Introduction

À qui s'adresse ce livre ?

Dans le cadre de votre activité professionnelle, vous utilisez souvent des noms, e-mails ou numéros identifiant vos clients ou administrés ?

Tenez-vous un listing de vos adhérents dans un cadre associatif ?

Vous manipulez des données à caractère personnel sûrement sans le savoir, et/ou peut-être avez-vous entendu que vous devez respecter le règlement européen sur la protection des données (RGPD)[1].

Si tel est le cas, alors ce livre est fait pour vous !

Que vous soyez étudiant, exerciez une fonction d'opérationnel ou de chef d'entreprise, que vous soyez dans le secteur public ou dans le secteur privé, ce livre s'adresse à toute personne voulant comprendre le RGPD par une approche simple et pratique.

Mais il s'adresse avant tout à des opérationnels pour qui la réglementation est avant tout une source de tracas quotidiens et qui sont souvent démunis par manque d'informations sur le sujet.

Le livre, que vous tenez dans vos mains, constitue la seconde édition. La première édition est sortie en janvier 2022. Le monde a changé depuis, la COVID-19 et ses procédures diverses ne sont plus d'actualité. Les transferts de données vers les États-Unis ont désormais un cadre plus formel.

1. *Voir glossaire.*

L'IA, cette fameuse Intelligence Artificielle est sur toutes les lèvres et des expérimentations commencent à apparaître dans les organisations. La législation européenne évolue et avance à grands pas dans différents domaines liés au cyberespace.

Enfin, la responsabilité sociétale des entreprises est plus que jamais mise en avant et le RGPD est un outil qui se révèle complémentaire.

Cette seconde édition vise à éclairer le lecteur sur ces points tout en essayant de rester vulgarisateur sur un sujet qui ne devrait plus être une découverte dans les organisations.

Cette édition met également plus en avant des liens provenant d'autres autorités de protection nationales telles que l'APD (Belgique) et la CNPD (Grand-Duché de Luxembourg). Ces deux APD ont produit plusieurs documents, en langue française, qu'il est intéressant d'étudier par leur approche parfois différente de la CNIL.

Bien entendu, ces documents renvoient aussi vers des textes propres à leurs législations nationales. Le lecteur sera attentif à ce point et devra faire les correspondances vers ses propres législations.

Pourquoi un tel guide ?

J'ai toujours été intéressé par la protection des données et la protection des libertés individuelles. Je me suis penché sur le RGPD dès 2016, et lorsque je discute avec nombre de professionnels ou de personnes, notamment dans le domaine associatif, force est de constater que cette réglementation, pourtant fondamentale, est incomprise.

Trop complexe, trop lourde, combien d'affirmations faussées peut-on entendre…

Ce livre axe sur une synthèse, visuelle et pratique, en évitant le jargon juridique, de la réglementation du RGPD, dans le but d'amener le lecteur à se poser les bonnes questions sur ce qu'il faut faire, ce qu'il fait ou non au quotidien, et de lui donner les clés pour se mettre en conformité avec l'aide d'un professionnel.

Partie 1

VOUS AVEZ DIT RGPD ?

Scène de la vie quotidienne

UN LUNDI MATIN DANS UNE RÉUNION DE SUIVI DE PROJET MARKETING...

LA SOCIÉTÉ TRUC S'APPRÊTE À LANCER UNE NOUVELLE VERSION DE SON SITE INTERNET ET SOUHAITE PROFITER DE CE LANCEMENT POUR FAIRE DE LA COMMUNICATION AUTOUR DES PRODUITS...

Chapitre 1
Cinq mythes couramment entendus

Les mythes ont la vie dure… L'application du RGPD en mai 2018 s'est accompagnée de larges communications dans la presse, certaines maladroites, ce qui a conduit à des interprétations souvent erronées. Faisons le point sur certaines d'entre elles.

1 - Le RGPD fixe des durées de conservation de documents

Par son principe de proportionnalité, le RGPD impose que les données à caractère personnel ne soient conservées que pour des durées précises. Aucune donnée personnelle ne peut être conservée sans limite de durée, mais le RGPD ne fixe pas, dans son texte, de durée précise de conversation pour un type de document précis.

2 - Le RGPD, c'est juste l'affaire du DPO

Le délégué à la protection des données (DPO) est l'interface entre les organismes (entreprises, administrations, associations…) et les autorités de contrôle. Il s'assure aussi de la conformité au RGPD de son organisme et conseille les responsables de traitement. Le DPO n'est pas la seule personne impliquée dans la conformité au RGPD d'un organisme. Cette conformité est l'affaire de tous ses employés, à tous les niveaux.

3 - Pour échapper au RGPD : il suffit de mettre ses centres de données hors d'Europe

Ce serait évidemment trop simple ! Le RGPD s'impose à toute entité européenne. Mais aussi par effet d'extraterritorialité aux entités établies en dehors de l'Union qui ont à gérer des données personnelles de citoyens européens.

À noter : Le RGPD s'impose aussi aux particuliers s'ils ont à gérer des données à caractère personnel dans le cadre d'une activité professionnelle, extraprofessionnelle ou associative. Le RGPD ne s'impose pas, à ces mêmes personnes, si les fichiers sont utilisés dans un cadre strictement personnel. Par exemple, un carnet d'adresses.

4 - Le RGPD, c'est juste des grosses amendes

Certes, les amendes peuvent être colossales : 2 % du CA mondial ou 10 millions d'euros, 4 % du CA mondial ou 20 millions d'euros, selon les manquements constatés. Mais ce ne sont pas les seules sanctions possibles : une action de groupe est possible, une simple mise en demeure d'une autorité de contrôle peut avoir des conséquences en termes d'image si elle est rendue publique…

5 - Le consentement est obligatoire

Le consentement a une valeur particulière dans le RGPD mais n'est pas systématiquement requis ! C'est un des mythes les plus fréquents. Chaque traitement de données à caractère personnel est basé sur une des six bases légales reconnues. Le consentement qui est l'une de ces bases est requis pour certains types de traitements, pas pour tous. Ces bases sont décrites dans la partie 2, chapitre 1 *La licéité du traitement*.