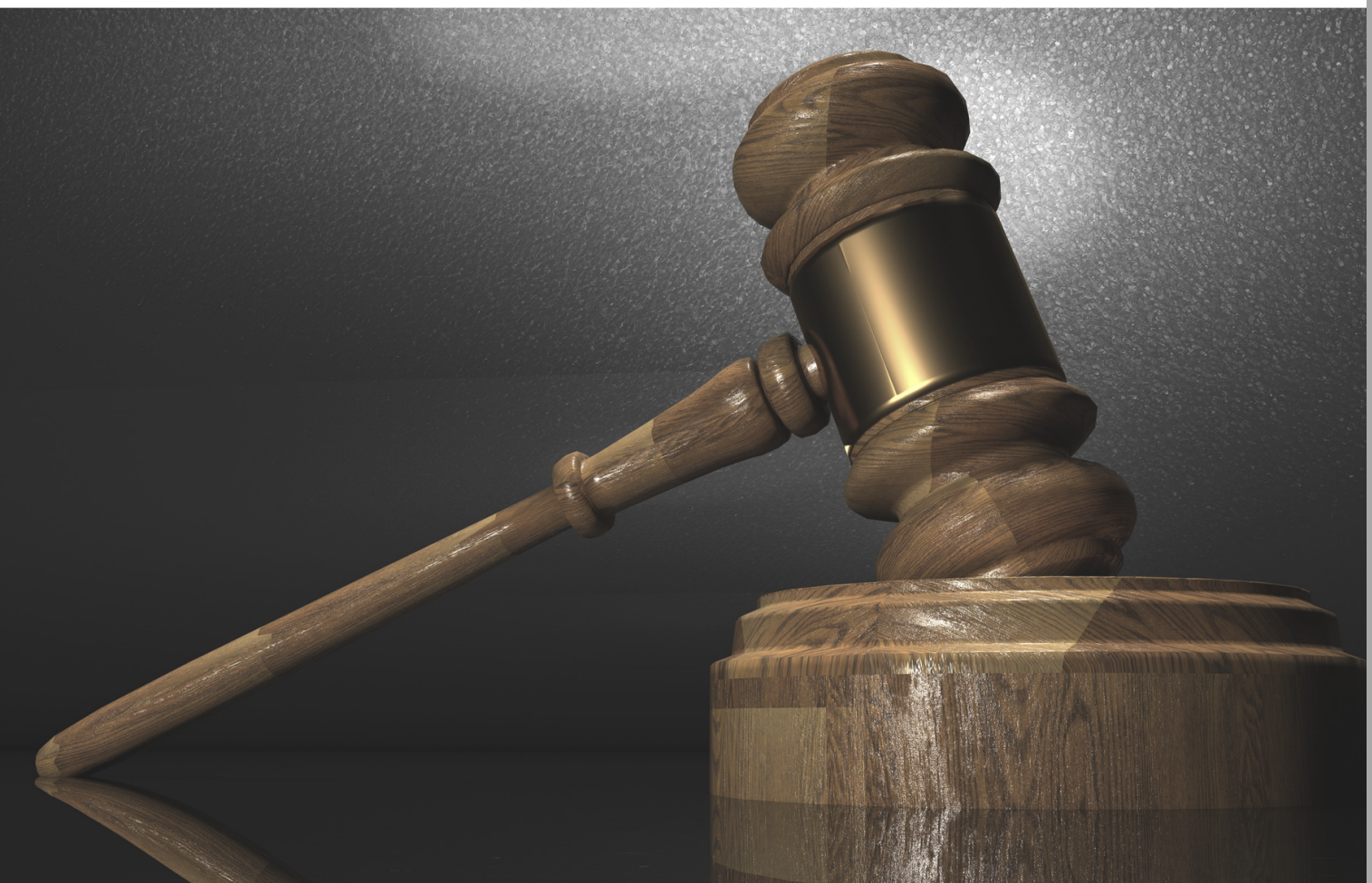
T. Devergranne

6 conseils pratiques pour limiter vos risques RGPD

Et aller à l'essentiel !



A propos de l'auteur

Docteur en droit et titulaire du Certificat d'Aptitude à la Profession d'Avocat, Thiébaut Devergranne a conseillé les services du Premier Ministre pendant la période de négociation du RGPD (2012-2015) en qualité d'expert national. Il est l'auteur de donneespersonnelles.fr le site le plus visite en France sur le RGPD après le site de la CNIL.

Comprendre les risques

La raison d'être du RGPD est de **protéger les droits et libertés des personnes au regard des risques liés au traitement de leurs données personnelles.**

En effet, l'informatisation crée par nature des risques pour les personnes :
- des données personnelles peuvent être piratées ;
- l'identité d'une personne peut être usurpée en ligne ;
- etc

Pour éviter ces atteintes, la règlementation créé une série de règles juridiques qui ont pour fonction d'assurer qu'un système informatique opère le traitement de données personnelles en toute confiance. Ces règles sont autant des règles relatives à la sécurité (15% du RGPD) que des règles juridique relatives au consentement, ou au transfert des données hors de l'UE.

Des sanctions réelles ?

Les sanctions ont été considérablement augmentées par rapport à la règlementation précédente. Une infraction au RGPD peut aujourd'hui être sanctionnée à hauteur de 4% du chiffre d'affaire global du groupe - ou 20 million d'euros (le plus haut des deux).

L'objectif de cette nouvelle réforme a été d'augmenter les sanctions car la règlementation ancienne ne sanctionnait pas assez efficacement.

Le RGPD a retiré à la CNIL une partie de son pouvoir d'appréciation sur les sanctions en lui imposant de prononcer des sanctions qui soient systématiquement "**dissuasives**" :

"*1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées (...) soient,* ***dans chaque cas, effectives, proportionnées et dissuasives***" (**article 83**)

Il est important néanmoins de comprendre que **le risque ne vient pas de la CNIL**. Au regard du niveau important de sanctions de nombreux acteurs vont se servir du règlement comme contre-pouvoir dans des conflits classiques (ex : salarié licencié, consommateur mécontent).

Il est donc essentiel de mettre son organisation en conformité.

Comment se mettre en conformité ?

Viser une conformité à 100% est hors de portée de la majorité des entreprises en raison de sa complexité. L'objectif d'une conformité est donc avant tout d'éliminer les principaux risques.

Ce guide pratique vous permettra d'avancer mais il est essentiel de se former pour maitriser entièrement le sujet. Une formation de deux jours suffit pour appréhender l'essentiel ses risques juridiques. **Si l'entreprise a plus de 50 salariés il est essentiel qu'une personne au moins suive une formation.**

Il existe beaucoup de formations, voici quelques témoignages de participants à la notre que vous pouvez retrouver ici : http://www.donneespersonnelles.fr/formation-gdpr

"*La formation nous a fait économiser énormément de temps et d'argent. J'ai énormément apprécié l'approche très analytique et très construite de la problématique RGPD complétant l'approche "terrain" du projet de mise en conformité de l'entreprise.* " - le DSI d'une grande entreprise dans le domaine de la sécurité.

"*Formation concrète et efficace, mettant en avant les points clés du règlement, et les pièges à éviter. On en ressort avec une approche très pragmatique et des process précis de mise en conformité. Le tout avec d'excellents échanges entre les participants, facilités par un animateur maîtrisant parfaitement son sujet*" - FX Vincent, IT Risk Leader, **AXA**

Conseil 1 : Utiliser des logiciels conformes

> Les éditeurs de logiciel mutualisent les coûts de conformité au RGPD

Une action simple de conformité - en particulier pour les petites entreprises - consiste à **s'assurer de n'utiliser que des logiciels qui sont conformes au RGPD**.

En général si un éditeur est vraiment conforme au règlement, vous trouverez de nombreuses communications sur son site Internet - de même qu'une déclaration claire et sans ambiguïté sur au fait que le logiciel est bien conforme (« nous sommes conforme au RGPD »).

Les coûts de conformité pour les éditeurs sont souvent très lourds, donc s'ils ont fait l'effort de vraiment se mettre en conformité, en général ils communiquent largement sur le sujet.

Les actions à mener sont :
- recenser l'ensemble des logiciels existants dans l'organisation ;
- rechercher sur le site de chaque éditeur s'ils sont conforme ;
- conserver cette trace (« preuve »).

Conseil 2 : Éviter de traiter des données sensibles

Le règlement a adopté une démarche pragmatique centrée autour des risques relatifs au traitement de certaines données, dites sensibles.

Celles-ci font l'objet de contraintes juridiques plus importantes que les autres en raison des risques qui leur sont associés. Voici la liste :
- *les données à caractère personnel qui* ***révèlent l'origine raciale ou ethnique***
- ***les opinions politiques, les convictions religieuses ou philosophiques***
- ***l'appartenance syndicale***
- ***les données génétiques, des données biométriques***
- ***des données concernant la santé***
- ***des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne***

Il existe 10 exceptions permettant d'opérer leur traitement mais de manière générale leur traitement va augmenter considérablement le niveau de risques.

Eviter leur traitement va donc considérablement faire baisser le niveau de risque juridique.

Conseil 3 : Minimiser les données collectées

> Minimiser les données personnelles collectées fait immédiate ment baisser son niveau de risque

Un des changements opérés par le règlement européen en pratique tient au fait que celui-ci impose de ne collecter que les données qui strictement nécessaires à l'organisation.

L'article 5 du règlement européen précise à ce titre que les données personnelles doivent être :

« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)»

Deux actions doivent donc être mis en oeuvre à ce titre :

- **purger l'ensemble des données qui ne sont pas strictement nécessaires au sein des applications informatiques existantes ;**
- s'assurer de limiter les données collectées à l'avenir.

Conseil 4 : Mettre en place le registre de conformité

Le règlement impose aux organisations de tracer l'ensemble des traitements de données personnelles mis en oeuvre afin de s'assurer que ceux-ci soient en conformité avec la loi.

Ce principe de responsabilité est indiqué à l'article 24 :
le responsable « *met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* ».

Or, pour cela, il faut non seulement tracer les traitements mis en oeuvre, mais également tracer le fait qu'ils sont bien conformes à l'ensemble des obligations imposées par le règlement.

Le plus simple est d'utiliser un logiciel de gestion du registre comme Legiscope (www.legiscope.com - qui dispose d'une version gratuite). Ce type de logiciel vous permettra en plus de gérer le registre, de vous guider au travers du processus de conformité et documenter vos traitements.

https://www.legiscope.com

Conseil 5 : Afficher les mentions RGPD

> Les mentions légales permettent de montrer que vous avez une fait attention à la protection des données

A chaque fois que vous collectez des données personnelles (ex : un email, un nom, un prénom), vous devez afficher des mentions légales RGPD.

Celles-ci permettent entre autre de montrer que vous avez géré le problème de la protection des données personnelles et que vous avez mené des actions à cet égard.

Les mentions à indiquer sont précisées par l'article 13 du RGPD, voici un court extrait :

"*a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement*
b) le cas échéant, les coordonnées du délégué à la protection des données;
c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement (...)"

Conseil 6 : Ne pas transférer des données personnelles hors de l'UE

Le RGPD est très strict sur le transfert de données personnelles hors de l'Union Européenne et **c'est un des facteurs qui va substantiellement augmenter les risques juridiques**.

A partir du moment ou une entreprise hors de l'UE la protection des données personnelle ne dispose plus systématiquement des garanties juridiques appropriées. En conséquence, le transfert dans un pays tiers fait courir des risques potentiellement importants aux personnes dont les données sont traitées.

Le plus simple est d'éviter tout traitement hors UE. Ce qui signifie souvent vérifier que l'entreprise n'utilise aucun logiciel - en particulier de logiciel SAAS (en ligne) - basé en dehors de l'UE.

Si l'entreprise utilise des solutions Cloud (ex : Amazon, Google), il faut alors systématiquement vérifier que l'hébergement des serveurs/données se fait au sein de l'UE (Irlande...).

Il existe un régime juridique qui permet d'opérer ces transferts, mais il est quasiment systématiquement nécessaire de disposer d'un avis juridique spécifique pour s'assurer de ne pas réaliser d'infraction au règlement.

Conclusion

Ces conseils peuvent paraître simple, mais cumulés ils vont limiter très substantiellement vos risques.