

*Livre
BLanc*

RGDP

*Comment vous préparer aux
nouveauautés du RGPD ?*

*Préparez votre organisation pour le
RGPD :*

Explication en 10 étapes

Table des matières : RGPD

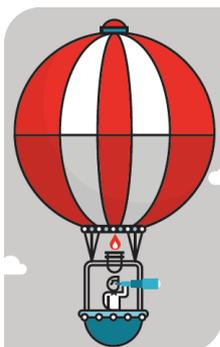
Qui est Creditsafe ?.....	3
---------------------------	---

Comment se préparer aux nouveautés du RGPD ?

Introduction	4
Qu'est-ce que le RGPD ?.....	5
Pourquoi le nouveau RGPD est-il nécessaire ?	5
À quelles organisations s'applique-t-il ?	6
Que sont les données personnelles ?.....	6
Responsable et sous-traitant de traitement des données	8
Quels sont les droits des personnes concernées ?.....	8
Quelles sont les principales et nouvelles obligations du RGPD ?	9
Protection des données by design (dans la conception des projets)	9
Analyses d'impact pour la protection des données	12
Obligation de documentation	12
Collecte des données dans un but particulier	12
Droit à l'oubli	12
Extraterritorialité	13
Notification des fuites de données ou des failles	13
Délégué à la protection des données	13
Amendes	13
Pour conclure ?	14
Étapes : explication en 10 étapes	15
Sources	19

Qui est Creditsafe ?

Après avoir révolutionné le monde de l'information commerciale et financière, nous visons maintenant la grandeur à l'échelle planétaire, en devenant les experts mondiaux de l'intelligence d'affaires, avec la passion et l'envie qui nous sont propres de fournir au monde entier des données de qualité supérieure. Partenaires des petites, moyennes et grandes entreprises, nous leur offrons une vision éclairée, soutenue par des sources d'informations de confiance et des plateformes intuitives.



GLOBAL

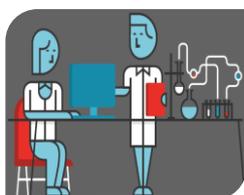
Avec 16 bureaux dans 13 pays et 1 500 collaborateurs dans le monde entier, nous pouvons nous positionner fièrement comme un solide et véritable fournisseur mondial d'information à destination des entreprises. Un réseau de 26 partenaires nous permet de renforcer, améliorer et associer l'offre de produits, les données et le contenu, pour que nos clients puissent constamment acquérir de nouvelles connaissances sur plus de 230 millions d'entreprises dans 170 pays.

BUSINESS

Nous avons changé la manière dont les entreprises utilisent les informations commerciales, et bien sûr, nous continuons à nourrir notre offre de services pour aider les entreprises à atteindre leurs objectifs. Notre gamme de produits propose un éventail de solutions professionnelles pour la gestion des risques de crédit, les procédures de conformité et de données marketing. Nous comprenons le marché et nous comprenons les entreprises.



INTELLIGENCE



La connaissance apporte le pouvoir, et c'est notre connaissance qui nous a fait croître. En utilisant une combinaison d'ensembles de données uniques, nous visons à créer et à fournir une multitude de produits aux entreprises de toutes tailles, leur donnant ainsi la perspicacité nécessaire pour prendre des décisions commerciales solides et éclairées.

EXPERTS

Avec près de 15 ans d'expérience dans le monde de l'entreprise et en moyenne 10 ans d'expérience parmi nos équipes de gestionnaires de comptes, notre objectif est de continuer à innover, à élargir nos connaissances et ainsi à devenir de véritables experts dans tous les domaines, sur tous les marchés.



Comment vous préparer aux nouveautés du RGPD ?

Introduction

La nouvelle version du règlement relatif à la protection des données est entrée en vigueur le 24 mai 2016. Néanmoins, les entreprises ont encore du temps pour se préparer à son application et à appliquer les adaptations nécessaires. À partir du 25 mai 2018, toutes les entreprises doivent être prêtes.

Bien sûr, la législation relative à la confidentialité des données n'est pas une nouveauté. Les différentes règles qu'elle comprend existent déjà depuis un certain temps. Les « nouvelles règles ou règles renouvelées » modifieront (légèrement) la structure actuelle, ce qui signifie qu'elles comprennent quelques nouveautés et que les règles actuelles ont été adaptées et améliorées. Tout cela pour la simple raison que nous vivons dans une société en mutation, où la numérisation, l'automatisation et les médias sociaux ont un impact de plus en plus important sur nos vies. Une étude récente de « The Economist » a montré que la ressource la plus précieuse au monde n'est plus le pétrole mais les données collectées.

Les autorités locales chargées de la confidentialité des données et le Groupe de Travail Européen « Article 29 » sur la protection des données apporteront l'aide nécessaire en collaboration avec les différents secteurs. Des directives et outils supplémentaires seront développés pour aider les entreprises à prendre les mesures préparatoires nécessaires.

Le RPD ou RGPD mettra particulièrement l'accent sur l'obligation de documentation qui pèse sur les responsables de traitement des données. Il est également important de savoir que les dispositions du RGPD ne sont pas aussi contraignantes pour toutes les entreprises. Ainsi, les nouvelles dispositions sont très importantes pour les entreprises opérant dans un secteur B2C. Et encore plus spécifiquement pour les entreprises qui font du profilage ou les organisations qui travaillent avec des données personnelles comme les données des mineurs.



Qu'est-ce que le RGPD ?

Nous expliquerons d'abord simplement ce que signifie le RGPD.

Le Règlement Général sur la Protection des Données (RGPD) est la législation européenne relative à la manière dont les gouvernements, les institutions, les entreprises et les organisations doivent gérer l'utilisation et le traitement des données personnelles et le respect de la vie privée des personnes concernées. Ces règles mises à jour qui ont été incorporées dans le RGPD doivent bien sûr être appliquées et respectées.



Les données personnelles signifient littéralement toutes les informations qui peuvent être reliées à l'identité d'une personne. Très variées, elles vont des données des patients d'un hôpital ou autre, aux données des enfants, en passant par les adresses IP.

Le RGPD vise précisément à éviter que l'utilisation et le traitement des données puisse nuire à la personne concernée.

Pourquoi est-il nécessaire ?

Le nouveau RGPD vise à renforcer les lois et règlements en vigueur et à pallier à leurs lacunes ou manquements. Il s'agit notamment des différentes règles de documentation des données, des procédures informatiques, de la notification de certaines « infractions » aux utilisateurs finaux et aux autorités, du renforcement des règles de minimisation des données et d'autres encore.

Le contrôle portera sur toutes les données à caractère personnel comme les noms, adresses, numéros de téléphone personnels, numéros de comptes bancaires, adresses e-mail et adresses IP.

En fait, ce contrôle est tout à fait logique lorsque l'on considère les données que nous venons de mentionner. Il est important qu'existe une réglementation claire et structurée qui contienne tant les nouvelles règles que les règles existantes qui ont été renforcées.

Autrement dit, l'objectif du « nouveau RGPD » consiste à légaliser les principes logiques de protection des données, et principalement la protection de la collecte de données personnelles, la minimisation de ces données et la suppression de certaines données qui ne sont pas nécessaires ou qui ne sont pas (ou plus) utilisées.



À quelles entreprises et organisations le RGPD s'applique-t-il ?

Le RGPD s'applique en fait à pratiquement toutes les entreprises et organisations. Effectivement, presque toutes les organisations traitent ou sont susceptibles de traiter différents types de données à caractère personnel pour leurs activités et services divers. Le RGPD met surtout l'accent sur deux rôles différents, à savoir les « responsables » et les « sous-traitants » du traitement des données (*ces rôles seront expliqués plus loin dans ce document*).



Quels types de données personnelles sont concernées par le RGPD (et lesquelles ne le sont pas ?)

En toute honnêteté, leur définition reste sujette à interprétation. En d'autres termes, un débat peut toujours naître par rapport à la définition des données personnelles qui entrent dans le cadre du RGPD et de celles qui y échappent.

Ce que nous pouvons dire avec certitude, c'est que les organisations doivent (vont) collecter beaucoup moins de données. Autrement dit, utiliser uniquement les données nécessaires aux fins de l'organisation.



Que sont les données personnelles ?

Les données personnelles sont des informations qui peuvent être reliées à une identité. Ce sont les données qui permettent d'identifier une personne comme les photos, les noms, les adresses et les numéros de sécurité sociale. Pour utiliser ces données, nous devons désormais obtenir le consentement de la personne concernée. Cela concerne tant les données personnelles qui seront collectées à partir de 2018 que les données déjà collectées.

Qu'en est-il des adresses IP, des noms d'utilisateur et autres données de ce type ?

Ces données ne sont pas épargnées non plus. Tout ce qui peut être relié au nom (d'une personne) relève de la législation RGPD actualisée. Les adresses IP par exemple peuvent être rapportées à une personne par une voie détournée.

Données anonymes

L'exception à la règle sont les données personnelles anonymisées. Parmi ces données, on trouve les fichiers cryptés, les données anonymes, les photos non identifiables, etc.

Conformité

Comme on peut le voir, de nombreuses organisations auront beaucoup de travail à abattre. Elles devront revoir la quantité de données dont elles disposent et la manière dont elles les utilisent.

Quelles données puis-je utiliser ?

Est-il permis d'utiliser certaines données et de les conserver ?

Mieux vaut prévenir que guérir !



Quelles données vais-je conserver et lesquelles peuvent ou doivent être effacées ?

Le principe de base : la différence entre le « responsable » et le « sous-traitant » de traitement des données



Le responsable :

Il est responsable du traitement des données. C'est une personne physique ou morale qui détermine le but du traitement des données personnelles et les moyens pour le faire. Il peut s'agir d'un annonceur qui a besoin de données pour la promotion de son produit ou service.



Le sous-traitant :

Le sous-traitant est celui qui traite effectivement les données personnelles. Il s'agit de toute personne ou entité qui traite les données pour le compte du responsable de traitement. Il peut s'agir de centres d'appels, de fournisseurs informatiques et d'autres entreprises de ce type.

Quels sont les droits des personnes concernées ?

Traitement :

Le traitement des données personnelles doit être clairement défini dans la politique de confidentialité. En outre, il doit exister une raison clairement définie pour laquelle les données doivent être traitées. Pour traiter leurs données personnelles, l'organisation doit demander l'autorisation préalable des personnes concernées, avec une raison fondée. Le tableau ci-dessous reprend les droits des personnes concernées :

Actuellement	Nouveaux droits
<ul style="list-style-type: none">- Droit d'être informé- Droit d'accéder aux données les concernant- Droit de corriger les données erronées (= rectification)- Droit de s'opposer au traitement de leurs propres données s'ils avancent des raisons sérieuses et justifiées. Pour ce qui est du marketing direct, dont les campagnes publicitaires, les personnes concernées peuvent s'opposer au traitement de leurs données sans aucune justification. <p>La seule exception à la règle : lorsque les données sont nécessaires pour conclure un contrat.</p>	<ul style="list-style-type: none">- Droit de ne pas être soumis à une décision automatisée dans le cadre du profilage, lorsque sont évalués certains aspects de la personnalité des personnes concernées et que ce traitement de leurs données peut avoir des conséquences importantes pour ces personnes.- Droit à l'oubli- Droit de limiter le traitement de leurs données- Droit à la portabilité des données, c'est-à-dire le droit de transmettre leurs données à un autre responsable de traitement sans que le responsable de traitement initial ne puisse y faire obstacle. Ce droit peut être exercé uniquement sur la base du consentement ou d'un contrat et si les données sont traitées de manière automatisée.

Les nouvelles et principales obligations du RGPD :

Comme vous pouvez l'imaginer, le RGPD comprend de nombreux textes, règlements et normes juridiques. Vous pouvez aussi trouver toutes les nouveautés dans la nouvelle version du RGPD de l'Union européenne. Voici les éléments principaux et les plus importants du « nouveau » RGPD.



Protection des données by Design - Protection des données by Default.

Les organisations doivent tenir compte de la protection des de la vie privée des utilisateurs lors de la conception et du développement d'un système d'information. Cette règle s'applique aussi aux organisations qui traitent des données personnelles. Tout organisme ou organisation doit développer des politiques internes en ce qui concerne la vie privée. Ces mesures doivent également se conformer à la protection des données par la conception des projets et à la protection des données par défaut (**Data Protection by Design et Data Protection by Default**).

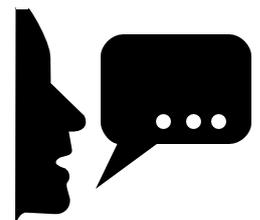
La protection des données par la conception est une approche qui vise à tenir compte à l'avance du respect de la vie privée en s'assurant que les garanties pour la protection des données soient intégrées dans les produits et services dès le développement initial des logiciels, des biens et des services. Autrement dit, cela signifie que les entreprises qui traitent les données doivent prendre très au sérieux le respect et la protection de la vie privée des personnes dès la première étape, celle de la définition du projet.

Quelles mesures techniques et organisationnelles sont possibles ?

La pseudonymisation fait partie d'une technique améliorant la protection la vie privée. Une technique qui vise à favoriser la protection de la confidentialité des données. Avec la pseudonymisation, toutes les données personnelles sont englobées dans un ensemble de données qui ne peuvent pas être directement reliées à une personne. En d'autres termes, les données sont cryptées ou codées. Avec cette technique, toutes les données personnelles permettant d'identifier directement une personne, comme les noms, dates de naissance, adresses, etc., sont supprimées et converties en un code déterminé. Par la suite, ces codes peuvent être reconvertis à l'aide du code ou de la clé de cryptage, de sorte qu'elles redeviennent « lisibles ». L'ensemble de données et la clé doivent être conservés séparément. La pseudonymisation réduit les risques pour le respect de la vie privée, mais aussi le risque pour les organisations qui travaillent avec ces données.



Procéder de manière transparente en ce qui concerne le traitement des données personnelles. Le responsable de traitement des données doit utiliser un langage clair et simple pour expliquer l'identité, la finalité du traitement des données, et toute information supplémentaire qui pourrait être fournie. Les personnes concernées doivent être informées des risques, règles, garanties et droits existants qui accompagnent ce processus.



Contrôlable :

Les personnes concernées doivent être en mesure d'exercer un contrôle sur le traitement de leurs données. Les responsables de traitement doivent être en mesure d'adapter, d'améliorer et même de changer certains dispositifs de sécurité.



Minimisation : Toutes les organisations qui traitent des données personnelles doivent prendre toutes les mesures nécessaires pour garantir que seules sont collectées les données réellement nécessaires aux fins de l'organisation. Ce principe est appelé « minimisation de la collecte de données ».



Le principe « au moins, au mieux »

La durée de conservation des données nécessaires, la minimisation de la collecte de données et leur subdivision permettront en fin de compte de renforcer la protection de la vie privée. Ces 3 éléments permettent par exemple de limiter les données susceptibles d'être volées par des pirates informatique. Si un hacker a accès à d'innombrables données en vue de les utiliser pour du « phishing », c'est que les organisations ont failli à assurer la sécurité de leurs clients. Avec la nouvelle réglementation, et notamment l'exigence d'une plus grande transparence dans le traitement des données, l'UE peut savoir plus facilement d'où provient une telle « fuite ».



Le Big Data et le respect de la vie privée peuvent aller de pair grâce au principe de privacy by design :



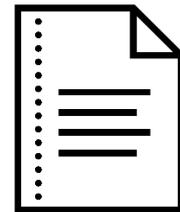


Les analyses d'impact sur la protection des données (AIPD)

En pratique, il s'agit d'évaluer les conséquences ou les effets du traitement des données vis-à-vis de la protection des données et du respect de la vie privée. Pour déterminer clairement où se situent les risques, le RGPD impose de les identifier au moyen d'une AIPD. Avant même de développer des produits ou des services, les entreprises doivent identifier, comprendre et résoudre les problèmes de confidentialité qui pourraient survenir. Ces risques doivent donc être analysés avant même le lancement d'une nouvelle activité.

Obligation de documentation

L'obligation de documentation est le changement le plus caractéristique. L'obligation de documentation implique que les organisations puissent démontrer quelles informations sont conservées et lesquelles sont traitées. D'autre part, elles doivent pouvoir expliquer d'où proviennent les données, où et comment elles sont conservées et comment elles sont protégées.



Collecte des données dans un but particulier

Comme déjà mentionné à plusieurs reprises dans le présent document, les données personnelles peuvent uniquement être traitées dans un but précis. Le traitement abusif des données personnelles n'est pas permis et des données précédemment collectées ne peuvent être utilisées pour la fourniture d'autres biens ou services sans l'autorisation de la personne concernée.

Le droit à l'effacement des données ou à l'oubli

Le citoyen européen concerné a le droit de demander à être oublié ou à faire effacer ses données. Le sous-traitant est contraint de le faire si les données ne sont plus nécessaires aux fins de l'entreprise pour laquelle elles ont été collectées ou si la personne concernée a retiré son autorisation pour leur utilisation. Si d'autres parties ont fait usage des données collectées par le sous-traitant, il doit également informer ces parties du fait que la personne concernée a demandé à être oublié ou à faire effacer ses données.

Il existe bien sûr quelques exceptions. Par exemple, l'organisation n'a aucune obligation si les données sont utilisées pour l'exercice du droit à la liberté d'expression et d'information et afin de respecter des obligations légales. Vous trouverez d'autres raisons dans le texte du nouveau règlement. Il est également important de savoir que sur la base du droit à l'oubli, les personnes concernées ont le droit de faire supprimer des archives de l'organisation des données incorrectes, obsolètes ou comportant un risque pour sa vie privée.





Extraterritorialité

Toute entreprise qui collecte des données sur le sol de l'UE est soumise au RGPD, même si elle n'a pas de « présence physique » dans l'UE.

Un exemple bien connu est Facebook. La société Facebook est basée aux États-Unis, mais elle collecte des données personnelles dans le monde entier, y compris l'Europe. Facebook doit donc se conformer à ces nouvelles règles. Le règlement aura ainsi un impact majeur sur les entreprises du monde entier qui sont actives dans l'e-commerce et le cloud computing.

Notification des failles ou violations

Une nouvelle règle obligeant les entreprises à notifier aux autorités compétentes toute violation du règlement relatif au traitement des données dans les 72 heures. Une remarque importante doit être soulevée par rapport à cette règle : elle s'applique uniquement dans le cas où cette faille représente une menace directe pour les droits et libertés des personnes concernées.



Le délégué à la protection des données

Un DPD est une personne, liée ou non à l'entreprise, et qui la conseille et l'informe en ce qui concerne le traitement des données personnelles. Le DPD vérifie également qu'il n'y a pas de fuites ou de failles dans la protection de la vie privée et doit pouvoir prouver que l'organisation concernée est conforme aux obligations du RGPD. Évidemment, un DPD ne peut être lui-même un sous-traitant ou une personne exerçant une fonction de direction au sein de l'organisation. Il doit aussi maîtriser une des langues nationales.

Amendes

Différentes amendes sont prévues qui peuvent être infligées en fonction de la gravité de l'infraction. L'UE souhaite imposer strictement le respect de la nouvelle législation. Ces amendes en sont un exemple car elles peuvent représenter une charge importante pour une organisation, jusqu'à 4 % du chiffre d'affaires total de l'ensemble de l'organisation.



Pour conclure ...

Concrètement, nous pouvons déduire de ces différentes règles nouvelles et actualisées que l'intention de l'Union européenne est de renforcer, améliorer et optimiser la protection de la vie privée de ces citoyens.

Il n'est pas difficile de comprendre pourquoi elle a cette intention.

La multiplication des procédures automatisées, le monde numérique, les méga-données, les médias sociaux mondiaux et ainsi de suite sont autant de belles innovations technologiques. Malheureusement, elles s'accompagnent de menaces concrètes comme les cyber-attaques, la fraude et le vol des données personnelles, etc. Il suffit de penser à la récente cyber-attaque du 12 mai 2017, qui a eu des conséquences graves dans le monde entier. Les hôpitaux ont été paralysés, les parkings automatiques ont offert malgré eux une journée « portes ouvertes » à tous, les entreprises n'ont pas pu fonctionner normalement...

Il est donc logique et évident que nos données personnelles doivent être mieux protégées. Comme déjà indiqué dans ce document, la ressource la plus précieuse au monde n'est plus le pétrole mais les données (personnelles) collectées (= une multitude de données).

L'Europe veut donc sensibiliser davantage les entreprises. Celles-ci doivent adopter des automatismes, être transparentes et pouvoir fournir toutes les preuves en ce qui concerne la protection des données qu'elles utilisent.

Les organisations doivent comprendre l'importance de la sensibilité des données personnelles.

Vous trouverez ci-après une feuille de route sur la manière de préparer votre organisation pour le RGPD. Vous souhaitez obtenir plus d'informations sur les méga-données, la protection des données ou Creditsafe ?

N'hésitez pas à nous contacter :

T: 02/481.88.60

E: info@creditsafe.be

Préparez votre organisation pour le

RGPD : explication en 10 étapes

1.

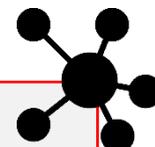
Sensibilisation



Tous les décideurs et chefs d'entreprise doivent être informés des changements annoncés. Ils doivent être en mesure d'estimer (évaluer) les implications du RGPD ou RPD pour la société. Ces évaluations déterminent les différents risques pouvant être présents. La mise en œuvre de l'évaluation peut mobiliser de nombreux processus, procédures, moyens et mises en application. Cela explique qu'une longue période de transition est laissée aux entreprises pour se préparer à temps à ces nouvelles règles.

2.

Cartographie du traitement des données



Cartographiez les traitements des données personnelles mis en œuvre au sein de l'organisation. Ce sont les données que vous utilisez et conservez. Vous devez être en mesure d'expliquer où et comment les données ont été collectées, et avec qui vous les partagez. Enfin, ces traitements des données doivent enfin être enregistrés et documentés. Vous devez garder à l'esprit le cadre juridique applicable à ces situations. Pour ce faire, vous devez identifier la base juridique régissant toute utilisation de données personnelles par votre entreprise.

Pour appliquer cette règle dans la pratique, il peut être indiqué d'organiser un audit pour l'ensemble de l'entreprise ou pour certains départements.

Un exemple pratique des raisons pour lesquelles la cartographie peut être importante :

Lorsque la « société A » transmet des données inexactes à la « société B », la « société B » doit être informée de ces données inexactes. Ainsi, la « société B » peut les corriger dans ses registres et dans sa documentation.

3.

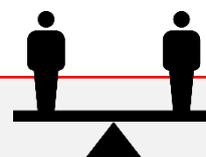
Communiquer



Dès l'instant où l'organisation traite des données personnelles, elle doit en informer les parties concernées et leur indiquer l'identité du sous-traitant et la manière dont il utilisera ces données. Habituellement, ces procédures sont consignées dans une déclaration de confidentialité. La première étape est donc d'évaluer votre déclaration de confidentialité existante. Sur la base de cette analyse, vous pouvez déterminer les éventuelles adaptations nécessaires. Ces adaptations doivent bien sûr être conformes à la nouvelle réglementation. Communiquez ensuite ce « nouveau » règlement relatif à la vie privée (par exemple sur votre site internet).

4.

Les droits des personnes concernées



Étudiez les procédures éventuellement existantes au sein de l'entreprise et sur lesquelles les personnes concernées peuvent s'appuyer. Concevez et appliquez une procédure de suppression des données personnelles à la demande des personnes concernées et une politique de transmission des données. Ces procédures ont aussi leur importance pour la communication des données à des tiers.

D'autre part, le consentement préalable au traitement des données est essentiel. Vous devez donc évaluer la manière dont vous demandez et obtenez le consentement des personnes concernées et dont vous les informez du but dans lequel vous collectez leurs données personnelles. Vous devez ensuite appliquer les ajustements nécessaires, si besoin.

DROITS DES PERSONNES CONCERNÉES:

- **Droit d'information et d'accès à leurs données personnelles**
- **Droit de rectification et d'effacement d'éventuelles données incorrectes.**
- **Droit d'opposition aux pratiques de marketing direct**
- **Droit d'opposition à la prise de décision automatisée et au profilage**
- **Droit à l'oubli**
- **Droit d'opposition au transfert des données**

5.

Je souhaite accéder à ...



Pour certains services, les personnes concernées souhaitent avoir accès à certaines données. Le traitement de ces demandes doit peut-être être mis à jour pour respecter la nouvelle réglementation. Réfléchissez à la manière dont vous traiterez ce type de demandes à l'avenir. La protection des noms d'utilisateur et des mots de passe est un bon exemple.

6.

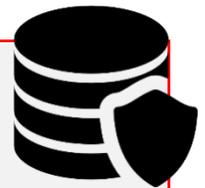
Fuites de données



Enquêtez sur les éventuels défauts des systèmes de traitement. Mettez en œuvre des procédures définies d'enquête et de rapport.

7.

Protection by design et AIPD



Il est important de vous familiariser avec ces deux concepts. Une fois que vous pouvez clairement différencier ces concepts, vous devez envisager la manière dont vous pouvez les appliquer dans le fonctionnement opérationnel de l'entreprise.

- **Protection des données lors de la conception ou data protection by design**
Comme déjà indiqué dans le document, vous devez vous assurer que les mesures de protection des données soient incorporées dans vos produits ou services dès leur développement initial ou étape préliminaire.
- **Analyses d'impact sur la protection des données ou Data Protection Impact Assessments**
En outre, comme déjà mentionné dans ce document, il est nécessaire d'effectuer une évaluation préliminaire des incidences sur la vie privée. En d'autres termes, vous devez être en mesure de prouver que pour toute nouvelle action de la société en matière de collecte, de traitement et de gestion des données personnelles, votre organisation a tenu compte du respect de la vie privée des personnes concernées. Les risques de violations doivent être identifiés et des mesures doivent être prises pour limiter autant que possible les atteintes à la vie privée.

8.

Activité internationale



Si la société est aussi active au niveau international, il est important d'établir quelle autorité de surveillance est compétente pour l'organisation.

9.

Contrats existants



Si vous travaillez avec des sous-traitants, il est important d'évaluer ces contrats afin d'apporter les changements éventuellement nécessaires.

10

Délégué à la protection des données



Désigner un délégué si nécessaire. Cette personne est appelée DPD (délégué à la protection des données). Cette personne est responsable du respect des règles relatives à la protection des données. Les critères qui doivent être pris en compte :

- **Cette personne doit maîtriser une des langues nationales**
- **Une personne doit être nommée pour chaque entité (= pays).**
- **Son titre et sa fonction doit être clairement indiqués**

Sources

Ce livre blanc a pu être constitué grâce à des sources précieuses dont voici les références :

- Creditsafe - Data Business Teams & Marketing Teams
 - Commission vie privée - Commission de la protection de la vie privée - Règlement général sur la protection des données - Rue de la Presse 35 | 1000 Bruxelles
 - Commission vie privée - Règlement général sur la protection des données et publications (<https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees-0>)
 - Commission de la vie privée - Publications du groupe de travail 29
 - Commission européenne - – Justice Rules of Law – Data Protection – Protection of personal data – RGPD(<http://ec.europa.eu/justice/data-protection/>)
 - Varonis – RGPD: A practical guide – EU RGPD LESSONS – www.varonis.com
 - STIMA | BDMA - Groupe de travail RGPD | Groupe de travail juridique - NOUVEAU RÈGLEMENT SUR LA PROTECTION DES DONNÉES - participation à plusieurs ateliers -
 - STIMA | BDMA - Groupe de travail RGPD | Groupe de travail juridique - NOUVEAU RÈGLEMENT SUR LA PROTECTION DES DONNÉES - Prise de position - (<https://www.stima.be/nieuws/gdrp-positioning>)
 - RGPD PORTAL EU - Les principaux éléments du règlement général relatif à la protection des données générale (RGPD) -(<http://www.euRGPD.org/>)
 - Smartbiz – article/post : De RGPD-wetgeving uitgelegd in vijf vragen (Le règlement RGPD expliqué en cinq questions) – Karen Gijsbrechts (09/08/2016) - (<http://www.smartbiz.be/achtergrond/167961/de-RGPD-wetgeving-uitgelegd-vijf-vragen/>)
 - Smartbiz – article/post : Checklist voor de RGPD : maak je bedrijf compliant in 13 stappen (Checklist pour le RGPD : 13 étapes pour la mise en conformité de votre entreprise) – Karen Gijsbrechts (26/09/2016) - (<http://www.smartbiz.be/achtergrond/168496/checklist-voor-de-RGPD-maak-je-bedrijf-compliant-13-stappen/>)
 - The Economist – Article : Fuel of the future: Data is giving rise to a new economy
 - LinkedIn – www.Linkedin.com – Éclairages et messages utiles
-

Creditsafe Belgium

Chaussée de Zellik 12

1082 Brussels

T: 02.481.88.60

E: info@creditsafe.be