous allez faire de ses données ;
- En cas d'usages multiples, il doit pouvoir choisir entre chacun d'entre eux ;
- L'opt-in ne doit pas être passif, d'où la fin des cases pré-cochées et des formulations trompeuses.

... et conserver la preuve du consentement !

Le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

Date	Informations du lead
18/01/2018 17:24	Prénom : Eric Nom : Bouleau Email : eric.bouleau@monentreprise.com Téléphone : 0105252829 Consentement : Exploitation des données dans le cadre de la demande de contact et de la relation commerciale qui peut en découler

RGPD - E-MARKETING

Il vous reste maintenant à reprendre l'ensemble de vos listes de contacts et vérifier si elles sont conformes, sinon de les mettre en conformité avec des outils qui vous permettent de gérer cette contrainte, notamment des logiciels de emailing et/ou auto-répondeur...



SG Autorépondeur
Votre marketing prend vie

digitaleo



mailpro

 **sendinblue**



Sarbacane Desktop
l' emailing tout simplement



 **AWeber**


MailChimp

 **mailjet**TM
Real-time emailing

infomaniak

RGPD - QUAND ?

Et cela d'ici au **25 mai prochain...** ou à défaut pouvoir démontrer que vous êtes dans la démarche de mise en conformité.



conformité
RGPD

Règlement Général de Protection des Données

RGPD - S'Y PRÉPARER...

Règlement européen sur la protection des données personnelles se préparer en 6 étapes

En mai 2018, le règlement européen sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

- Désigner** un pilote
- Cartographier** vos traitements de données personnelles
- Prioriser** les actions
- Gérer** les risques
- Organiser** les processus internes
- Documenter** la conformité

CNIL
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

www.cnil.fr

La Confédération suisse
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence (PFPDT)

Page d'accueil | Plan du site | Contact | DE | FR | IT | EN

Actualités | Protection des données | Principe de la transparence | Documentation | La PFPDT

Page d'accueil > Documentation > Bases légales > Protection des données - International > Le règlement général de l'UE sur la protection des données

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence PFPDT

État : mars 2018

Le RGPD et ses conséquences sur la Suisse¹

Sommaire

Introduction	2
Le règlement général sur la protection des données (RGPD)	2
Champ d'application matériel (art. 2 RGPD)	2
Champ d'application territorial (art. 3 RGPD)	3
Droits des personnes concernées	4
Applicabilité aux entreprises suisses (art. 3 et 27 RGPD)	6
Obligations des entreprises concernées par le Règlement	8
Obligation de désigner un représentant des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union (art. 27 RGPD)	10
Sanctions prévues	11
À qui s'adresser	11

¹ Avertissement : le présent texte fera l'objet d'ajouts et de modifications à la lumière de l'évaluation et de la réflexion aux niveaux national et européen. En effet, des clarifications sont en cours afin de connaître la position et l'interprétation des autorités de référence et de contrôle (G29, Commission européenne, autorités de contrôle des États membres de l'Union).

Page 8 sur 18

t général de l'UE sur la protection des données

RGPD

Lignes directrices du G29

Informations de la Commission européenne relatif au RGPD

"On en parle" du 26.02.2018

Interview de Jean-Philippe Waser

Le règlement européen sur la protection des données est entré en vigueur le 25 mai 2018 dans toute l'Union européenne. Le RGPD sera directement applicable à tous les États membres de l'Union européenne. Les nouvelles règles imposent plus de contrôle sur leurs données et visent à renforcer le rôle des autorités de protection des données en réduisant les répercussions directes sur un grand nombre d'entreprises, organismes publics et associations de données.

Conséquences sur la Suisse (PDF, 806 kB, 27.03.2018)

les autorités de protection des données

Préparé par la CNIL

pour accompagner les TPE et PME dans leur démarche de conformité au règlement européen sur la protection des données.

Préparé par la CNIL

NIL

PO auprès de la CNIL

entreprises, organismes publics et associations de données délégué à la protection des données (DPO), accueilli par la CNIL afin de faciliter et accompagner la conduite d'une démarche de protection des données.

www.edoeb.admin.ch

Nous restons à votre disposition pour tout ce qui concerne les conseils et l'accompagnement dans cette nouvelle réglementation.



Vous trouverez également des informations sur notre site web : alrix.ch rubrique services/RGPD

MERCI !

**Merci pour votre
attention !**