GUIDE

PRATIQUE

1ère édition - 2018

RGPD – GUIDE PRATIQUE

La nouvelle législation européenne sur la confidentialité des données

Auteur : Viktor D'Huys, Group Joos

Co-auteur : Peter Witsenburg, Belgium Cloud & Cloud Makelaar

Table des matières

Avant-propos

« Ce n'est plus l'argent qui fait tourner le monde, ce sont les données. » J'ai récemment lu cette phrase écrite par un journaliste. Voilà qui en dit long... Les données ont une influence grandissante sur nos vies. D'une part, elles sont la matière première du moteur de la nouvelle économie numérique et, d'autre part, elles dirigent toujours plus nos vies via les nouvelles technologies.

Que les choses soient claires : c'est une bonne chose. Les appareils et applications intelligents améliorent notre vie personnelle et la vie en société. Des apps sur nos smartphones aux nouvelles technologies dans les villes intelligentes, les données nous aident à avancer. Qu'il s'agisse de faciliter la mobilité, d'améliorer la qualité de l'air ou d'offrir des soins de santé sur mesure, les applications sont infinies.

Au vu de cette foi dans l'efficacité des applications, les données à caractère personnel sont devenues le nouvel Eldorado. Elles sont très prisées par les développeurs, qui sont convaincus qu'elles offriront demain la réponse aux problèmes d'aujourd'hui. De plus en plus, nos faits et gestes sont enregistrés. Ces dernières années ont été marquées par une augmentation colossale de la numérisation, du stockage, du traitement, de la diffusion et de l'échange de quantités impressionnantes de données à caractère personnel.

Cela implique aussi inévitablement des risques en termes de respect de la vie privée des citoyens. Plus que jamais, la protection de la vie privée est un défi de taille. Elle nous place devant une question fondamentale : comment garantir, d'une part, que les citoyens gardent le contrôle sur leurs données personnelles et veiller, d'autre part, à ce que l'entrepreneur et l'économie numériques continuent à s'épanouir ?

La réponse de l'Europe à cette question est le Règlement Général sur la Protection des Données (ou « General Data Protection Regulation »). Elle reconnait que les intérêts des développeurs et des citoyens ne sont pas contradictoires mais largement concordants. Les citoyens se préoccupent du respect de leur vie privée, mais ils sont également en quête de nouvelles applications, souvent personnalisées, qui améliorent leur vie.
Les entreprises, quant à elles, cherchent des données pour développer leurs produits, mais elles prennent aussi conscience que, de plus en plus, le respect de la vie privée est un sujet sensible pour les clients.

La solution choisie est on ne peut plus claire : une meilleure protection et considération des données à caractère personnel sur un marché numérique européen unifié. Nous y sommes parvenus en harmonisant les 28 pratiques différentes dans l'Union européenne. Il reste aux entreprises à se conformer à une législation unique. Cette législation facilite l'échange des données à caractère personnel et stimule les applications numériques innovantes pour tous les habitants d'Europe.

Parallèlement, les responsables du traitement des données seront contraints de se servir de manière responsable des données personnelles de leurs clients neufs et existants. C'est en outre à l'Autorité de Protection des Données qu'il appartient de veiller au respect de la protection de la vie privée, en guidant et en coachant les entreprises afin qu'elles se conforment à la nouvelle législation. Les sanctions sont d'ailleurs utilisées en dernier recours, elles ne sont jamais un but en soi.

Tout cela mène à plus de considération pour nos données à caractère personnel. Le but de la stratégie numérique européenne n'est en effet pas que les entreprises utilisent nos précieuses données à caractère personnel avec une efficacité maximale. Il s'agit du moteur sous-jacent au marché numérique florissant dans lequel les limites du progrès technologique sont chaque jour repoussées un peu plus loin. Pour découvrir tout son potentiel, chaque entreprise doit analyser et optimiser son traitement des données.

La nouvelle législation réalise ainsi son double objectif. Elle prévoit les barrières nécessaires qui, même à l'ère numérique, protègent le droit fondamental au respect de la vie privée. Simultanément, elle permet aussi aux entreprises de se développer pleinement sur le marché numérique. Il convient toutefois de ne pas perdre de vue un acteur crucial : les organisations qui œuvrent pour informer les citoyens et les entreprises sur cette nouvelle législation. Et c'est exactement ce que font Group Joos et le CloudMakelaar avec ce livre. En tant que secrétaire d'état à la protection de la vie privée, je leur en suis très reconnaissant.

Bonne lecture !

Philippe De Backer

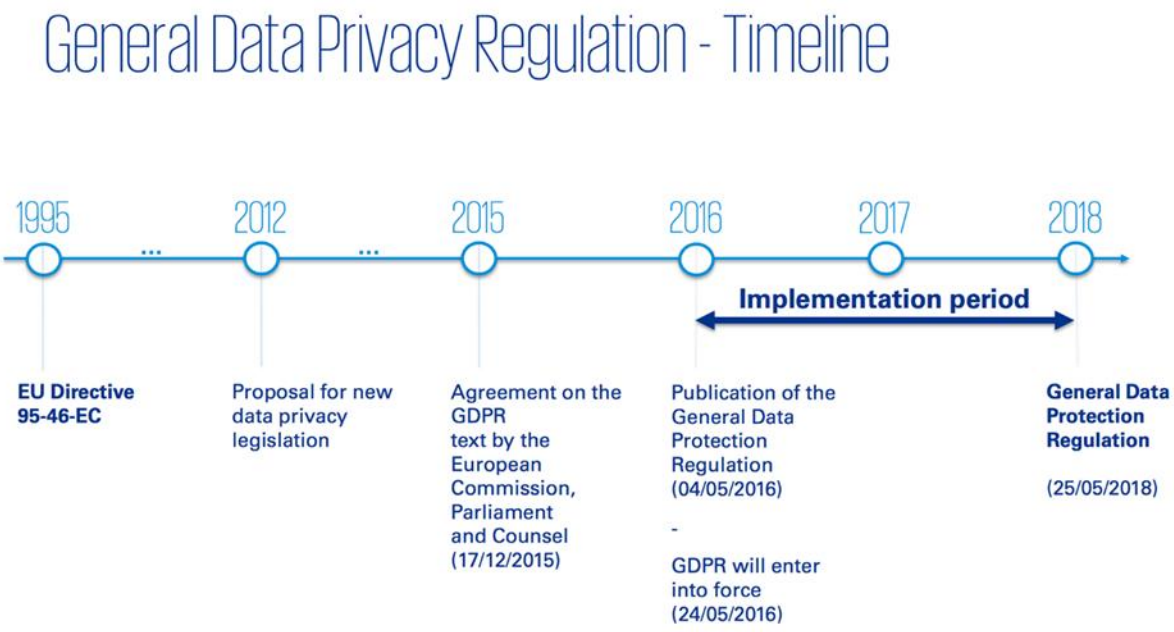
Secrétaire d'état belge à la Lutte contre la fraude sociale, à la Protection de la vie privée et à la Mer du Nord

RGPD : nouvelles règles, nouveaux défis

La nouvelle législation européenne relative à la confidentialité et au traitement des données personnelles, ou Règlement Général de Protection des Données (en anglais GDPR pour General Data Protection Regulation), est en vigueur depuis le 25 mai 2018. Le RGPD, officiellement Règlement (UE) 2017/679 du 27 avril 2016, est un règlement européen de 88 pages, 99 articles et 173 'Considérations'. Il s'applique à toute personne ou organisation qui, dans ou hors de l'UE, collecte ou traite des données personnelles de personnes vivant dans l'un des 28 pays membres ou de non-Européens qui s'y trouvent. Elle s'étend également aux pays non membres de l'UE, mais liés à l'Espace Economique Européen (EEE) (Liechtenstein, Norvège et Islande).

Avec le RGPD, l'Union Européenne souhaite trouver un nouvel équilibre entre la vie privée de ses citoyens et la collecte de données personnelles par les entreprises. Quiconque collecte, utilise ou traite des données à caractère personnel au nom de tiers doit connaître et appliquer les nouvelles règles.

Quelles sont les nouveautés du RGPD et, plus important encore, qu'est-ce que cela implique pour votre entreprise ? La législation relative à la protection de la vie privée n'est évidemment pas neuve. Depuis la ratification de la Déclaration Universelle des Droits de l'Homme en 1948, il existe une zone de tension entre le droit à la vie privée et l'utilisation des données que les entreprises collectent à notre sujet et utilisent.



Depuis l'avènement d'Internet et des big data, nous sommes en quête d'un nouvel équilibre. C'est dans ce contexte qu'arrive le RGPD.

Avec ces nouvelles règles, l'UE veut uniformiser la législation existante dans tout l'Espace Economique Européen (EEE). En outre, ces règles sont nettement plus strictes, ce qui a des conséquences majeures, en particulier pour les entreprises qui collectent et utilisent des données personnelles à grande échelle, ou dont c'est l'activité principale.

Tout d'abord, les données personnelles conservées par votre entreprise doivent être parfaitement protégées : cryptage des données sur le site web, sauvegarde des données dans un lieu bien sécurisé et transparence quant aux personnes qui, dans votre entreprise, ont le droit d'accéder aux données.

En outre, il faut veiller à une communication transparente sur les types de données conservées, sur ce qui en est fait et dans quel but. Les visiteurs de votre site doivent par exemple donner leur accord pour l'utilisation de leurs données dans un but préalablement communiqué. Ils doivent être informés des données que vous conservez, et de ce que vous en faites. De plus, chacun doit pouvoir consulter ses propres données, les modifier et éventuellement les faire supprimer. Vous l'aurez compris, satisfaire à de telles exigences demande un travail titanesque.

Enfin, en cas de fuite de données, vous devez disposer d'un plan d'urgence. Dans certains cas, vous devez également signaler cette fuite à l'Autorité de protection des données et aux personnes concernées. Ajoutez à cela que toutes les règles s'appliquent également à toutes les entreprises du processus, sous-traitants compris.

1. Définitions

1.1. Qu'entend-on par données personnelles ?

Impossible d'évoquer le RGPD sans définir les données personnelles[1]. Les données personnelles, ce sont « toutes les informations en relation avec des personnes physiques identifiées ou identifiables ». Comme pour toutes les définitions, chaque mot a son importance. Voyons cela dans le détail.

- Personnes physiques :
  Il s'agit des données de personnes individuelles encore en vie, et non de personnes morales. Les données d'entreprises qui sont votre client ou votre fournisseur ne relèvent donc pas de cette catégorie ; mais celles d'une personne de contact, par exemple, en relèvent bien.
- Personnes identifiées :
  Une personne peut par exemple être identifiée à l'aide de son nom, de son prénom, de son adresse et de sa date de naissance. Plus vous concentrez de données et plus le groupe de personnes est petit, plus il est facile de ramener l'information à une personne.
- Personnes identifiables :
  Certaines données ne peuvent être liées à une personne, mais comportent une clé leur permettant d'être combinées avec d'autres données. Si cela peut conduire à une identification, il s'agit aussi de données personnelles. Le RGPD stipule explicitement que cela reste ainsi tant que la combinaison peut être établie avec des efforts raisonnables.
- Toutes les informations :
  Cela indique clairement qu'il ne s'agit pas uniquement d'informations numériques dans des fichiers de données, mais aussi de données collectées sur papier, provenant d'images ou d'enregistrements sonores, etc. Certaines initiatives législatives antérieures se limitaient aux informations numériques, mais pour le RGPD, ce n'est explicitement pas le cas.
- Informations en relation avec une personne :
  Les informations qui en soi ne disent rien sur une personne peuvent être des données personnelles en raison du fait qu'elles sont liées à une personne. Les données de localisation en sont un bon exemple (l'endroit où se trouve une personne à un moment donné).

[1] Article 4.1 en 4.6 : Recital 15, 26-27 en 30-31

Il s'agit donc d'une très large gamme de données, allant de vos nom, adresse et date de naissance à votre dossier médical chez votre médecin traitant, en passant par votre état civil, les noms de votre conjoint et de vos enfants, mais aussi un extrait de votre casier judiciaire. Vos diplômes, vos connaissances linguistiques et votre expérience professionnelle sont des informations que vous mettez souvent à disposition de manière volontaire. Vous partagez vraisemblablement uniquement vos expériences privées avec votre famille et vos amis via les réseaux sociaux, en vous protégeant correctement du monde extérieur. Mais avez-vous déjà pensé à la liste de tous les articles que vous avez achetés au cours de l'année écoulée dans votre supermarché préféré ou à un aperçu de toutes les informations que vous avez recherchées sur Internet ? Il s'agit même de la localisation précise de votre GSM à un moment donné (et donc de votre localisation précise).

Conseil:

Afin de percevoir l'ampleur des informations auxquelles s'applique le RGPD, vous pouvez commencer par dresser un premier inventaire des données personnelles auxquelles vous êtes confronté(e) dans votre environnement professionnel, ou des données qui, selon vous, sont détenues à votre sujet par votre employeur ou des contacts professionnels dans d'autres entreprises. Ne poursuivez pas votre lecture avant d'avoir fait ce premier exercice.

Vous avez dressé votre liste ? Avez-vous pensé aux éléments suivants ?

- Un tiroir plein de cartes de visite, une feuille de calcul avec des coordonnées
- Le numéro de téléphone privé de collègues ou le numéro direct d'un consultant, transmis en toute confiance pour les urgences
- Les photos de la dernière fête du personnel
- Votre CV
- Les rapports d'entretiens d'évaluation ou de fonctionnement
- Les récapitulatifs des jours prestés, des absences et des jours de maladie
- Les images enregistrées par les caméras surveillant les accès aux bâtiments de l'entreprise
- Les journaux (logs) consignés par le département ICT : les heures auxquelles vous vous connectez au réseau ou à certaines applications, les sites web consultés…
- Vos échanges d'e-mails (leur contenu mais aussi leur nombre, les destinataires, etc.)
- Les questionnaires que vous complétez pour recevoir des informations d'un fournisseur, télécharger un livre blanc ou vous abonner à une newsletter (vos centres d'intérêt, vos loisirs, votre fonction dans l'entreprise, vos années d'expérience, etc.)

Cet aperçu est loin d'être complet, mais il montre clairement pourquoi il est nécessaire d'avoir une législation veillant à ce que tous ceux qui utilisent des données personnelles les gèrent de manière scrupuleuse et respectent certaines règles. D'autre part, il est inévitable et même nécessaire que les données personnelles puissent être utilisées, non seulement dans la sphère privée ou par l'administration, mais aussi par le monde des entreprises.

Le RGPD veut garantir un bon équilibre entre d'une part le droit au respect de la vie privée des individus et d'autre part la possibilité, pour les entreprises, d'utiliser la richesse des informations disponibles, même en dehors des frontières d'un pays.

Dans la suite de cette publication, vous comprendrez que dans le RGPD, tout est question d'équilibre entre ces deux points de vue. Savoir quelles sont les informations utilisées et à quelles fins est crucial pour les obligations qu'il convient de respecter. La section suivante examinera plus en détail les degrés de sensibilité des données personnelles et ce que l'on entend par « catégories spéciales ». Nous verrons également ce qu'il en est exactement du traitement des données, ainsi que des rôles et responsabilités définis à cet égard.

1.2. Catégories particulières de données à caractère personnel

Le RGPD repose essentiellement sur l'équilibre entre vos propres intentions liées à la collecte et à l'utilisation de données à caractère personnel et le droit de chaque individu à la protection de sa vie privée. La nature et la quantité des données traitées doivent toujours être proportionnées à l'objectif poursuivi.

Il y a de grandes différences dans l'ensemble des données à caractère personnel. Certaines sont publiques ou si largement diffusées et aisément accessibles que leur divulgation ne pose pratiquement pas de problème et ne peut pas véritablement être considérée comme une violation de la vie privée. D'autres sont à ce point confidentielles que le RGPD les classe dans des « catégories particulières », auxquelles s'appliquent des règles supplémentaires. Il est donc essentiel d'identifier immédiatement les données à caractère personnel appartenant à ces catégories[2].

C'est pourquoi elles sont explicitement énumérées dans le RGPD :

- Informations relatives à l'origine raciale ou ethnique,
- Données concernant les convictions religieuses ou philosophiques,
- Informations relatives aux opinions politiques ou à l'appartenance syndicale,
- Données concernant la vie sexuelle ou l'orientation sexuelle,
- Informations médicales,
- Données d'identification biométriques et ADN,
- Informations relatives à des infractions ou à des condamnations pénales.

Le principe général veut que de telles informations ne devraient être ni collectées, ni traitées. Si cela s'avère toutefois nécessaire, il conviendra de préciser clairement l'objectif et la base légale, conformément aux règles spécifiques prévues à cet effet. Des normes plus strictes s'appliquent en outre aux différents stades du processus de traitement : sécurisation de l'information, transfert de telles données en dehors de l'Europe (EEE) et, en particulier, gestion d'une éventuelle fuite de données. Nous y reviendrons à d'autres occasions dans cet ouvrage.

Au delà de ces catégories particulières, une distinction peut toujours être faite entre les données présentant un faible risque de violation de la vie privée et les informations plus sensibles. Des informations financières, par exemple, sont plus sensibles qu'une adresse. De même, le traitement de données concernant des enfants requiert toujours la plus grande prudence.

[2] Article 4.13-15; Article 9-10 : Recital 34-35 en 51-56

Personal Data Categories (Privacy Commission)	Personal Data Category?
A. Identificatiegegeven B. Financiële bijzonderheden C. Persoonlijke kenmerken D. Fysieke kenmerken E. Leefgewoonten F. Psychische gegevens (informatie over karakter en persoonlijkheid) G. Samenstelling van het gezin H. Vrijetijdsbesteding en interesses I. Lidmaatschappen K. Consumptiegewoonten L. Woningkenmerken N. Opleiding en vorming O. Beroep P. Rijksregisternummer / Identificatienummer van de sociale zekerheid V. Beeldopnamen W. Geluidsopnamen	"Regular" Personal Data
J. Gerechtelijke gegevens M. Gegevens betreffende de gezondheid Q. Raciale of etnische gegevens R. Gegevens over het seksuele leven S. Politieke opvattingen T. Lidmaatschap vakbond U. Filosofische of religieuze overtuigingen	Special Category

Si vous collectez et utilisez des données à caractère personnel, vous devez donc systématiquement évaluer leur réelle nécessité pour l'objectif visé, ainsi que le niveau de risque d'encourir une violation de la vie privée. Plus le nombre de personnes et la quantité de données les concernant sont importants, plus le risque est élevé. Une telle évaluation est l'essence d'une étude d'impact sur la vie privée (*data privacy impact assessment* - DPIA). Selon les circonstances, il peut s'agir d'un projet à part entière ou d'une simple évaluation (qui doit cependant être enregistrée).

Certaines mesures permettent également de rendre les données à caractère personnel moins sensibles.

- La meilleure solution est de travailler avec des données anonymes. Si les données ont été correctement anonymisées (c'est-à-dire qu'elles ne peuvent plus être reliées à des individus), elles ne revêtent plus un caractère personnel et ne sont plus soumises à le RGPD. Ce procédé est appliqué, dans la mesure du possible, à des données pour la recherche scientifique et s'avère également indiqué pour des traitements à grande échelle à des fins de marketing.
  L'une des méthodes utilisées consiste à grouper les données. Il doit alors s'agir d'un nombre suffisant de données, de sorte que les groupes ne soient jamais constitués de seulement quelques individus (50 est généralement considéré comme un minimum).

Vous devez être conscient que plus le nombre de données différentes collectées est important, plus le risque d'identification d'une personne par leur combinaison est élevé.

- Autre méthode très utilisée : la pseudonymisation[3]. Elle consiste à supprimer, dans un ensemble de données, tous les éléments permettant d'identifier une personne et à les remplacer par une clé anonyme. Le fichier de cryptage est sauvegardé séparément. De telles données sont toujours considérées comme présentant un caractère personnel car elles concernent une personne identifiable. Néanmoins, le risque d'impact pour la personne concernée est considérablement réduit. La pseudonymisation constitue donc une bonne mesure de sécurisation pour des données sensibles nécessitant, par exemple, un transfert.

Les définitions relatives aux données à caractère personnel et, parmi celles-ci, aux données sensibles ou appartenant à des catégories particulières, ne sont pas fondamentalement différentes dans le RGPD de celles visées par l'ancienne législation en matière de protection de la vie privée ; mais elles doivent bien entendu servir de base à toute considération sur la signification du règlement. Nous examinerons ci-après le traitement des données à caractère personnel et les différents rôles définis dans la loi. Il y a là des différences fondamentales entre le RGPD et l'ancienne réglementation.

[3] Article 4.5; Article 25 : Recital 78

1.3. Traitement des données et différents rôles

Pour évaluer l'impact du RGPD sur votre entreprise ou votre fonction, vous ne devez pas seulement savoir quelles données sont à caractère personnel, mais aussi ce que la loi entend exactement par traitement des données. Vous devez également bien comprendre les différents rôles impliqués dans le traitement des données à caractère personnel[4]. Le rôle que vous jouez détermine en effet dans une large mesure vos responsabilités et obligations.

Traitement des données

Vous devez considérer le traitement des données au sens large. La collecte de données de contact ou portant sur les centres d'intérêt, le comportement d'achat, les visites de sites web, etc. nous vient certes spontanément à l'esprit. Ces informations servent à des campagnes de vente ou de marketing.

Or, cela va bien au-delà. Toute activité ayant trait aux données de personnes constitue en fait une forme de traitement des données à laquelle s'applique le RGPD. Regarder ou consulter des données, conserver ou effacer des données, transporter des données,... sont autant d'exemples de ce que la loi entend par traitement des données.

Et puisque chacun devra bientôt dresser un inventaire des traitements de données qu'il effectue lui-même ou confie à des tiers, il convient d'interpréter la matière aussi largement que possible. Qu'une entreprise chargée de la gestion du personnel pour des tiers traite des données à caractère personnel, cela va de soi. Mais le prestataire qui vient collecter du vieux papier à la demande de votre entreprise procède également à un traitement des données, dès lors qu'il s'agit de documents personalisés. L'utilisation de données personnelles par des personnes privées[5] dans le cadre familial ne tombe toutefois pas sous le coup du RGPD ; le travail des tribunaux et des services d'ordre non plus, car il est soumis à une autre législation.

Les rôles

En ce qui concerne le traitement des données, la législation relative à la protection de la vie privée distingue différents rôles, dont les principaux sont le « Responsable du traitement » et le « Sous-traitant ». On utilise également souvent les termes anglais « data controller » et « data processor ».

[4] Article 2.1-2; Article 4.2
[5] Article 2.2c : Recital 18

Le **Responsable du traitement**[6] est celui qui prend l'initiative de (faire) collecter et tenir des données à caractère personnel, dans le but de les traiter d'une manière ou d'une autre. Le Responsable doit déterminer les finalités spécifiques du traitement des données et prouver que celui-ci repose sur une base légitime. Il doit examiner au préalable quelles données à caractère personnel sont nécessaires à cet effet. Pour la législation, il est essentiel de ne pas collecter et traiter de données au-delà de celles qui sont strictement nécessaires pour atteindre l'objectif visé. Le non-traitement de données constitue en effet le meilleur moyen de protéger la vie privée. Le Responsable garantit également la sécurité des données collectées. Il assure leur disponibilité et veille à ce que leur confidentialité et leur intégrité soient en tout temps préservées (autrement dit, qu'elles ne soient ni modifiées ni effacées à tort). Les données doivent par ailleurs être exclusivement utilisées aux fins pour lesquelles elles ont été collectées.

Le rôle du **Sous-traitant**[7] consiste, pour sa part, à traiter les données à caractère personnel mises à sa disposition par le Responsable, conformément aux instructions et à l'objectif de ce dernier. Le Responsable peut bien entendu remplir lui-même ce rôle. S'il fait toutefois appel à une tierce partie, celle-ci n'endosse que le rôle de sous-traitant. Il s'agit d'une distinction fondamentale qui sert de base aux obligations légales. À noter que, contrairement à l'ancienne loi sur la vie privée, le RGPD impose également explicitement des obligations au Sous-traitant.

[6] Article 4.7
[7] Article 4.8

Mais, dans les faits, on se rend bien compte que la répartition des tâches n'est pas toujours si simple. Il est ainsi parfaitement possible que les données à caractère personnel soient en fait collectées par un Sous-traitant. Un Responsable peut en effet confier à un Sous-traitant la tâche de collecter, enrichir et analyser des données à caractère personnel dans le cadre de sa mission. L'ensemble de ces tâches illustre ce que la loi entend par « traitement des données à caractère personnel ». Ce n'est pas parce que vous collectez des données que vous êtes automatiquement le Responsable ; mais, inversement, vous demeurez responsable en tant que donneur d'ordre, même si vous confiez la collecte des données à un sous-traitant.

À l'avenir, un contrat devra clairement indiquer quels sont les rôles du donneur d'ordre et du preneur d'ordre dans le traitement des données. Il convient donc d'y prêter l'attention nécessaire. La nouvelle loi part d'ailleurs du principe que le traitement des données est toujours encadré par une convention de sous-traitance fixant clairement les obligations respectives en termes de confidentialité des données. Dans le même temps, vous devez comprendre que vos responsabilités sont liées au rôle que vous jouez en réalité, quelles que soient les dispositions du contrat. Cela veut dire qu'en tant que sous-traitant, vous devez veiller à ne pas prendre de responsabilités ne relevant pas de votre rôle. La limite la plus importante et évidente à respecter consiste à ne jamais utiliser les données que le responsable vous confie à d'autres fins que celles fixées dans le cadre de votre mission.

Enfin, la loi détermine également un troisième rôle clair, celui de la **Personne concernée**[8] (ou « data subject » en anglais). La Personne concernée est la personne individuelle à laquelle se rapportent des données à caractère personnel spécifiques. C'est la Personne concernée qui est au premier chef protégé par la loi. Le RGPD octroie explicitement à la Personne concernée un certain nombre de droits sur ses données personnelles. Il s'agit d'un fondement du nouveau règlement. Tout d'abord, le RGPD exige la transparence à l'égard de la Personne concernée quant au traitement de ses données. Celle-ci a en outre droit à ce que l'on appelle généralement un usage loyal (« fair use ») de ses données. Sont concernés tant l'acquisition et le traitement légitimes des données que le soin apporté pour les tenir à jour, les protéger suffisamment et ne les utiliser que dans le but fixé. La Personne concernée a le droit d'être informée de tous ces aspects. Dernier point mais non des moindres, la Personne concernée peut disposer dans une large mesure de ses données individuelles (elle peut les demander, les faire corriger ou supprimer ou faire cesser leur traitement). Les droits et obligations incombant à chaque rôle seront expliqués ultérieurement en détail.

[8] Article 12

1.4. Le Data Protection Officer (DPO)

Il y a fort à parier que le Data Protection Officer[9] (DPO), ou Délégué à la Protection des Données en français, jouera un rôle important dans votre parcours RGPD. Cette section s'intéresse aux entreprises qui doivent se doter d'un DPO et au rôle de cette personne.

Le RGPD n'oblige pas chaque Responsable à désigner un DPO. Durant les discussions préparatoires à cette réglementation, il a semblé, pendant longtemps, que l'obligation s'appliquerait à toutes les sociétés de 250 travailleurs et plus. Toutefois, cette disposition n'a finalement pas été retenue. Désormais, l'obligation se fonde davantage sur la nature de l'entreprise. Si les activités d'une société présentent un risque réel de violations graves de la vie privée, que ce soit par la quantité des données traitées, leur nature ou la fréquence des traitements, celle-ci doit se doter d'un DPO chargé de veiller au respect de la législation. Un certain nombre de structures doivent désigner un DPO dans tous les cas : tous les organismes publics, toutes les sociétés dont l'activité principale consiste à assurer le traitement de catégories particulières de données à caractère personnel, ainsi que toutes les structures dont l'activité principale porte sur la collecte et le traitement de données à caractère personnel sur une base régulière, systématique et à grande échelle.

Même si ce n'est pas obligatoire légalement, il est conseillé d'attribuer explicitement le rôle de DPO à une personne. Vous disposerez ainsi immédiatement d'un éclaireur pour le parcours préparatoire. Le DPO veillera à ce qu'une culture de la protection des données règne au sein de votre société, à ce que la question de la confidentialité des données soit régulièrement à l'ordre du jour et à ce que votre entreprise soit prête à temps pour le RGPD. Pour remplir sa tâche, le DPO devra disposer de suffisamment de temps pour étudier la législation et se familiariser avec la matière concernée, mais ses connaissances pourront ensuite être communiquées au reste de l'entreprise. Il est dès lors logique que le DPO joue un rôle de premier plan dans le parcours RGPD.

[9] Article 37-39 : Recital 97

Conditions relatives au Data Protection Officer

Les sociétés qui désignent un DPO doivent tenir compte d'une série de prescriptions. Le nom et les coordonnées du DPO doivent être communiqués à l'Autorité de protection des données (l'ancienne Commission de la Vie privée). Le DPO doit être un spécialiste de la législation relative à la protection de la vie privée, mais il doit également connaître de manière approfondie sa propre société, son fonctionnement ainsi que le marché sur lequel elle opère. Il doit en outre disposer d'une autorité et de moyens suffisants pour remplir sa tâche.

Il est censé faire rapport à la haute direction et donc bénéficier d'une autonomie suffisante. Il convient par ailleurs d'éviter les conflits d'intérêts. Par exemple, dans la plupart des cas, un responsable informatique ne pourra pas simultanément porter la casquette de DPO, car il devrait alors contrôler les mesures de protection mises en place par sa propre équipe. Bien entendu, les modalités de mise en œuvre dépendent de la taille de la structure concernée.

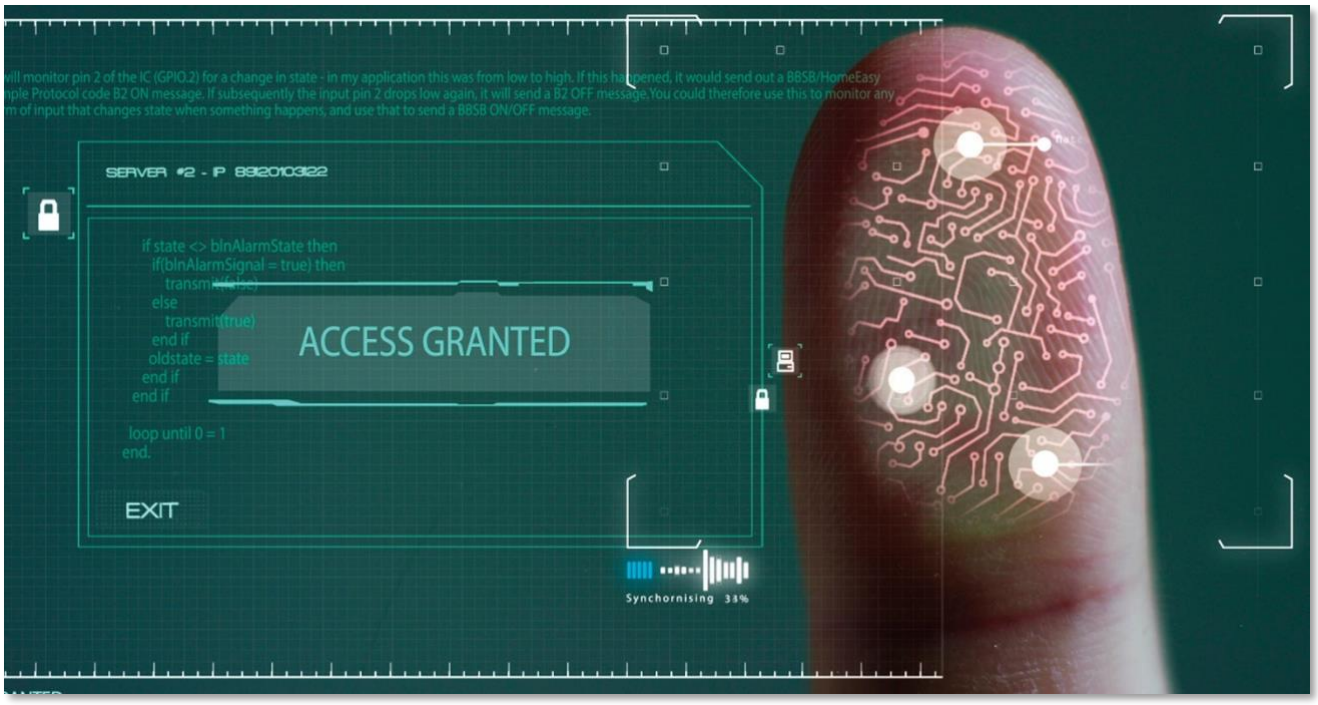
Dans une petite entreprise, le rôle de DPO n'est pas une mission à plein temps, mais se combine à d'autres tâches. Signalons au passage que la fonction de DPO peut également parfaitement être assumée par une personne externe.

Le RGPD n'indique pas le diplôme ou les certificats qu'un DPO doit posséder et ne précise pas non plus les connaissances et l'expérience qui doivent primer : juridiques, organisationnelles ou techniques. Bien entendu, des connaissances minimales sont nécessaires, même au sein d'une petite entreprise. Outre le renforcement des connaissances, qui peut se faire à travers toutes sortes de forums, il sera évidemment utile d'investir dans quelques journées de formations spécifiques.

Un DPO est un atout

Disposer d'un DPO est donc un grand avantage, même si ce n'est pas légalement obligatoire dans votre situation spécifique. Le DPO joue un rôle dans chacune des étapes préparatoires pour le RGPD.

Du reste, dans le cadre de diverses autres procédures ayant trait aux données à caractère personnel, d'autres tâches importantes sont confiées au DPO. Il est associé à la mise en place de chaque nouveau traitement de données à caractère personnel et dispense des conseils sur les risques et les mesures de protection nécessaires. Il est impliqué dans le suivi des incidents ou des réelles fuites de données et constitue à cet égard le premier interlocuteur tant des clients que des personnes concernées et des autorités de surveillance. Enfin, la tâche première du DPO consiste à garantir les droits des personnes concernées. Il est donc leur point de contact direct. La fonction de DPO sera abordée régulièrement dans d'autres sections de ce document.



2. Principes de base du RGPD

Dans ce chapitre, nous identifierons, à partir des principes de base du RGPD[10], les obligations qui vous incombent en tant que responsable du traitement des données à caractère personnel et indiquerons d'emblée six démarches à accomplir pour être parfaitement en règle.

Usage loyal des données à caractère personnel

Le RGPD entend créer un cadre réglementaire permettant l'utilisation d'informations personnelles par les entreprises et organisations, tout en garantissant le mieux possible le respect de la vie privée des personnes concernées.

Les principes de base pour un usage fondé des données à caractère personnel sont les suivants :

- Faire preuve de transparence sur les données que vous détenez et les traitements que vous effectuez ;
- Utiliser les données de façon légale et loyale ;
- Préserver les droits des personnes concernées ;
- Respecter la confidentialité et l'intégrité des données ;
- Répondre en tant que Responsable du traitement.

Ces principes figurent depuis longtemps déjà dans la législation sur la vie privée et ont été régulièrement précisés au fil du temps.

Les principales obligations imposées par le RGPD au Responsable du traitement des données découlent directement de ces principes.

- Vous garantissez la transparence en indiquant clairement quelles données personnelles vous détenez, quel traitement vous effectuez et quel objectif vous poursuivez. Les informations à ce propos doivent être faciles à trouver et rédigées dans un langage clair et simple, afin que chacun puisse les comprendre.
- L'usage loyal des données à caractère personnel suppose que vous les obteniez de manière légale, que vous ne les utilisiez qu'aux finalités prévues et que vous n'en collectiez pas davantage ni ne les conserviez plus longtemps que ce qui est nécessaire pour atteindre l'objectif.
- Toute personne concernée a le droit d'être informée sur le traitement dont font l'objet ses données. Elle peut demander l'accès aux données concrètes et les faire rectifier, compléter ou supprimer. Elle peut en faire cesser le traitement à certaines conditions. Ce ne sera dès lors pas une mince affaire de respecter tous ces droits.

[10] Article 5 : Recital 39

- Le respect des données implique que vous mettiez tout en œuvre pour les introduire et les tenir à jour qualitativement et le plus correctement possible, et que vous les protégiez convenablement de sorte qu'elles ne puissent être divulguées indûment ou utilisées à mauvais escient.
- Le Responsable doit pouvoir prouver qu'il satisfait à l'ensemble des obligations de la réglementation et devra répondre en cas de manquements.

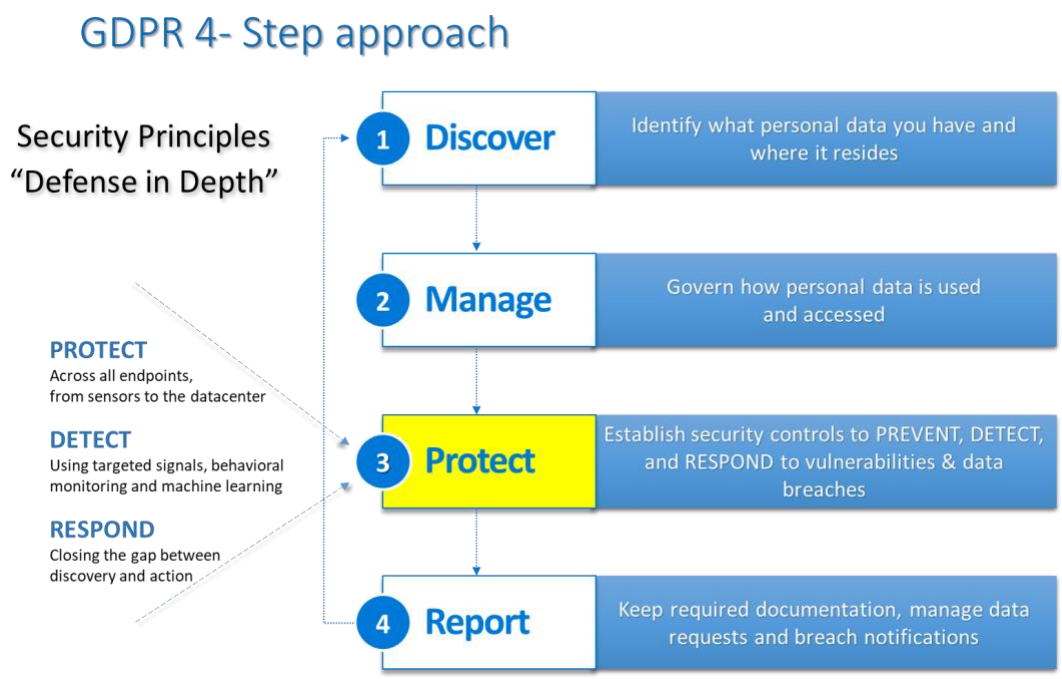
Toute entreprise qui fait de la responsabilité sociétale une priorité souscrira logiquement à ces objectifs. Nous devons dès lors considérer le RGPD et les compléments d'explications fournis par les autorités de contrôle nationales (l'Autorité de protection des données ou APD en Belgique) comme une aide. Ceux-ci doivent servir de repères pour atteindre un but valable sans compromettre le fonctionnement d'une entreprise ou organisation. Le RGPD ne doit en effet pas être à l'origine de crispations en la matière.

Se préparer pour le RGPD

Nous énumérons brièvement ci-dessous les principales démarches qu'un responsable du traitement des données doit accomplir pour se mettre en conformité avec la nouvelle réglementation.

1. Établissez un **registre des activités de traitement des données à caractère personnel**. Vous devez pouvoir soumettre ce registre sur demande à l'Autorité de protection des données. Considérez-le d'abord comme un outil pour vous-même. Vous aurez en effet un aperçu de toutes les données à caractère personnel que vous utilisez. Le registre doit mentionner le type de données, le type de traitement, la finalité et le fondement légal du traitement.
2. Rédigez **une déclaration de confidentialité**. Celle-ci doit pouvoir être facilement consultée partout où vous collectez des données de contact et autres informations sur des personnes.
3. Vérifiez si vous disposez d'une **protection adéquate** de toutes les données à caractère personnel collectées. Votre réseau est-il sécurisé ? Les fichiers contenant des données à caractère personnel sont-ils cryptés ou protégés au moyen d'un mot de passe sécurisé ? Les données qui ne sont plus nécessaires sont-elles supprimées en toute sécurité, qu'il s'agisse d'informations sur support numérique ou sur papier ?

4. Rédigez les instructions à suivre **lorsqu'une personne concernée vous contacte pour exercer ses droits**, afin que vous puissiez accomplir à temps les démarches nécessaires. Chez qui arrive la demande ? Qui fait quoi ?
5. Rédigez une **procédure** claire indiquant toutes les démarches à entreprendre **en cas de fuite de données** et de risque de violation de la vie privée des personnes concernées. Tous les travailleurs sont-ils au courant de cette procédure ?
6. Si vous impliquez des **tierces parties** dans le traitement des données à caractère personnel, établissez un **accord contractuel** décrivant clairement ce que le sous-traitant doit faire et quelles sont ses obligations et responsabilités en vertu du RGPD.



Nous développerons très concrètement chacun de ces points d'action dans des chapitres spécifiques. Nous ne voulons en effet pas nous limiter à des considérations générales mais entendons donner également des conseils pratiques.

3. Registre des traitements des données à caractère personnel

3.1 Inventaire des données à caractère personnel et registre obligatoire

Pour se conformer au RGPD, le meilleur point de départ consiste à dresser un bon inventaire des données à caractère personnel que votre société ou organisation utilise et tient à jour. Peut-être devez-vous également transposer ces informations dans un registre formel des traitements[11]. Il peut être difficile de déterminer si ce registre est obligatoire dans votre cas. Cette section vise donc à vous apporter des précisions à ce sujet.

Inventaire des données à caractère personnel

Pour dresser l'inventaire de leurs données à caractère personnel, les grandes organisations ont recours à des logiciels spécialisés. Mais un simple tableur peut suffire, s'il contient les informations nécessaires.

Conseil:
Vous en saurez déjà davantage en discutant avec vos différents services :

- Quelles sont les données à caractère personnel qu'ils recueillent ou utilisent (quelles catégories, quels types de personnes, combien de personnes concernées) ?
- Comment les données sont-elles traitées (que fait-on avec celles-ci) et dans quel objectif ?
- Avec quels fournisseurs, partenaires ou autres tiers sont-elles partagées ?
- Arrive-t-il que les données soient transférées hors de l'Espace Economique Européen (EEE) ?

Vous devez ensuite vous poser la question de savoir si le but de l'utilisation de ces informations se justifie au regard du droit à la protection de la vie privée des personnes concernées. Enfin, vérifiez les menaces qui pèsent sur la confidentialité et l'intégrité des données, ainsi que les mesures mises en place pour les protéger. Tout responsable du traitement de données à caractère personnel doit se poser ces questions.

Le résultat de cet exercice fournit immédiatement la plupart des informations dont vous avez besoin pour constituer un registre des traitements, une nouvelle obligation du RGPD.

[11] Article 30 : Recital 82

Registre des traitements des données à caractère personnel

La précédente loi sur la protection de la vie privée avait une obligation de déclaration des traitements automatisés à l'autorité de surveillance. En Belgique, il s'agissait de la Commission pour la Protection de la Vie Privée (CPVP), généralement dénommée « Commission Vie Privée ». Ces informations étaient reprises dans un registre public que chacun pouvait consulter. Mais les utilisations les plus courantes des données à caractère personnel en étaient exemptées, par exemple la gestion du personnel, l'administration des salaires et la comptabilité, la gestion des clients et des fournisseurs, les données de contact (sans informations complémentaires), les listes de membres d'associations, l'administration des étudiants... En conséquence, la plupart des organisations n'étaient pas tenues de faire une déclaration.

Mais cela change avec le RGPD : le responsable du traitement composera lui-même le registre. Ce registre devra être numérique et pouvoir être présenté rapidement et aisément en cas d'audit de l'Autorité de protection des données ou dans le cadre d'une enquête découlant d'une plainte ou d'une fuite de données. Il devra démontrer que le Responsable dispose d'un aperçu clair des données à caractère personnel dont il assure le traitement. Ce dernier prouve ainsi qu'il a réfléchi à son droit d'effectuer ces traitements et qu'il protège les informations efficacement.

Autre différence avec l'ancienne loi sur la protection de la vie privée: le RGPD ne se limite pas au traitement automatisé de données et ne fait plus d'exception pour les « données à caractère personnel couramment utilisées ».

Obligation de registre : qui est concerné ?

Dans une certaine mesure, les petites entreprises sont exemptées de l'obligation de registre[12], mais le RGPD n'est pas très précis à ce sujet. C'est pourquoi la Commission Vie Privée de Belgique a publié (le 14 juillet 2017) une recommandation détaillée dont nous synthétisons ici les points essentiels.

- Chaque Responsable (et chaque sous-traitant, mais nous aborderons ce point en détail plus tard), peu importe qu'il s'agisse d'une entreprise, d'un organisme public, d'une association ou d'une personne physique, doit tenir à jour un registre des traitements.

[12] Article 30.5 : Recital 13

- Toutefois, on fait une exception pour les structures comptant moins de 250 travailleurs (et générant un chiffre d'affaires inférieur à 50 millions d'euros). À vrai dire, cette exception ne cadre pas avec l'esprit de la législation, puisque toutes les mesures doivent découler de l'analyse des risques. Or le traitement de données à caractère personnel au sein d'une petite structure peut comporter autant voire davantage de risques. C'est pourquoi l'obligation de registre reste tout de même applicable dans toute une série de cas complémentaires, y compris pour les PME.

  Vous ne pouvez pas vous soustraire à l'obligation de registre si :

  - Vous traitez des catégories particulières de données à caractère personnel ou les données de personnes spécialement vulnérables (comme les enfants) ;
  - Le traitement présente des risques pour les droits et les libertés des individus et peut donc entraîner des dommages corporels, matériels ou immatériels. La recommandation propose une série d'exemples : s'il y a un risque de violation de la confidentialité d'informations financières ou de données protégées par le secret professionnel ; s'il y a un risque de vol ou d'usurpation d'identité ; si des données concernant la santé, la personnalité, le comportement, les déplacements, etc. sont utilisées pour l'établissement de profils personnels ;
  - La personne concernée n'a pas la possibilité d'exercer ses droits personnels et n'a donc aucun contrôle ;
  - Un responsable traite les données de manière non pas occasionnelle, mais structurelle, c'est-à-dire que le traitement d'informations ne se fait pas par hasard ou une seule fois, mais de manière habituelle. À titre d'exemple, la note mentionne des informations sur les clients, les fournisseurs et les travailleurs.

En résumé, on constate que les limites sont difficiles à établir. Car chaque organisation dispose de certaines données qui, en cas de violation de leur caractère confidentiel, peuvent occasionner des dommages, et toutes les organisations conservent des données de manière structurelle.

L'Autorité de protection des données conseille dès lors à toutes les entreprises et à tous les organismes de tenir un registre, les PME pouvant le réduire aux données traitées structurellement.

Dans une petite structure, l'exercice reste donc relativement limité.

3.2. Registre des activités de traitement des données à caractère personnel

Penchons-nous à présent sur le contenu du registre des activités de traitement des données à caractère personnel[13]. Il est recommandé à tous les responsables de tenir un tel registre, bien que pour les petites organisations, cela ne soit pas toujours obligatoire au sens strict.

La première étape consiste en une simple liste des données à caractère personnel des personnes avec lesquelles votre entreprise ou organisation travaille. L'Autorité de protection des données explique quelles sont les exigences de ce registre et les articule autour de six questions simples : qui, pourquoi, quoi, où, jusqu'à quand, comment. Vous trouverez sur son site un bref résumé, une note circonstanciée et même, depuis peu, un modèle de registre à télécharger. Examinons ces six questions.

Qui ?

Votre registre stipule avant tout qui est le responsable. Il faut donc indiquer les coordonnées correctes de votre entreprise ou organisation, ainsi que le nom et les coordonnées de votre Data Protection Officer ou, à défaut, de la personne à contacter en cas de questions, problèmes, plaintes ou fuites de données.

Dans les grandes organisations, il est utile de spécifier quel département ou quelle personne est responsable de chaque ensemble distinct de données à caractère personnel. Ce responsable sera en effet le point de contact pour aider à compléter les autres points du registre.

Pourquoi ?

Il est primordial de savoir dans quel but vous utilisez des données à caractère personnel. Le principe de base de toute législation relative à la protection de la vie privée, et surtout du RGPD, est de ne récolter et traiter des informations que si c'est absolument nécessaire pour la finalité établie. Par exemple, vous avez évidemment besoin de leurs coordonnées pour communiquer avec vos clients et vos fournisseurs. Et pour les activités commerciales et de marketing de votre entreprise, il vous faut collecter des noms et des adresses. Il est en outre souhaitable d'enrichir ces données de base avec des informations supplémentaires, comme la répartition géographique des clients ou leur secteur d'activité.

L'Autorité de protection des données souligne que l'objectif doit être aussi concret que possible, et doit démontrer clairement la nécessité de traiter ces informations. Une liste indicative de types de finalités est jointe à leur note.

[13] Article 30.1 : Recital 39

Il est également utile de s'arrêter un instant sur la base juridique dont dispose votre organisation pour traiter ces données à caractère personnel, bien que cela ne doive pas impérativement figurer dans le registre. Dans certains cas, la base juridique donnera lieu à des obligations spécifiques ou des procédures à suivre. Le fait d'ajouter immédiatement cette indication dans le registre vous facilitera la vie lorsque vous voudrez contrôler par la suite que vous respectez bien toutes les obligations légales.

Quoi ?

Pour chaque finalité, vous définissez ensuite de quelles catégories de personnes les données à caractère personnel traitées relèvent : clients, travailleurs, visiteurs… Indiquez d'emblée les nombres approximatifs concernés, car cela peut vous donner une idée de l'impact en cas de fuite de données.

Précisez ensuite quelles sont les informations conservées et utilisées à propos de ces personnes : s'agit-il uniquement des noms et adresses ou également d'informations sur l'âge, le sexe, la fonction, les centres d'intérêt, etc. ? L'explication de l'Autorité de protection des données donne une liste de catégories possibles.

Il est crucial de mentionner explicitement si certaines informations relèvent de catégories particulières (cfr. Section 1.2), pour lesquelles des règles et des limitations spécifiques sont applicables. Cela vaut également pour les informations ne relevant pas de ces catégories particulières, mais qui sont malgré tout considérées comme sensibles, comme les informations financières ou les données relatives aux mineurs.

Où ?

Pour chaque finalité identifiée, le registre doit énumérer où vont les informations. Il peut s'agir de personnes physiques, mais aussi d'organismes publics ou d'un centre de traitement des données interne ou externe. Tous les destinataires sont mentionnés.

Il est important de spécifier si ces informations sont exclusivement traitées au sein de l'Espace Economique Européen. Si ce n'est pas le cas, il faut disposer de garanties quant à la protection adéquates des données à caractère personnel et quant au fait que les personnes concernées jouissent des mêmes droits et protections. Cela doit être démontré dans le registre.

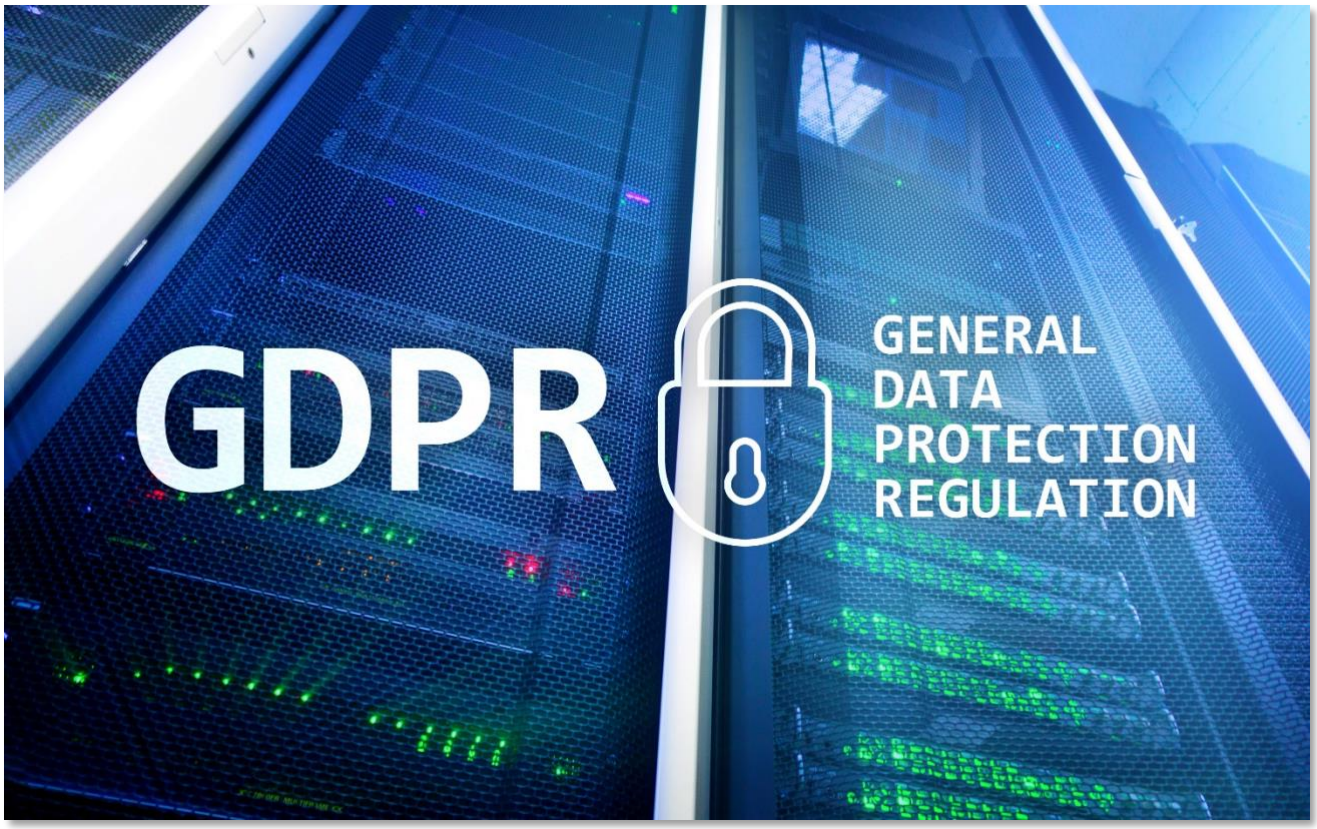
Jusqu'à quand ?

Comme ces données ne peuvent être utilisées que pour la finalité envisagée, il va sans dire qu'elles ne peuvent être conservées plus longtemps que nécessaire. L'Autorité de la protection des données précise que les délais de conservation ne doivent pas toujours être exprimés en nombre de jours, de mois ou d'années. Une formulation telle que « le délai de conservation prévu par la loi » est également possible.

Comment protégeons-nous les données ?

Dans le cadre du RGPD, vous êtes responsable de la protection des données à caractère personnel traitées. Vous devez prendre toutes les mesures nécessaires pour éviter que leur confidentialité ou leur intégrité ne soit menacée. Elles ne peuvent être ni rendues publiques de manière injustifiée, ni transmises à des destinataires erronés ni modifiées injustement.

Si vous avez correctement et minutieusement complété ce registre, vous disposez d'une bonne base pour démontrer que vous gérez le traitement des données à caractère personnel de façon adéquate, et que vous prenez cette responsabilité au sérieux. C'est le point de départ pour, ensuite, élaborer vos procédures internes et contrôler leur bonne application. Enfin, ce registre constituera une aide précieuse lors de la rédaction d'une déclaration relative à la protection de la vie privée.



4. Fondement juridique pour le traitement

4.1 Fondement juridique pour le traitement des données à caractère personnel

Lors de l'élaboration du registre des activités de traitement des données à caractère personnel, le responsable a tout intérêt à définir le fondement juridique[14], même s'il ne s'agit pas d'une composante obligatoire du registre. Pour une utilisation légale des données, le traitement doit faire l'objet d'une finalité spécifique et d'un fondement juridique démontrable. En outre, le traitement doit respecter les règles de subsidiarité et de proportionnalité. En d'autres termes, il doit être nécessaire et proportionnel à l'objectif.

Le RGPD prévoit plusieurs fondements juridiques possibles, qui ne sont pas applicables dans tous les cas. Il est important de bien réfléchir au fondement avant de commencer un traitement. Ce processus doit être documenté et peut jouer un rôle important en cas de litige ou de plainte ultérieurs.

Le RGPD fournit des instructions on ne peut plus claires et spécifiques à propos de **l'autorisation de la personne concernée** comme fondement juridique, mais nous en parlerons plus spécifiquement plus loin dans ce chapitre.

D'autres fondements juridiques peuvent en outre être invoqués. **Les données peuvent être nécessaires pour la réalisation ou la préparation d'un contrat**. Pour la collaboration entre les clients et les fournisseurs, toutes sortes de données à caractère personnel sont nécessaires. Il s'agit avant tout de coordonnées, mais dans l'univers B2C, des données de paiement et des informations financières peuvent s'y ajouter. Pour autant que le caractère nécessaire des informations traitées puisse être démontré pour l'établissement du contrat ou la prestation des services convenus, ce fondement juridique suffit comme justification.

Une **obligation légale** peut également constituer la base pour le traitement des données à caractère personnel. Il peut s'agir de la législation européenne ou nationale qui oblige les entreprises à transmettre des informations aux autorités. C'est notamment le cas pour les banques, les compagnies d'assurances, les compagnies aériennes, etc.

En outre, l'**intérêt général** peut lui aussi constituer un fondement juridique, par exemple si les autorités conviennent d'accords organisationnels avec des entreprises pour l'administration des impôts. Ce fondement juridique permet également de collecter des informations à des fins scientifiques ou historiques. Les tâches des autorités publiques relèvent également de l'intérêt général.

[14] Article 6 : Recital 40-50

La loi prévoit également, pour les **affaires vitales** (s'il est véritablement question de vie ou de mort), la possibilité d'utiliser les données à caractère personnel de la personne concernée ou d'une autre personne physique. Il faut évidemment agir dans l'intérêt de la personne individuelle, avec suffisamment de bon sens.

Enfin, il reste **l'intérêt légitime du responsable ou d'un tiers**. Cela ne s'applique pas aux autorités publiques. Lorsqu'on invoque ce fondement juridique, il convient toujours de l'expliciter et d'équilibrer les intérêts avec le droit de confidentialité des personnes concernées. Dans le registre comme dans les déclarations de respect de la vie privée rédigées à titre d'explication pour les personnes concernées, cela doit être clairement démontré et explicité. Un intérêt purement économique ne suffit plus comme justification. Et le traitement doit bel et bien être nécessaire. Il s'agit dans tous les cas du fondement juridique le plus faible de tous.

Le RGPD demande explicitement d'accorder une attention particulière au traitement des données relatives aux enfants (jusqu'à l'âge de 16 ans). Une autorisation parentale est alors nécessaire, ce qui n'est guère facile à organiser.

S'il s'agit du traitement de catégories spéciales[15] de données à caractère personnel (voir leurs définitions à la section 1.2), les règles sont encore plus strictes. Un tel traitement est interdit, sauf dans certains cas énumérés par le RGPD.

Parcourons brièvement les différents cas autorisés :

- Si la personne concernée a explicitement donné son autorisation
- S'il s'agit de données déjà publiquement disponibles parce qu'elles ont manifestement été publiées par la personne concernée elle-même
- Sur base de la législation relative à l'emploi (toutes sortes de données doivent être traitées dans le cadre de la sécurité sociale, des obligations légales et des accords contractuels)
- Dans les affaires d'importance vitale, si la personne concernée n'est pas en mesure de donner son autorisation (il s'agit souvent précisément de l'utilisation ou de la transmission de données médicales)
- Pour les ASBL ou les œuvres caritatives, pour autant qu'il s'agisse d'une utilisation légale des données relatives aux membres, anciens membres ou personnes avec lesquelles elles sont en contact régulier
- Pour les associations, syndicats ou organisations politiques et religieuses (à des fins politiques, philosophiques ou religieuses)

[15] Article 9 : Recital 51-56

- Les données relatives à des infractions ou des affaires pénales ne peuvent être traitées que par les autorités publiques ou dans les cas prévus par la législation (européenne ou nationale).
  Chaque pays peut en outre imposer ses propres limitations. Le droit pénal est d'ailleurs une matière nationale, qui n'est pas régie par le RGPD.
- Si les données sont nécessaires dans le cadre d'un procès
- Dans certains cas, en raison de l'intérêt général :
  - En cas d'intérêt général substantiel, et couvert par la législation européenne ou nationale, protégeant également les droits de l'individu
  - Dans le cadre des soins de santé (diagnostic par des professionnels de la santé, données pour l'organisation des soins de santé ou la sécurité sociale, évaluation de la santé des travailleurs, étude des médicaments)
  - Données nécessaires pour la recherche scientifique ou historique, ou l'archivage, avec la prise des mesures de protection nécessaires (les résultats de l'étude peuvent par exemple être anonymisés ou pseudonymisés).

Il faut toujours une raison importante pour traiter des données à caractère personnel. Dans les sections suivantes, nous nous pencherons sur l'autorisation de la personne concernée et l'intérêt légitime du responsable comme fondement juridique.

4.2 Autorisation de la personne concernée

Le meilleur fondement pour le traitement légal des données à caractère personnel est d'obtenir l'autorisation[16] de la personne concernée. Dans la pratique, cela n'est toutefois pas évident. Et comme cette autorisation peut être retirée à tout moment, ce fondement juridique comporte une certaine incertitude.

L'autorisation est depuis longtemps ancrée dans la législation relative à la protection de la vie privée, mais les règles sont devenues de plus en plus strictes au fil des ans. À l'origine, une sorte d'accord tacite était possible, souvent dans le cadre d'un contrat plus vaste et sans objectif bien défini. S'en est suivie l'obligation de pouvoir retirer cette autorisation (le fameux « opt out »). Aujourd'hui, le RGPD définit toute une série de conditions à remplir pour pouvoir parler d'une autorisation légalement valable (« opt in »). L'autorisation doit être donnée de manière volontaire, active, informée, clairement spécifiée, et elle doit pouvoir être retirée tout aussi facilement.

Volontaire

L'autorisation de la personne concernée ne peut être utilisée comme fondement juridique s'il n'y a pas de rapport équilibré entre le responsable et la personne concernée. Cela vaut par exemple pour la relation entre le travailleur et l'employeur. En effet, le travailleur n'est généralement pas en mesure de refuser.

L'autorisation ne peut non plus être liée à l'octroi d'un service, sauf si les données sont directement nécessaires à l'exécution du contrat. Dans ce cas, la nécessité contractuelle constitue le fondement juridique, et il est préférable, pour que les choses soient claires, de ne pas demander d'autorisation. L'autorisation pour l'utilisation des données dans le cadre de campagnes marketing et publicitaires ultérieures ne peut faire partie d'un contrat à conclure ou de conditions générales. Pour le RGPD, cela n'est valable que si les deux actes peuvent être séparés.

Active

La personne concernée doit faire une déclaration claire ou poser un acte indiquant qu'elle donne son autorisation pour un traitement donné. À cet égard, toute méthode ou tout mode de travail adéquats sont autorisés. Le RGPD énumère même les méthodes les plus courantes : accord verbal ou écrit pour marquer son accord, case à cocher sur laquelle il faut cliquer ou activation d'un paramètre dans un navigateur ou une app. Ce qui est nouveau, c'est que le RGPD exclut explicitement que cet accord soit tacite ou découle de l'inactivité. Une case préalablement cochée est par exemple exclue.

[16] Article 4.11; Article 7-8 : Recital 32-33,38,42-43

Ne pas utiliser une fonction « opt-out » ou un bouton « se désinscrire » ne constitue pas non plus une autorisation valable. Il s'agit là d'une condition très importante pour toutes les organisations qui développent des campagnes de marketing direct.

Informée

La personne concernée doit recevoir, avant que son accord ne lui soit demandé, des informations détaillées sur l'identité du responsable, les traitements prévus, l'objectif, le fondement légal et les mesures prises pour protéger ses données. Cela doit se faire de manière honnête, en des termes clairs et simples. Il doit y avoir un lien clair entre l'objectif, les données nécessaires à cet effet et l'autorisation à donner. Une forme adéquate pour cette communication est par exemple une déclaration détaillée de respect de la vie privée. Nous évoquerons dans un prochain chapitre les informations qui doivent y figurer et comment les mettre de préférence à la disposition des personnes concernées.

Spécifique et sans ambiguïté

L'autorisation pour le traitement des données à caractère personnel est toujours donnée pour un objectif spécifique. Le responsable ne peut donc utiliser les données à d'autres fins, sauf si le nouvel objectif est très proche de l'objectif de départ. Un bon exemple : le fait de contacter un ancien client ou un client existant pour l'informer d'un produit ou d'un service apparenté à ce qu'il a déjà acheté par le passé.

Une attention particulière est nécessaire si vous envisagez de combiner les données d'une autre manière ou de les utiliser à une toute autre fin. Dans ce contexte, le « datamining » pose problème. Cette technique est régulièrement utilisée, notamment dans le marketing, pour découvrir des modèles possibles ou des liens inattendus dans de grandes quantités d'informations. De ce fait, il n'y a pas d'objectif établi. Le RGPD permet, dans les cas de réutilisation des données, une certaine latitude pour un assouplissement. Il est possible de demander l'autorisation explicite de la personne concernée lors de la prochaine utilisation de ses données.

L'autorisation peut être retirée

Dans tous les cas, vous devez informer la personne concernée du fait qu'elle a toujours la possibilité de retirer son autorisation. Cela doit pouvoir se faire par le biais d'un acte simple, aussi facilement que pour l'octroi de l'autorisation. Désormais, le RGPD impose clairement cette obligation au responsable.

Bien que cette approche semble logique et équitable, sa mise en pratique n'est pas toujours aussi évidente. En particulier parce que le RGPD oblige le responsable à démontrer clairement que les personnes concernées ont bel et bien donné leur autorisation.

4.3 Autorisation ou intérêt légitime ?

Nous avons évoqué les fondements juridiques possibles pour le traitement des données à caractère personnel. Dans certains cas, plusieurs fondements juridiques[17] peuvent être invoqués. Mais comment choisir le meilleur pour justifier votre traitement ?

Il est moins facile de répondre à cette question qu'il n'y paraît. Pourtant, il est important de s'y arrêter, car votre choix n'est pas sans conséquences. Tel fondement juridique vous apportera plus de sécurité à long terme que tel autre. Mais passer de l'un à l'autre est source de confusion et peut donner l'impression que vous voulez induire en erreur les personnes concernées.

Tant que cela concerne des données traitées dans le cadre de l'exécution d'un contrat (comme par exemple des coordonnées pour des commandes, livraisons ou prestation de services et facturation) ou dans le cadre d'obligations légales, aucun doute n'est possible. Par contre, il est nettement plus complexe de choisir entre l'autorisation de la personne concernée ou l'invocation d'un intérêt légitime.

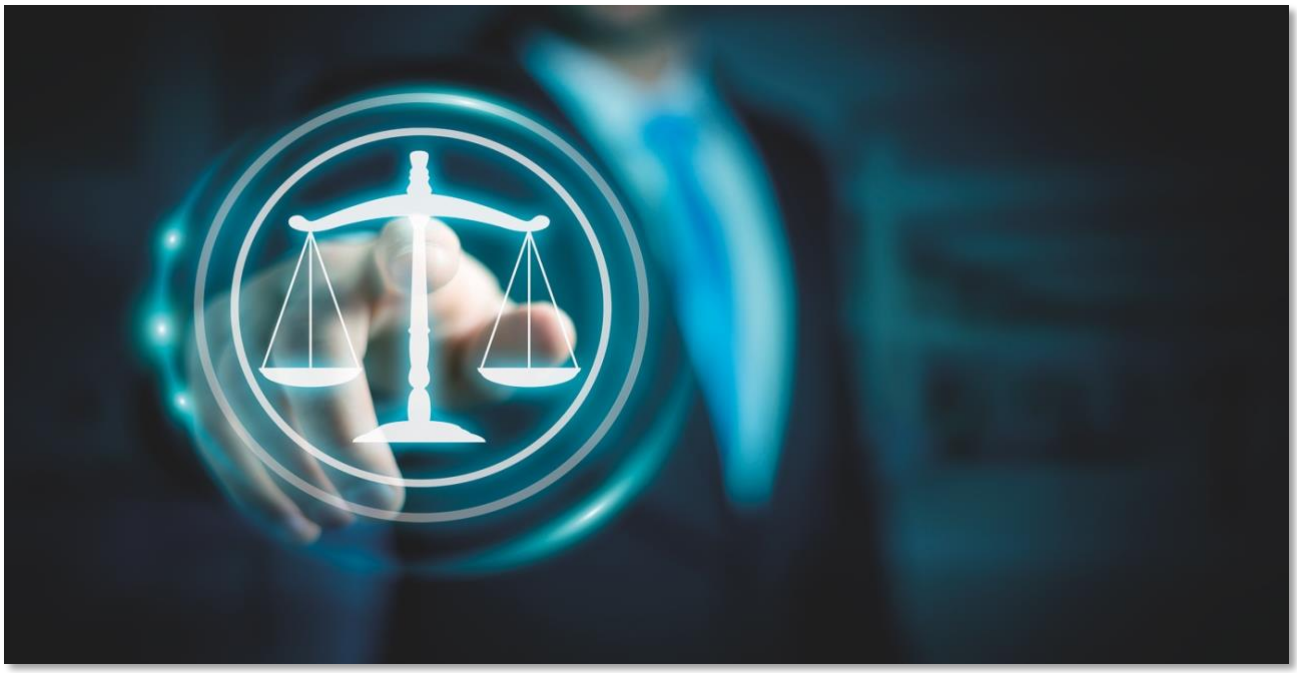
Demander l'accord des personnes concernées semble toujours être une bonne option, mais cela comporte également des risques. Si vous demandez une autorisation que vous n'obtenez pas, vous ne pouvez évidemment plus traiter les données. Imaginez que vous demandiez à chaque personne reprise dans un fichier pour une campagne marketing son autorisation explicite pour pouvoir la contacter à l'avenir. Le taux de réponse à ce genre d'action se situe aux alentours de 10 %. Conséquence ? Vous ne pouvez plus utiliser la majeure partie de vos contacts.

Dans tous les cas où vous pouvez démontrer que vous avez bel et bien obtenu cette autorisation, vous êtes bien sûr protégé(e). Vous créez également une bonne image, en communiquant ouvertement sur vos intentions et en tenant compte des préférences de vos contacts. Mais cela entrave une diffusion vaste de vos campagnes et rend l'ajout de nouveaux destinataires particulièrement complexe. Enfin, il y a toujours le risque qu'une personne concernée revienne ultérieurement sur sa décision et retire son autorisation, ce qui réduit encore votre base de contacts.

Quelles alternatives s'offrent alors à vous ? Vous pouvez toujours invoquer l'intérêt légitime de votre organisation comme fondement juridique. Une organisation commerciale – pour reprendre l'exemple des campagnes marketing – ne peut en effet pas fonctionner sans la possibilité de présenter et de vanter ses produits ou services. Comme nous l'avons déjà dit, votre dossier doit dans ce cas être soigneusement constitué.

[17] Article 6-9 : Recital 47-49

Pour commencer, limitez les données à traiter au strict nécessaire. Avec moins d'informations, le risque d'une atteinte grave à la vie privée est automatiquement réduit. Un fichier ne contenant que des coordonnées est évidemment moins critique qu'une grande collection de données dont certaines sont sensibles.



Prenez ensuite toutes les mesures nécessaires pour protéger correctement ces données et assurer leur confidentialité. Démontrez que les données collectées ne peuvent être utilisées à d'autres fins. Vous préservez de la sorte l'équilibre entre les intérêts des personnes concernées et les intérêts de votre organisation. Décrivez brièvement (ou de manière plus circonstanciée) votre argumentaire dans votre registre. En cas de litige, vous pourrez toujours attester que vous agissez de bonne foi, en ayant fait les bonnes considérations.

Toutefois, aucune de ces mesures n'empêche que le fondement juridique de l'intérêt légitime ne puisse être contesté. Une personne concernée qui se sent lésée, ou un concurrent qui estime que vos pratiques sont malhonnêtes, peut déposer plainte à l'Autorité de protection des données. Cette plainte peut entraîner une enquête et éventuellement aboutir devant le tribunal. Le résultat de tout cela dépend alors de l'interprétation des faits concrets par les auditeurs ou par le juge, et cela peut s'écarter de vos propres estimations.

Un jugement en votre défaveur peut mener à une amende, vous empêcher de poursuivre le traitement ou vous contraindre au paiement d'une indemnité. Lors de l'établissement du jugement et des mesures correctives, l'Autorité de la protection des données tiendra toutefois compte de la situation générale. Si une organisation ne respecte aucun aspect de la législation relative au respect de la vie privée, les faits reprochés pèseront plus lourd.

Par contre, si vous avez pris les mesures nécessaires et pouvez démontrer selon quels raisonnements vous avez justifié certains traitements, les faits qui vous sont reprochés paraîtront moins graves.

Nous avons conscience de ne pas avoir fourni de réponse simple, ni de directive univoque. Mais le respect de la vie privée est un droit qu'il convient de confronter à d'autres droits, et ce sera toujours une question d'interprétation et de discussion. Du bon sens et une approche ouverte et honnête constituent déjà un bon début. Ensuite, vous devez communiquer clairement votre point de vue et bien le documenter. Vous devez évidemment veiller à prendre toutes les mesures de protection attendues tout au long du processus de traitement afin de limiter les risques d'infraction.

5. Transparance

5.1 Qu'est-ce qu'une Déclaration de confidentialité et que doit-elle comporter?

Dans les chapitres précédents, nous avons largement évoqué le registre des activités de traitement des données à caractère personnel. Dans ce registre, vous consignez quelles données à caractère personnel sont traitées au sein de votre organisation, dans quel but et selon quel fondement juridique. Ce registre doit exister au sein de toute organisation. L'utilité de ce registre va toutefois bien plus loin. Vous pouvez l'utiliser comme point de départ pour une analyse des risques et pour un aperçu des mesures de protection et des procédures internes de votre organisation. Nous reviendrons sur ce point plus tard. Par ailleurs, un registre bien tenu vous fournit la source idéale pour informer les personnes concernées quant au traitement de leurs données. C'est le sujet de ce chapitre.

Le RGPD exige de votre part une grande ouverture envers toutes les personnes concernées, en d'autres termes toutes les personnes dont vous utilisez les données. Elles ont parfaitement le droit d'être informées des traitements appliqués à leurs données. Une « Déclaration de confidentialité » est un texte dans lequel votre organisation rend ceci public[18].

Le RGPD définit les informations à fournir à la personne concernée. Une Déclaration de confidentialité soigneusement rédigée doit donc aborder chacun de ces points.

- Le **responsable des activités de traitement des données** doit se présenter clairement, avec le nom exact de l'entreprise ou de l'organisation et l'adresse complète du siège. Si l'organisation a désigné un Data Protection Officer (DPO), la Déclaration de confidentialité doit mentionner comment le contacter. Il n'est pas nécessaire de communiquer le nom de cette personne, mais il faut au moins fournir une adresse, un numéro de téléphone ou un e-mail permettant de la joindre. À défaut de DPO, il faut assurément renvoyer vers un point de contact.
- La partie la plus importante de la déclaration concerne **l'énumération des activités de traitement** des données à caractère personnel qu'exécute votre organisation. Cette énumération doit être suffisamment détaillée et distincte pour chaque finalité. Précisez chaque fois dans quel **but** certaines données sont collectées, quelles sont les **catégories** de données traitées et les catégories de personnes concernées, quelles sont les **activités de traitement** réalisées et quel est le fondement juridique invoqué pour effectuer ces traitements.

[18] Article 13-14 : Recital 60-62

Vous pouvez évidemment vous inspirer de votre registre interne afin de ne rien oublier.

- Les **destinataires** doivent être clairement définis. Qui a accès à ces informations ? À qui sont-elles transmises ? Spécifiez les catégories de collaborateurs impliquées en interne dans le traitement de ces données, et qui ont donc droit de regard sur ces informations. Précisez si des parties externes sont impliquées dans le traitement. Si les informations collectées sont transmises à des tiers pour une autre utilisation, cela doit être explicitement indiqué. Le plus souvent, cela se fait à l'aide de termes généraux, tels que « sociétés-sœurs » ou « partenaires ». Le RGPD mise sur une transparence maximale. Il est en effet important que les personnes concernées comprennent ce qu'il advient de leurs données, sans que l'on attende de votre part que vous nommiez chaque partenaire ou fournisseur.
- Vous devez ensuite démontrer que vous avez pris **suffisamment de mesures de sécurité** pour garantir la confidentialité et l'intégrité des données. Ici encore, il n'est pas nécessaire de dévoiler la technologie et les procédures dans le détail, car cela nuirait précisément à la sécurité. Mentionnez les principes appliqués et la façon dont vous les garantissez en interne.
- Une exigence spécifique concerne les informations relatives au **délai de conservation des données**. Le RGPD stipule que vous ne pouvez utiliser les données collectées que pour la finalité établie, et que vous ne pouvez pas les conserver plus que nécessaire pour cette finalité. En outre, en tant que responsable, vous devez veiller à la qualité des données. Cela implique donc qu'elles ne soient pas obsolètes. Il est préférable de préciser ce délai de conservation pour chaque finalité spécifique.
- Votre Déclaration de confidentialité doit également énumérer clairement les **droits des personnes concernées**.
    - La personne concernée peut toujours déposer une plainte à l'Autorité de protection des données si elle estime que ses données ne sont pas traitées correctement.
    - Elle peut demander au responsable des informations quant aux activités de traitement de ses données ; vous devez lui expliquer quelle procédure suivre pour cela.
    - Elle peut consulter les informations disponibles et si nécessaire les faire modifier ou supprimer.

Nous aborderons les droits de la personne concernée plus loin dans ce document.

- Enfin, le RGPD vous demande de spécifier si vous **exportez certaines données en dehors de l'Espace Economique Européen (EEE)**. Si tel est le cas, la protection adéquate des données et des droits de la personne concernée est exposée à des risques supplémentaires. Pensez par exemple aux compétences d'une instance comme la NSA aux États-Unis. Les garanties varient en fonction du pays vers lequel les données sont exportées ou du secteur de l'entreprise ou de l'organisation. Il s'agit d'une matière juridique très complexe. Le plus souvent, il suffit de mentionner que les données ne sortent pas de l'EEE et sont donc parfaitement couvertes par la protection juridique du RGPD. Si ce n'est pas le cas, vous devez spécifier où vont les données et quelle est la protection applicable. La personne concernée peut alors décider si la confidentialité de ses données est suffisamment garantie.

Le RGPD prévoit non seulement le contenu de votre Déclaration de confidentialité, mais fournit aussi des directives relatives à sa forme et à sa structure. La façon dont vous communiquez ces informations aux personnes concernées, le moment auquel vous le faites et la manière dont vous les gardez à jour sont également importants. C'est ce que nous examinons dans la section suivante.

5.2 Comment présenter au mieux une Déclaration de confidentialité?

Nous avons évoqué tout ce qu'il fallait mentionner dans une Déclaration de confidentialité, afin que toutes les personnes concernées soient correctement informées des traitements subis par leurs données. La manière dont vous présentez cette déclaration est également importante. Les auteurs du RGPD y ont accordé une attention particulière.

En tant que responsable, vous êtes tenu(e) de fournir ces informations de **manière concise et dans un langage compréhensible**[19]. Par le passé, certaines entreprises s'étaient spécialisées dans la rédaction de textes particulièrement lourds, avec des formulations incompréhensibles pour le commun des mortels, et comptant des dizaines de pages. Vous décourageez ainsi le lecteur, ce qui est diamétralement opposé à la transparence souhaitée. Le RGPD attend de vous que vous utilisiez un langage simple, à la portée de tous. Aux Pays-Bas, cela correspond explicitement au niveau linguistique B1, le niveau de l'enseignement primaire. Si votre public compte également des enfants, il est primordial d'expliquer en mots simples ce que vous faites avec les données transmises. Il est généralement préférable de rédiger une Déclaration de confidentialité distincte pour les enfants.

La transparence est également meilleure si vous commencez par exposer **les grandes lignes**, avec un texte bien structuré. Vous pouvez par exemple décrire chaque thème dans une phrase courte ou un bref paragraphe et offrir la **possibilité de cliquer** pour obtenir de plus amples informations. L'utilisateur trouvera ainsi rapidement ce qu'il cherche et pourra approfondir ses recherches s'il le souhaite. L'utilisation d'icônes peut être utile pour faire passer le message encore plus simplement. Des groupes de travail œuvrent depuis plusieurs années au développement d'icônes spécifiques, mais il s'agit d'un défi de taille.

N'oubliez pas non plus de **dater** votre Déclaration de confidentialité et de préciser un **numéro de version**. En effet, ce genre de texte vit : la nature des données traitées peut être modifiée, tout comme les destinataires ou les mesures de protection prises. Votre texte doit comporter des informations correctes et actuelles. Il changera donc souvent. Or, les personnes concernées doivent être informées de ces changements. Vous devez donc au moins leur signaler que votre déclaration est susceptible d'être modifiée ultérieurement. Invitez-les à consulter régulièrement la page ad hoc de votre site web. Et pensez à conserver les anciennes versions de votre Déclaration de confidentialité, afin qu'en cas de litige relatif à un traitement de données, il vous soit possible de voir quelles étaient les informations à la disposition de la personne concernée au moment dudit traitement.

[19] Article 12.1 : Recital 58

Selon les circonstances, choisissez où et sous quelle forme vous publiez votre Déclaration de confidentialité. Veillez en tout cas à ce qu'elle soit **facile à retrouver**. Évitez la Déclaration de confidentialité coincée dans les conditions générales. La méthode la plus classique consiste en un lien depuis le site web, mais une Déclaration de confidentialité peut également être communiquée sur papier, voire verbalement. Vous devez toutefois tenir compte de quelques règles.

Si les utilisateurs complètent leurs données à caractère personnel sur un site web ou dans une application, vous devez veiller à ce que les informations nécessaires relatives au traitement leur aient été **préalablement** fournies. Le plus simple étant pour cela de renvoyer, dans l'introduction de l'application, à la Déclaration de confidentialité. Sur de nombreux sites web, vous trouverez cette mention dans une barre au bas de chaque page. C'est évidemment moins spécifique, et ce n'est pas en lien avec une finalité précise, mais les informations sont disponibles dès l'ouverture du site. C'est important sur les sites qui collectent des informations sur le comportement de surf des visiteurs, par le biais de cookies ou d'autres outils. Cela commence en effet dès l'ouverture du site web et par conséquent le visiteur en doit être immédiatement informé.

Vous pouvez parfaitement rédiger **plusieurs Déclaration de confidentialité**, adaptées à certains publics cibles. Vos clients et vos prospects ne sont sans doute pas intéressés par la façon dont votre organisation gère les données du personnel. Cela vous permet de réduire aussi la longueur du texte.

Conseil:
Le RGPD constitue en outre une bonne occasion, pour les organisations, **d'examiner leur politique en matière de traitement des données du personnel** et de communiquer en interne à ce sujet. Les données en circulation relatives au personnel sont bien plus nombreuses que ce que vous pensez, et certaines sont sensibles.

- Toutes sortes de données sont nécessaires pour le traitement des salaires (salaire, présence, absentéisme, composition du ménage). Pour de nombreuses entreprises, ces informations sont traitées en externe, par un secrétariat social qui endosse donc le rôle d'organisme qui traite les données. Désormais, des informations doivent être communiquées aux autorités, dans le cadre de la sécurité sociale et de l'administration fiscale.
- Les dossiers internes du personnel comportent toutes sortes d'informations relatives à la carrière. Lors de recrutements, d'évaluations ou de promotions, ces informations sortent du service du personnel. Il est important de mettre au point les procédures de confidentialité pour ces données.

- D’autres données ont trait à l’utilisation d’outils ICT. Cela peut aller du contenu d’e-mails via des comptes d’utilisateurs, groupes d’utilisateurs et niveaux d’autorisation, aux fichiers log relatifs à l’utilisation d’applications ou la consultation de sites web. Il est important de communiquer ouvertement sur les informations enregistrées dans les fichiers log et leur finalité. Il convient en outre de définir clairement ce que l’employeur peut et ne peut pas faire avec ces informations.

Au sein des plus grandes organisations, ces points doivent être évoqués lors du Conseil d’entreprise. Dans les plus petites entreprises aussi, il est nécessaire d’informer les travailleurs de tous les traitements de leurs données à caractère personnel. Cela peut se faire par le biais d’une Déclaration de confidentialité interne, que vous reprenez dans le règlement de travail ou que vous diffusez séparément, sur papier ou par voie numérique. Il peut également être indiqué de demander à vos travailleurs de signer cette Déclaration de confidentialité pour indiquer qu’ils en ont pris connaissance.

Cela nécessitera parfois un peu de créativité, mais avec un peu de bonne volonté, chaque organisation est capable de présenter clairement les traitements subis par les données personnelles, et pour quels motifs. La transparence est une exigence de base.

La protection des données l’est aussi ; c’est ce que nous allons expliquer au chapitre suivant. Qu’entend le RGPD par mesures de protection adéquates pour les données à caractère personnel. Cela pourrait être un défi de taille pour de nombreuses entreprises…

6. Protection des données à caractère personnel

6.1 Une protection adéquate des données à caractère personnel

Jusqu'à ce point, nous avons surtout évoqué les directives RGPD relatives au traitement des données à caractère personnel. Sous quelles conditions ces données peuvent-elles être traitées ? Comment veiller à une bonne communication avec les personnes concernées ? Toutefois, le RGPD prévoit également que vous devez suffisamment protéger ces données contre les risques, pendant leur traitement mais aussi en dehors.

L'obligation de protection des informations[20] existait bien sûr déjà dans la législation antérieure. La nouveauté, dans le RGPD, est que le responsable du traitement est responsable, au même titre que toute personne traitant les données à la demande d'un responsable.

Afin de mieux comprendre comment vous pouvez respecter cette obligation, nous devons nous pencher un instant sur ce qu'est la protection des informations. De grandes organisations ou entreprises qui traitent systématiquement des données confidentielles de leurs clients, sont évidemment familières du sujet. Il existe plusieurs normes pour la protection des informations, et ISO 27001 est assurément la plus connue. Ajoutez à cela un arsenal de documents stratégiques, de procédures et d'instructions, afin de soutenir les organisations et leur management. Il s'agit véritablement d'une « science » en soi. Nous ne pouvons cependant pas ne pas en parcourir les principes de base.

[20] Article 24.2 en 25; Article 32

Vous devez avant tout savoir contre quelles menaces protéger les données à caractère personnel, tout comme d'autres données confidentielles. À cet égard, l'acronyme CIA – toute ressemblance avec la fameuse agence américaine est fortuite – est souvent utilisé. CIA renvoie dans le cas présent à Confidentiality – Integrity – Availability. La protection des informations garantit la confidentialité, l'intégrité et la disponibilité des données.

- Garantir la **confidentialité** des données, c'est veiller à ce que les données ne deviennent pas publiques et ne se retrouvent pas entre les mains de personnes auxquelles elles ne sont pas destinées. Nous connaissons tous les exemples frappants de centaines de milliers de données de cartes de crédit volées ou de documents confidentiels rendus publics par des pirates informatiques. Mais il existe également des fuites de données à plus petite échelle : une lettre déposée dans la mauvaise boîte aux lettres ou un e-mail envoyé par erreur à un mauvais destinataire.
- La protection de l'**intégrité** des données, c'est veiller à ce que les données ne puissent pas être modifiées ou supprimées à tort. La falsification peut constituer une fraude. Les pirates peuvent manipuler les données. Toutefois, les modifications involontaires résultent le plus souvent d'erreurs humaines dans les logiciels ou lors de la configuration des systèmes ou des applications.
- Enfin, il faut pouvoir garantir la **disponibilité** des données. Des mesures telles que des copies de sauvegarde (back-up) ou un plan de récupération après sinistre doivent permettre d'éviter la perte de données ou leur non-disponibilité au moment opportun.

Un programme de sécurité informatique vous aidera à entreprendre systématiquement les démarches nécessaires. Vous devez connaître les risques spécifiques encourus par les informations, et essayer de les éliminer, de les réduire ou d'en atténuer l'impact.

Le RGPD ne précise pas quelles sont les mesures à prendre pour assurer une protection adéquate des données. Et c'est assez logique, car la bonne méthode dépend de nombreux facteurs. D'une part, les risques ne sont pas toujours les mêmes :

- La nature des données (catégories spéciales, données sensibles ou données d'identification par rapport à des données quasi publiques) et leur quantité déterminent l'impact d'une éventuelle fuite de données.
- La nature du traitement elle-même peut comporter certains risques. Il convient par exemple d'accorder une attention particulière aux analyses automatiques des données sur lesquelles reposent des décisions.
- L'échange et le transport de données peuvent comporter des risques supplémentaires.
- Le recours à des tiers pour le traitement peut constituer une menace supplémentaire.
- En dehors de l'Europe (ou plutôt en dehors de l'EEE), la protection n'est pas la même.
- Le délai de conservation des données peut également jouer un rôle.

D'autre part, la science et la technologie évoluent en permanence. Ce qui constitue une protection adéquate aujourd'hui ne le sera peut-être plus dans deux ans.

Cela revient donc à un fameux exercice d'équilibriste. Les coûts et les efforts pour prendre certaines mesures doivent être proportionnels à la nature des données et aux dommages pouvant survenir en cas de problème.

Les grandes organisations utilisent déjà toute une série de procédures. Elles formulent une politique relative à la protection des informations et ont établi un système de gestion. Elles répertorient les risques et évaluent s'ils sont acceptables. Elles rédigent des procédures et des instructions. Elles effectuent des contrôles et font auditer leur système. Elles analysent les incidents et tirent des leçons de leur fonctionnement actuel pour l'améliorer dans le futur. Toutes ces démarches sont par exemples reprises dans les normes ISO 27001.

Si vous disposez déjà d'un bon système de gestion, il ne vous reste pas grand chose à faire pour vous mettre en règle par rapport au RGPD en ce qui concerne la protection des informations. Vous devez évidemment veiller à ce que toutes les données à caractère personnel soient classifiées « confidentielles » et à ce que les procédures de traitement des données confidentielles y soient applicables. Il est en outre fort probable que d'autres procédures soient nécessaires pour mieux régler les traitements spécifiques subis par les données à caractère personnel. Mais pour le reste, le cadre général est applicable.

Le défi est bien plus grand pour une entreprise ou une organisation qui n'est pas familiarisée avec la protection des informations. Plus loin dans ce document, nous tenterons de vous donner quelques conseils quant à la façon d'aborder la protection des informations dans une petite organisation. Comment, en faisant preuve de pragmatisme et de bon sens, élaborer des procédures réalisables et prendre des mesures pour réduire au strict minimum le risque d'incidents impliquant des données à caractère personnel ? Et comment démontrer que vous avez agi de façon adéquate ?

6.2 Analyse des risques liés aux données à caractère personnel

Le RGPD insiste beaucoup sur l'obligation, pour chaque responsable ou personne qui traite des données à caractère personnel, d'offrir une protection efficace pour la confidentialité, l'intégrité et la disponibilité des données. Il n'est pas nécessaire de compter des spécialistes dans vos rangs pour respecter cette obligation, il est parfaitement possible d'entreprendre les mêmes étapes de manière simplifiée.

Le point de départ de toutes les mesures consiste en une analyse des risques[21]. Cela peut sembler ardu et lourd, mais ce n'est pas forcément le cas. Prenez votre registre des traitements de données et procédez par étapes. Posez-vous quelques questions ciblées. Ajoutez deux colonnes à votre registre (voir chapitre 3) et formulez-y les risques liés à chaque traitement spécifique et les mesures qui vous permettront de limiter ces risques.

Voici quelques exemples simples, que vous trouverez aussi sans doute dans votre registre. Vous disposez de coordonnées de personnes auxquelles vous envoyez de temps à autre de l'information sur vos produits et services. Vous avez évidemment leur nom et leur adresse, mais aussi le nom de leur entreprise, leur fonction et peut-être des informations relatives à leurs études, leurs loisirs et leurs centres d'intérêt. À côté de cela, vous avez une foule d'informations sur votre personnel, dont les CV et les rapports des évaluations annuelles. Vous communiquez chaque mois à votre secrétariat social qui a pris congé ou a été malade à quel moment. Vous devez connaître la composition familiale des membres de votre personnel, car le précompte professionnel en tient compte. Vous avez peut-être des caméras de surveillance qui filment votre personnel et les visiteurs qui entrent et sortent. Et ce ne sont là que quelques exemples. Il n'existe pas d'environnement qui ne traite aucune donnée à caractère personnel.

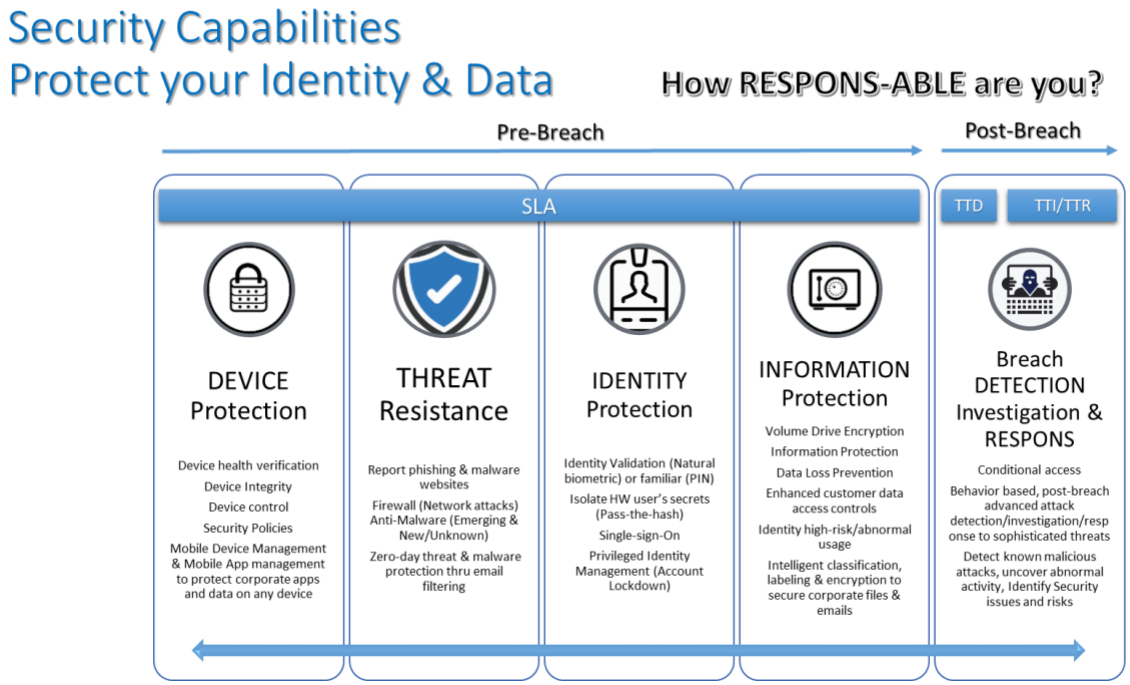
Quels sont les risques pour la sécurité de ces informations ? Cela dépend beaucoup de l'endroit où vous conservez les données ou, dans notre jargon, de la « technologie utilisée ».

- Si vous travaillez avec des dossiers sur papier, ces dossiers et fichiers sont-ils ouverts et exposés sur votre bureau ou sous clé dans une armoire ? Il est important de savoir qui a accès à votre bureau et qui peut ouvrir cette armoire. Fermez-vous la porte quand vous partez ? Rangez-vous votre bureau ?
- S'il s'agit d'un fichier informatique, les questions sont en fait les mêmes, mais les réponses sont plus complexes. Vous travaillez peut-être localement sur un ordinateur portable. Est-il protégé par un mot de passe ? Êtes-vous le seul à connaître ce mot de passe ? Avez-vous enregistré les informations confidentielles dans un dossier lui-même protégé par un mot de passe ? Si vous emportez votre ordinateur portable en dehors de l'entreprise, est-il protégé ? Le laissez-vous parfois dans la voiture ? Où le rangez-vous chez vous ?

[21] Article 32; Article 35-36 : Recital 75-76, 84, 89-95

- Si les données ne sont pas enregistrées localement, mais sur un serveur, la situation est à nouveau différente. Tous les utilisateurs du serveur ont-ils accès à toutes les données ? Est-ce vraiment nécessaire ? Le serveur ne peut-il pas être scindé en zones, avec des autorisations spécifiques attribuées aux différents utilisateurs ou groupes ? Faites-vous un back-up du serveur ? Où ce back-up est-il conservé ? Est-ce qu'une entreprise informatique se charge de la maintenance du parc de serveurs ? Cette entreprise a-t-elle accès à toutes les données ? Etes-vous convenu(e) avec eux de ce qu'ils peuvent faire et ne pas faire, même s'ils ont en fait tous les droits (parce qu'ils en ont besoin pour s'acquitter de leur tâche) ?
- Vos données sont peut-être enregistrées dans le cloud. Où se trouvent-elles et qui y a accès ? Quelles sont les garanties du cloud provider ? Les données sont peut-être enregistrées à l'étranger, voire hors de l'EEE, donc hors de la protection du RGPD. La transmission des données est-elle sécurisée ?
- Les images des caméras de sécurité sont-elles enregistrées et conservées ? Combien de temps les gardez-vous ? Qui peut les visionner et dans quelles circonstances sont-elles réellement visionnées ?

Comme ces questions le suggèrent, vous pouvez, pour chacune de ces situations, prendre des mesures pour réduire les risques d'infraction. Les exemples montrent également que les risques varient en fonction du contenu précis des fichiers. S'il s'agit de simples coordonnées, une atteinte à la confidentialité n'aura pas un impact important. Par contre, il en va différemment s'il s'agit de certaines données à caractère personnel. Si vous travaillez dans le domaine de la santé, par exemple, et conservez des données sensibles de patients ou de clients – des données médicales, par conséquent – une protection beaucoup plus stricte est nécessaire, car une atteinte à la confidentialité ou à l'intégrité de ces données pourrait avoir des conséquences beaucoup plus graves. En fonction de l'ampleur de votre base de données, l'impact est également plus grand, car les données concernent un plus grand nombre de personnes. Les mesures que vous prenez pour chacun des risques énumérés doivent toujours être proportionnelles à l'évaluation du risque.



Il est dès lors logique que le RGPD impose d'importantes obligations aux personnes qui utilisent des catégories spéciales de données et aux organisations dont l'activité principale est le traitement de données à caractère personnel. Dans certains cas, il convient de réaliser une Data Privacy Impact Analyse (DPIA) formelle et de la présenter à l'Autorité de protection des données avant le début du traitement.

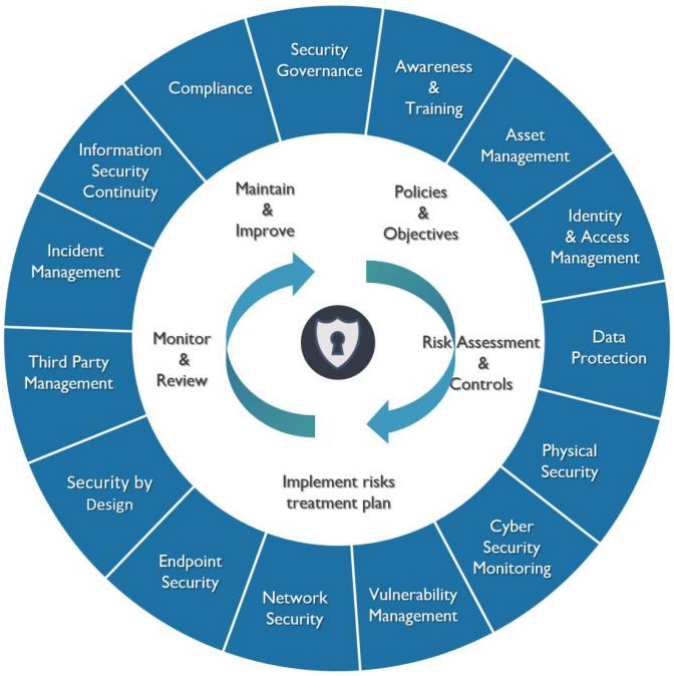
Indépendamment de cela, nous recommandons à toute entreprise ou organisation d'effectuer, grosso modo, le même exercice. Afin de pouvoir démontrer à tout moment que vous gérez les données à caractère personnel en connaissance de cause, il est indiqué de consigner les résultats de cette analyse. Des logiciels spécialisés et des méthodologies spécifiques peuvent vous y aider, mais dans bon nombre de cas, ce n'est pas nécessaire. Les deux colonnes évoquées plus haut, ajoutées à un simple registre des traitements des données, vous apportent déjà beaucoup, pour autant qu'elles soient soigneusement remplies.

Approfondissons à présent les différents domaines dans lesquels vous pouvez prendre des mesures de protection pour conserver et traiter en toute sécurité les données à caractère personnel.

6.3 Mesures pour la protection des données à caractère personnel

Nous avons évoqué l'importance d'une analyse d'impact. L'ampleur du risque détermine les mesures de sécurité[22] nécessaires.

Il est évident qu'une petite entreprise ne devra pas agir de la même façon qu'une grande organisation. Il est toutefois intéressant de présenter brièvement la trame d'un système tel qu'ISO 27001, car la réflexion et la logique à suivre restent les mêmes.



Les premiers éléments d'ISO 27001 concernent la **politique** et l'**organisation**. Vous devez formuler les points de départ de votre politique. Deux phrases peuvent suffire. L'utilisation des données à caractère personnel doit être légale et avoir un but légitime. Vous devez protéger les données de façon adéquate. La constitution de cette politique incombe au dirigeant d'entreprise. Il peut déléguer cette tâche, mais il demeure responsable et doit évaluer chaque année l'efficacité de sa politique.

[22] Article 32 : Recital 77-78

Viennent ensuite des **mesures dans plusieurs domaines**, qui doivent être interprétées de l'une ou l'autre manière en fonction du type d'entreprise ou d'organisation :

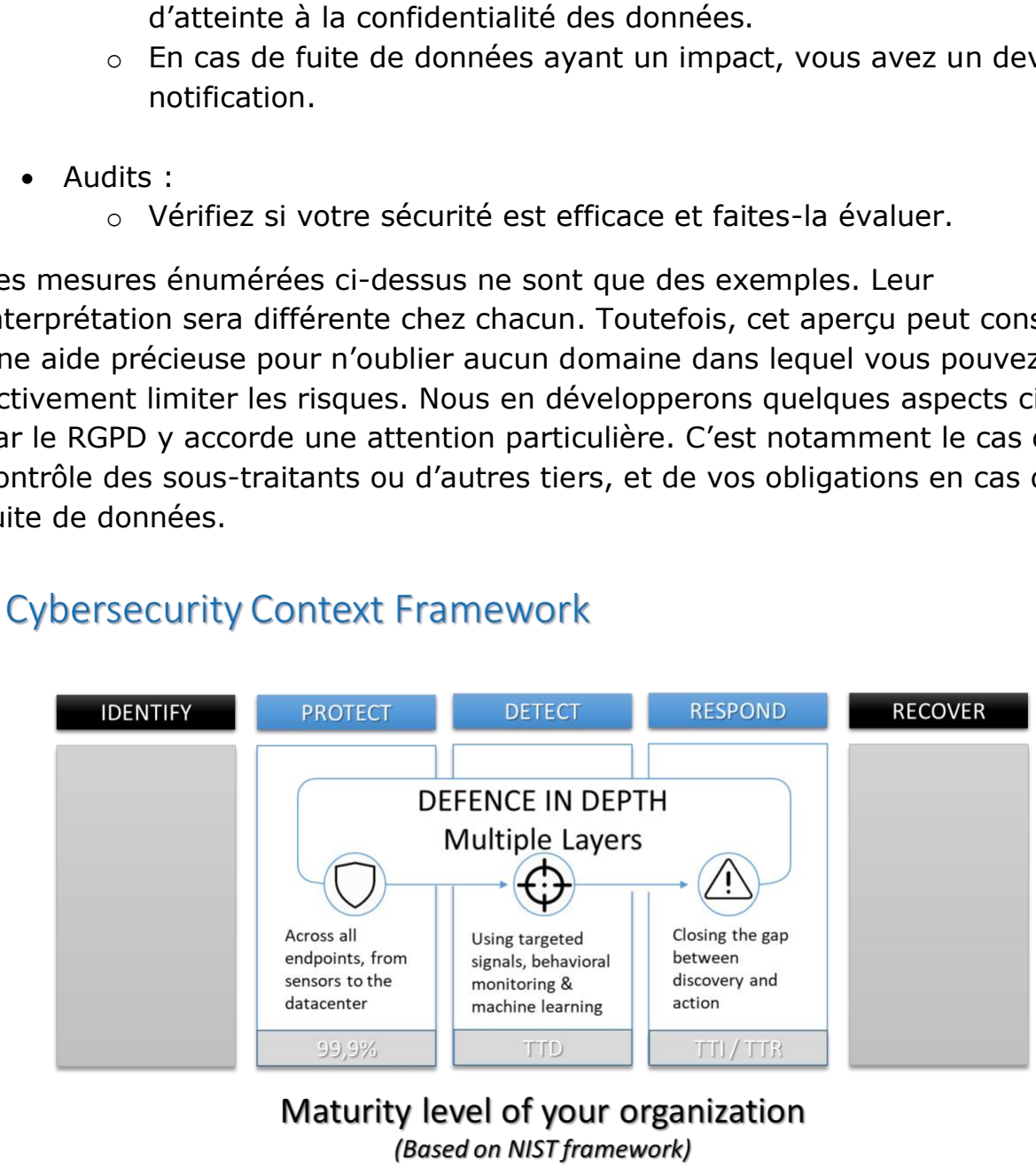
- Personnel (sélection / formation & sensibilisation / départ) :
    - Lors de l'engagement, accordez de l'attention au sens des responsabilités de vos collaborateurs.
    - Si vous traitez des données sensibles, demandez un extrait de casier judiciaire (que vous devez ensuite traiter lui aussi comme une information sensible !)
    - Reprenez une clause de confidentialité dans le contrat de travail. Il peut s'agir d'une simple phrase : « Toutes les données à caractère personnel utilisées par le travailleur dans son environnement de travail sont confidentielles et ne peuvent être utilisées que dans le cadre de la tâche réalisée ».
    - Formez régulièrement vos collaborateurs (et vous-même) au sujet de la protection des données.
    - Veillez à ce qu'un collaborateur qui quitte l'entreprise n'ait plus accès aux données et ne conserve pas de ressources de l'entreprise (en ce compris des données sur papier ou au format numérique).
- Classification et utilisation de ressources :
    - Établissez un registre des traitements subis par les données et complétez-le par une analyse des risques.
    - Faites attention aux supports amovibles (comme les clés USB contenant des données) et aux appareils transportés. Évitez que les données se retrouvent entre de mauvaises mains.
- Droits d'accès :
    - Paramétrez des mots de passe suffisamment complexes et veillez à ce qu'ils restent strictement personnels.
    - Vos collaborateurs ne doivent avoir accès qu'aux informations nécessaires à l'exercice de leur fonction. Travaillez à cet effet avec des « groupes de fonction ».
    - Limitez les droits d'administrateur sur les systèmes aux personnes compétentes.
- Cryptographie :
    - Le RGPD promeut explicitement le cryptage des données comme mesure de protection. C'est particulièrement indiqué pour l'échange de données et la conservation de longue durée.
    - Exemples : protocole https sur les sites web, protocole sftp pour le transfert de données, cryptage des e-mails, etc.
    - Un partenaire ICT peut vous aider. Mais n'oubliez pas de conclure de bons accords avec ce partenaire, afin qu'il ne devienne pas un nouveau risque pour la sécurité !

- Protection physique :
    - Activez un écran de veille sécurisé sur votre ordinateur lorsque vous n'êtes pas à votre poste.
    - En fin de journée, ne laissez pas traîner de documents (« clean desk »).
    - Établissez un plan de verrouillage des bureaux (et des armoires).
    - Vous avez peut-être besoin de grillages, d'un système d'alarme, de caméras de surveillance ou d'un système de badges (et de zones distinctes dans vos bâtiments).
    - Protégez vos appareils contre les coupures de courant. Évitez les pannes.
    - Accompagnez toujours vos visiteurs et communiquez-leur vos directives en matière de confidentialité.
    - Accordez une attention particulière aux locaux renfermant des données sensibles, comme une salle de serveurs ou une salle d'archives avec des dossiers confidentiels.
- Protection du réseau :
    - Protégez votre réseau contre les risques extérieurs à l'aide d'un pare-feu, d'un antivirus et d'une filtration du contenu.
    - Scindez les plus grands réseaux en zones. Évitez les pannes des systèmes. Contrôlez et consignez les activités sur le réseau.
- Mesures de sécurité pour le développement d'applications ou de systèmes :
    - Séparez l'environnement de test et la production, et rédigez un règlement pour les transferts.
    - Réfléchissez toujours au préalable à la sécurité des systèmes et testez-la avant utilisation.
- Contrôle sur les traitements par des tiers :
    - Convenez de dispositions contractuelles sur la sécurité et la confidentialité des données avec vos fournisseurs.
    - Évaluez le fonctionnement de votre fournisseur et assurez-en un suivi régulier.
- Continuité :
    - Limitez le risque de panne des systèmes par une bonne maintenance et par la redondance.
    - Prévoyez des copies de sécurité des données et établissez un plan de restauration de vos systèmes en cas de problèmes graves.

- Gestion des incidents :
    - Enregistrez toujours les incidents qui comportent un risque d'atteinte à la confidentialité des données.
    - En cas de fuite de données ayant un impact, vous avez un devoir de notification.

- Audits :
    - Vérifiez si votre sécurité est efficace et faites-la évaluer.

Les mesures énumérées ci-dessus ne sont que des exemples. Leur interprétation sera différente chez chacun. Toutefois, cet aperçu peut constituer une aide précieuse pour n'oublier aucun domaine dans lequel vous pouvez activement limiter les risques. Nous en développerons quelques aspects ci-après car le RGPD y accorde une attention particulière. C'est notamment le cas du contrôle des sous-traitants ou d'autres tiers, et de vos obligations en cas de fuite de données.



6.4 Maîtrise du risque des sous-traitants & Convention relative au traitement des données à caractère personnel

Comme nous l'avons vu, l'un des domaines à risque – pour lequel il faut donc prendre des mesures de sécurité – est le recours aux sous-traitants[23]. Le RGPD est très clair à ce sujet. Un sous-traitant est responsable et a plusieurs obligations, mais le donneur d'ordre qui fait appel à lui pour traiter les données conserve toujours la responsabilité finale. Il doit bien choisir son sous-traitant et se charger de l'application légale. Le donneur d'ordre doit formuler et encadrer clairement la mission, et contrôler le respect des instructions et de la législation, en particulier en matière de sécurité.

Ces dernières années, les spécialistes en sécurité des informations ont de plus en plus pris conscience du risque représenté par les sous-traitants. Rien d'étonnant dès lors à ce que le RGPD y accorde une attention toute particulière.

Des démarches doivent être entreprises aux différents stades de la collaboration.

Lors de la **sélection des fournisseurs**, il convient de ne jamais perdre de vue l'aspect « confidentialité des données et sécurité des informations ». Le responsable doit s'assurer qu'un sous-traitant auquel il souhaite recourir connait ses obligations et les respecte de manière adéquate. Il n'existe pas de certification « RGPD compliant », et pour autant que je sache, il n'y a actuellement rien de concret en ce sens. Les instances officielles encouragent les associations professionnelles à rédiger des codes de conduite, grâce auxquels les signataires peuvent démontrer qu'ils connaissent les règles et veulent les suivre. Il y a aussi de plus en plus de questionnaires, utilisés lors des procédures de sélection et dans les dossiers d'adjudication. Il existe des certificats relatifs à la sécurité des informations, mais ils ciblent fortement les grandes organisations et ne sont pas envisageables pour toutes les entreprises ou organisations. Informez-vous toujours auprès de votre futur fournisseur sur sa politique en matière de sécurité des informations et sur les mesures qu'il applique. Tenez-en compte dans vos critères de sélection. Et n'oubliez pas de conserver la documentation récoltée.

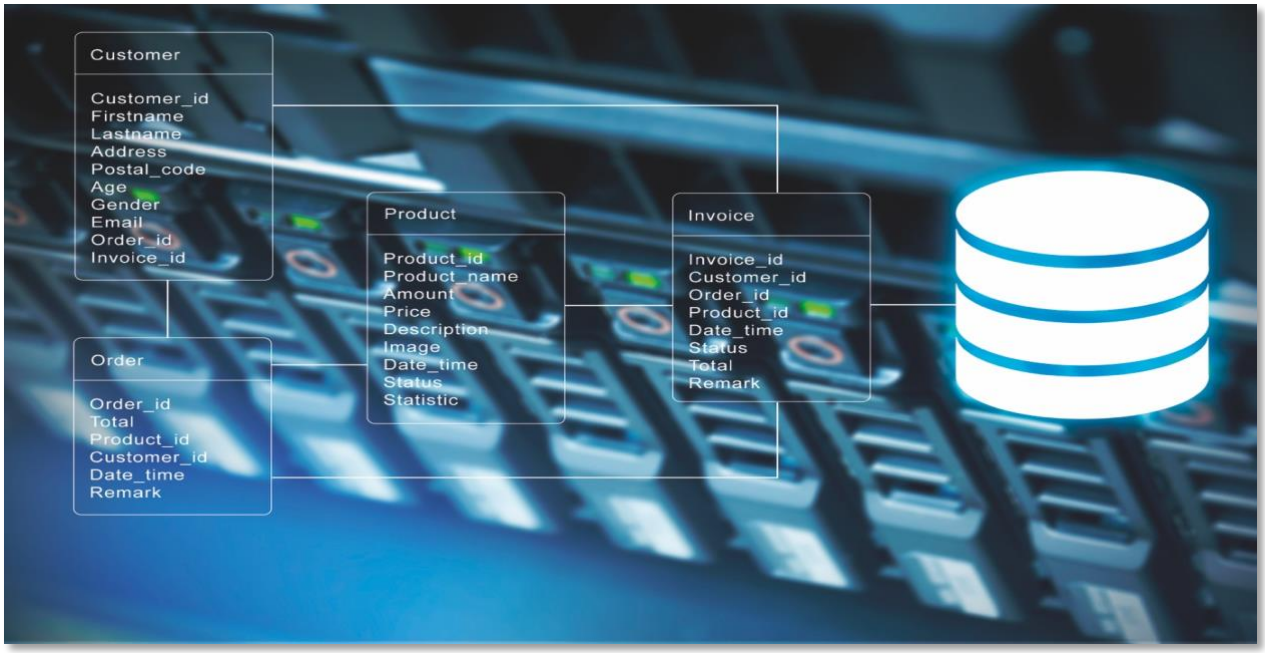
[23] Article 28-29 : Recital 79 en 81

Lors de **l'attribution d'une mission**, il est important de passer les accords contractuels nécessaires en matière de confidentialité des données. La forme toute indiquée à cet égard est la convention de traitement des données à caractère personnel. Il peut s'agir d'une annexe à un contrat ou d'un accord de coopération. Les dispositions peuvent également être intégrées aux conditions générales. Si vous collaborez avec un sous-traitant depuis longtemps, vous devez malgré tout veiller à ce que le RGPD soit respecté. Comme la législation antérieure insistait moins sur les obligations du sous-traitant, il est recommandé de rédiger une version adaptée.

Une convention relative au traitement des données à caractère personnel doit toujours comporter les clauses suivantes :

- Les rôles de responsable et de sous-traitant sont attribués respectivement au donneur d'ordre et à l'exécutant/fournisseur/sous-traitant.
- Le sous-traitant ne peut utiliser les données que conformément aux instructions formelles (de préférence écrites) du responsable.
- Le sous-traitant respecte la confidentialité des données et impose cette obligation à tous ses collaborateurs, qu'ils soient fixes ou temporaires.
- Le sous-traitant doit mettre en place une sécurité adéquate des données et veiller à ce qu'elles soient et restent disponibles pour la mission (à l'aide de back-ups et de mesures assurant la continuité).
- En cas de fuite de données, le responsable doit être informé immédiatement. Une procédure permettant de limiter l'impact de la fuite doit exister. Le sous-traitant ne peut en aucun cas en informer lui-même l'Autorité de protection des données ou les personnes concernées.
- Au terme de la mission (ou du délai de conservation établi), le sous-traitant doit supprimer les données de manière définitive, et prouver cette suppression. Si cela est applicable, il doit aussi restituer les données au donneur d'ordre.
- Les données ne peuvent être transmises à des tiers qu'avec l'autorisation du donneur d'ordre. Si le sous-traitant fait lui-même appel à un autre sous-traitant – moyennant accord du donneur d'ordre – il doit veiller à ce que ce dernier respecte les mêmes obligations contractuelles.
- Le sous-traitant autorise le donneur d'ordre à contrôler la bonne exécution de la mission par le biais d'évaluations ou d'audits.

Si vous êtes dans une petite organisation, vous pouvez sans doute profiter du travail de vos plus gros fournisseurs, qui ont probablement déjà rédigé une convention relative au traitement des données à caractère personnel pour la soumettre à leurs clients. Dans notre organisation, nous avons en tout cas veillé à ce que nos clients ne doivent pas tous fournir des efforts pour chercher quels sont les droits et obligations respectifs du donneur d'ordre et du sous-traitant. Nous avons rédigé une convention que nous avons voulue équilibrée et que nous présentons en temps opportun à nos clients. Nous nous engageons en tant que sous-traitant à appliquer le RGPD dans sa totalité.



Enfin, le responsable est tenu de s'assurer que le contrat est correctement exécuté par le sous-traitant. Dans le cas d'un contrat à plus long terme, il devra effectuer un **contrôle** régulier. À cet égard, il est important de reprendre le droit d'audit dans les accords contractuels. Cela ne veut pas dire pour autant qu'un responsable auditera chaque année chaque sous-traitant. Les grandes organisations le font – souvent au déplaisir de leurs fournisseurs – auprès des sous-traitants qui, selon elles, courent un risque élevé de causer des infractions ou chez lesquels une infraction aurait un impact considérable. Dans de nombreux cas, le fait de s'assurer que la certification obtenue par le fournisseur est renouvelée chaque année peut suffire. Vous pouvez également faire compléter et signer un questionnaire par le fournisseur, dans lequel il énumère les mesures prises.

Comme avec tous les aspects de cette législation, les actions à entreprendre doivent une fois encore être évaluées par rapport au risque de survenance d'un incident et à l'impact que cela pourrait avoir.

7. Fuites de données

7.1 Gestion des incidents

Dans les chapitres précédents, nous avons graduellement évoqué la prise de mesures adéquates pour protéger correctement les données à caractère personnel que vous traitez. Vous devez envisager les risques encourus et prendre diverses mesures pour les éliminer, si possible ou, à défaut, les réduire. Vous faites appel à des sous-traitants ? Vous devez alors veiller à ce qu'ils soient aussi bien organisés que vous. Les choses peuvent toutefois mal tourner. Nous allons évoquer ici les actions requises en cas d'incident.

Le terme « fuite de données », ou « data breach[24]» en anglais, est utilisé pour toute situation impliquant la perte, la modification injustifiée ou la publication de données confidentielles, ou encore le fait que des données confidentielles se retrouvent entre de mauvaises mains. Le RGPD prévoit dans ce cas que le responsable du traitement des données à caractère personnel signale sans délai inutile les fuites de données pouvant constituer une atteinte à la vie privée des personnes concernées. Si le risque de dommage est important, les personnes concernées doivent également être averties.

[24] Article 4.12; Article 33-34 : Recital 75 en 87-88

Avant de m'engager dans une discussion quant au fait qu'il faille signaler ou non une fuite de données à l'Autorité de protection des données, je souhaiterais d'abord me concentrer sur la gestion de l'incident à proprement parler. Votre première obligation, en tant que responsable et personne en charge du traitement des données, est d'éviter les incidents et d'en limiter autant que possible l'impact si vous n'avez pas pu les éviter.

La première préoccupation est de **constater les incidents le plus vite possible**. Plusieurs outils de réseau peuvent être utilisés à cet effet, afin de mettre en lumière un comportement anormal sur le réseau, de détecter des virus ou des malwares ou de filtrer le contenu. Des collaborateurs vigilants peuvent eux aussi constater et signaler des infractions. C'est la raison pour laquelle il est important d'organiser régulièrement des formations et des actions de sensibilisation pour le personnel, afin que chacun sache clairement quand une situation est anormale ou préoccupante. Il est également important que tous les collaborateurs sachent à qui faire appel en cas d'incident.

Deuxièmement, vous devez entreprendre dès que possible les démarches pour **enrayer l'incident ou en limiter l'impact**. Tous les collaborateurs doivent respecter plusieurs règles. S'ils trouvent des informations à un endroit inapproprié, ils doivent les supprimer ou en informer un responsable. Il peut s'agir de supports physiques, mais aussi de fichiers sur le réseau. Ils doivent également donner l'alerte s'ils rencontrent des étrangers non accompagnés dans une zone sécurisée. Et ainsi de suite. Si des alarmes indiquent un piratage ou une infection des systèmes, les gestionnaires de ces systèmes devront les examiner au plus vite et peut-être les désactiver de manière préventive.

En cas de doute, il est préférable d'arrêter un traitement ou d'empêcher le transport des données traitées jusqu'à ce que vous sachiez clairement s'il y a effectivement un problème, et dans quelle mesure les données traitées sont encore correctes. Cela permet souvent d'éviter qu'un incident ne se transforme en fuite de données. Tant que des données traitées à mauvais escient ne sont pas diffusées ou rendues publiques, il n'y a pas d'infraction, et donc pas d'impact. Au sens strict, il n'est pas encore question d'une fuite de données.

Ensuite, et éventuellement en parallèle, vous pouvez lancer une **analyse** des faits. D'une part, il faut établir la **cause du problème**. Vous pourrez ensuite réfléchir aux **améliorations** dans l'organisation, les systèmes ou les applications, et dans le mode de travail de vos collaborateurs, pour éviter que l'incident ne se reproduise.

D’autre part, il faut examiner l’**impact réel ou éventuel** de l’incident. Y a-t-il des risques pour la confidentialité et l’intégrité des données ? S’agit-il (en partie) de données à caractère personnel ? Quelles peuvent-être les conséquences de cette infraction ? Dans de nombreux cas, il vous faudra du temps pour savoir quelle quantité de données a été impactée et combien de personnes sont concernées. Souvent, vous ne saurez pas non plus d’emblée s’il y a véritablement un risque d’impact, ni quelle peut être l’ampleur des dommages.

Ce n’est que lorsque vous aurez une réponse à toutes ces questions qu’il vous sera possible de faire le bon choix quant à la nécessité de **signaler** la fuite de données à l’Autorité de protection des données ou aux personnes concernées. Le quand et le comment de ce signalement seront abordés dans le prochain article.

Par ailleurs, chaque incident doit être **consigné dans un registre interne**. Qu’il s’agisse d’une véritable infraction ou d’un quasi-accident, il faut toujours analyser l’incident. Ces informations sont importantes pour évaluer les procédures et les directives existantes, et vérifier si les mesures prises offrent une protection suffisante contre les risques éventuels. Les causes d’un incident doivent être consignées, au même titre que les actions visant une amélioration. En assurant un suivi systématique, vous améliorerez systématiquement la sécurité de votre organisation.

Dans les cas extrêmes, une fuite de données peut être catastrophique. Une organisation peut être confrontée à des problèmes de communication dantesques suite à une fuite de données très sensibles à propos d’un grand nombre de personnes. Il arrive que la fuite de données sorte des murs de l’organisation et que la presse en soit informée. En pareil cas, il est bon de pouvoir retomber sur des scénarios de **communication de crise** préalablement établis. Si votre organisation est couverte par une assurance couvrant les risques de cyber-sécurité, votre compagnie d’assurance devrait pouvoir vous aider.

Si vous soupçonnez que l'incident est d'origine criminelle, vous devez veiller à constituer un **dossier juridique** à temps. Il est parfois important de réaliser un back-up rapide des systèmes au moment de la découverte de l'incident ou de conserver les fichiers log, avant que ces informations ne soient perdues ou modifiées par les démarches entreprises pour résoudre l'incident. Il est évident qu'une telle étape ira parfois à l'encontre de ce qu'il convient de faire rapidement pour limiter le problème existant.

Si la police ou la justice intervient, ne perdez jamais de vue ce que vous pouvez et ne pouvez pas faire de votre propre chef, surtout si vous êtes en charge du traitement des données. Faites appel au responsable dès que possible. Si les autorités vous obligent à fournir des informations, vous devez toujours veiller à les protéger au mieux et à ne pas exposer de données (par exemple d'autres personnes concernées) si cela n'est pas nécessaire à l'enquête.

Il est judicieux de bien documenter ces démarches successives, afin que chacun dans l'organisation les connaisse et agisse en fonction. Cela peut également s'avérer utile pour démontrer que vous prenez le respect des obligations du RGPD très au sérieux.

7.2 Obligation de notification

Lorsqu'une fuite de données est constatée, la première préoccupation est d'en limiter l'impact autant que possible. C'est ce dont nous parlions précédemment. Indépendamment de cela, le RGPD exige qu'en tant que responsable du traitement des données, vous signaliez[25] sans délai aux autorités compétentes toute fuite de données présentant un risque d'atteinte à la confidentialité des données. Si le risque est élevé, les personnes concernées doivent être informées elles aussi.

Cette obligation suscite de nombreuses questions. Quand un incident relatif à la sécurité des informations est-il effectivement une fuite de données ? Quand une fuite de données présente-t-elle un risque d'atteinte à la vie privée ? Quand est-il question de risque accru de dommage ? À partir de quel moment êtes-vous informé(e), et de combien de temps disposez-vous pour le signalement ?

Si l'incident touche des données à caractère personnel, avertissez d'office votre Data Protection Officer. Si votre organisation ne dispose pas d'un DPO officiel, une personne doit en tout cas endosser ce rôle. C'est en effet le DPO qui est le mieux à même de déterminer le poids des données et l'impact qu'une atteinte pourrait avoir pour les personnes concernées et pour le responsable du traitement (votre organisation ou peut-être votre client, si vous traitez les données pour quelqu'un d'autre). Le DPO conseille l'organisation quant à la communication à mettre en œuvre. Il est le mieux placé pour décider de la nécessité d'une déclaration à l'Autorité de protection des données, et des informations à transmettre.

Conseil:

Les trois questions suivantes peuvent vous aider à déterminer si une déclaration est nécessaire :

- Y a-t-il effectivement une fuite de données ? Si un incident comportait un risque de fuite sans qu'aucune donnée n'ait été rendue publique ou ne se soit retrouvée entre de mauvaises mains, cela reste un incident. Consignez-le dans votre liste interne d'incidents, mais une déclaration n'est pas nécessaire.

[25] Article 33 en 34 : Recital 85-88

- Il n’y a vraisemblablement aucun risque ? Si les données se sont retrouvées en dehors des zones sécurisées ou de votre organisation, il est toujours possible que grâce aux mesures de protection, il n’y ait aucun risque. Les données peuvent par exemple être correctement cryptées, et ne pourront donc pas être utilisées par des étrangers.
- Le risque de dommage immédiat pour les personnes concernées est-il important ? En cas de fuite de données concernant des cartes de paiement, le risque de dommage financier est réel et les personnes concernées doivent être averties aussi vite que possible afin de pouvoir prendre des mesures. Cela peut également être le cas avec d’autres types de données sensibles. S’il s’agit par contre de données triviales, il est moins urgent d’en informer tout le monde. Le RGPD fait preuve de compréhension pour les situations dans lesquelles il est pratiquement impossible d’informer personnellement toutes les personnes concernées. Dans ce cas, une communication publique suffit.

Le RGPD définit en outre les informations à communiquer dans la déclaration :

- Une description de l’atteinte, avec si possible mention du type de personnes concernées et des catégories de données ;
- Si possible, le nombre approximatif de personnes concernées ;
- Les coordonnées de contact du DPO ou de la personne de contact pour la confidentialité des données chez vous ;
- Les conséquences potentielles de l’atteinte ;
- Les mesures prises par l’équipe en charge de l’incident pour en limiter l’impact.

Certaines parties de ces informations ne sont sans doute pas connues immédiatement et ne sont constatées qu’au terme d’une analyse plus approfondie. Le RGPD stipule également que la déclaration ne doit pas être « immédiate », mais doit bien être « sans retard inutile », la norme étant dans les 72 heures qui suivent la constatation de la fuite de données par le responsable. Moyennant une bonne motivation, la déclaration peut également se faire passé ce délai. Les informations sur l’atteinte peuvent par ailleurs être complétées après la première déclaration.

Si vous n'êtes pas le responsable mais intervenez en sous-traitance, vous devez être particulièrement vigilant(e) en cas de fuite de données. Vous risquez en effet d'outrepasser votre propre champ de responsabilité et de devoir endosser une plus grande responsabilité. La plupart des contrats de traitement stipulent de ce fait clairement qu'un sous-traitant en charge du traitement qui constate une fuite de données doit immédiatement contacter le responsable et ne communiquer en aucun cas directement avec l'Autorité de protection des données ou les personnes concernées. Il est également préférable de laisser la communication avec la presse au responsable. Le législateur prévoit que le responsable dispose, dans des conditions normales, d'un délai de 72 heures. On s'attend toutefois à ce que le sous-traitant contacte le responsable dès que possible. Cela permet à ce dernier d'assurer immédiatement ses obligations. Les contrats imposent souvent au sous-traitant de réagir dans les 24 heures, bien que la loi fasse état de 72 heures.

Il ne sera pas toujours facile de déterminer quelle communication et quelles notifications sont nécessaires. Ne pas signaler une fuite de données est punissable, et le responsable s'expose à des amendes potentiellement très élevées. D'autre part, l'aperçu des notifications de fuites de données est une information publique. Aucune entreprise n'a envie d'y être mentionnée, surtout s'il s'avère par la suite qu'il ne s'agissait pas vraiment d'une fuite de données ou que les données étaient tellement bien protégées qu'il n'y a pas eu de risque de dommage. Avant que cela ne soit tiré au clair, votre image peut avoir été fameusement ternie. À l'inverse, aucune organisation ne veut avoir la réputation de vouloir dissimuler ou étouffer les problèmes graves. À cet égard, l'ouverture et la transparence sont toujours préférables.

Nous devons sans doute nous attendre à des directives des autorités visant à mieux définir les cas où une notification est indiquée ou non. Les spécialistes de la protection de la vie privée s'inquiètent également du risque qu'en cas de doute, des entreprises ne fassent une notification trop rapide pour éviter des amendes, et que de ce fait, les autorités soient submergées de notifications impossibles à contrôler et à traiter. Cela s'est par exemple produit à aux Pays-Bas, où cette obligation de notification est imposée par la loi nationale depuis un certain temps déjà.

Ma recommandation est de consigner systématiquement chaque incident dans la liste interne d'incidents, ce qui constitue par ailleurs une obligation du RGPD. Mentionnez-y les faits constatés, les conséquences et les mesures correctrices prises. Vous pouvez également y documenter l'argumentation en vertu de laquelle vous ne faites pas de notification ou n'informez pas les personnes concernées. Vous pourrez ainsi par la suite démontrer qu'un incident a bien été remarqué et que des mesures adéquates ont été prises. Un tel suivi contribue d'ailleurs grandement à l'amélioration de vos procédures et mesures de protection.

8. Droits de la personne concernée

8.1 Droit à l'information

Nous avons jusqu'ici principalement parlé des obligations qu'entraînait le RGPD pour les entreprises ou les organisations qui traitent des données à caractère personnel. Nous avons surtout examiné la loi selon le point de vue du responsable du traitement des données et du sous-traitant. Le moment est à présent venu d'étendre le champ d'action aux personnes concernées.

L'un des principaux objectifs du RGPD est en effet de définir vos droits en tant que personne individuelle[26] dans le cadre des nombreuses données qui circulent à votre sujet et sont utilisées par autrui. En tant que personne concernée, vous pouvez avoir prise sur ces informations, même si, comme nous allons le voir, vos droits ne sont pas absolus.

L'un des concepts majeurs du RGPD est la **transparence**. Un responsable du traitement des données doit faire preuve d'ouverture envers les personnes dont il traite les données. Vous devez facilement savoir quelles données conserve et traite un responsable du traitement à votre sujet, ce qu'il en fait et pourquoi il a besoin de ces traitements. Il doit pouvoir vous expliquer cela dans un langage simple et intelligible. Dans le chapitre 5 nous avons largement évoqué la façon dont une entreprise ou une organisation pouvaient par exemple fournir ces informations sur leur site web, sous la forme d'une **déclaration de confidentialité**.

C'est principalement lorsqu'un responsable du traitement des données vous demande des données en vue de les enregistrer et de les utiliser qu'il doit veiller à bien vous informer **préalablement** de ses intentions, des conséquences possibles et des risques que vous encourez. Il doit vous faire comprendre clairement que les avantages compensent les inconvénients.

En outre, le responsable du traitement des données doit vous **indiquer ce que vous pouvez faire en cas de question ou de plainte**. Vous devez bénéficier d'un interlocuteur direct au sein de l'organisation. Et le responsable doit vous expliquer que vous pouvez vous opposer au traitement des données en déposant une plainte auprès de l'Autorité de protection des données. Il faut évidemment que votre plainte soit fondée.

[26] Article 12-15; Article 23 : Recital 58-64

Outre le droit à des informations générales, vous avez également, en tant qu'individu concerné, des droits spécifiques en ce qui concerne vos propres données personnelles. Chacun peut s'adresser à un responsable du traitement des données pour **consulter les données que cette entreprise ou organisation conserve à son sujet et les traitements qui en sont faits.** Cela peut sembler une requête simple à résoudre, mais cela peut représenter une montagne de travail pour une organisation. Le fait de pouvoir réagir correctement à de telles demandes nécessite une bonne préparation et une procédure claire, d'autant plus que les personnes concernées ont, selon le RGPD, le droit de recevoir une réponse dans le mois. Soit le responsable doit fournir les informations demandées dans ce délai, soit il doit au moins expliquer de façon plausible pourquoi il a besoin de plus de temps.

Respecter cette obligation ne se fait pas sans difficultés. Tout d'abord, le responsable doit savoir précisément où se trouve quelle information. Pour les fichiers de coordonnées dans une application CRM ou pour les données du personnel dans un système administratif, ce n'est pas trop compliqué. De nombreuses informations sont toutefois réparties dans des informations non structurées, dans des dossiers sur papier ou des fichiers qui ne sont pas gérés dans le cadre de la gestion documentaire ou qui sont gérés localement quelque part par des travailleurs individuels. Ces données sont beaucoup moins faciles à rassembler. Le RGPD stipule en outre explicitement que ce service doit être gratuit, sauf si la demande est manifestement infondée ou exagérée.

Il faut ajouter à cela que ce **droit de consultation est en conflit avec d'autres droits et intérêts**. Le responsable du traitement des données doit par exemple veiller à ce qu'en communiquant des informations à une personne concernée, il n'enfreigne pas en même temps les droits d'une autre personne concernée. Clarifions cela par un exemple. Une organisation ne pourra que très rarement, voire jamais, satisfaire la demande d'une personne de consulter tous les documents ou e-mails dans lesquels elle est mentionnée. En effet, ces documents contiennent également des informations relatives à d'autres personnes concernées, dont la vie privée doit aussi être protégée. Certaines sources d'information contiennent en outre d'autres données confidentielles, dont la divulgation peut porter préjudice aux intérêts de l'entreprise. Dans tous ces cas, il est nécessaire de confronter les différents droits pour aboutir à un point de vue équilibré. De la sorte, il peut arriver qu'il soit impossible d'accéder à la demande d'une personne concernée. En tant que demandeur, vous devez toutefois recevoir une explication motivant le refus du responsable d'accéder à votre requête.

Outre le droit à l'information, le RGPD confère de nombreux autres droits à la personne concernée. Nous les évoquerons dans la section suivante.

8.2 Droits relatifs aux données propres

Nous évoquions le droit à l'information des personnes concernées. Tout responsable du traitement des données doit fournir des informations transparentes sur le type de données qu'il conserve, les traitements qu'il effectue et la finalité visée. En outre, toute personne concernée dispose du droit de demander ses données personnelles.

Les droits de la personne concernée (et donc les obligations du responsable) vont toutefois bien plus loin. Une personne concernée peut également **demander de corriger, compléter ou supprimer les données conservées et traitées à son sujet**[27]. Dans ce cas également, il ne s'agit pas d'un droit absolu, et les possibilités de satisfaire cette demande doivent être confrontées aux autres droits ou obligations légales. Les données à archiver pendant un certain temps à la demande des autorités ne peuvent évidemment être supprimées à la demande d'un individu. Il arrive que des données doivent être conservées longtemps pour respecter toutes les obligations contractuelles. Un responsable du traitement doit même conserver un nombre limité de données pour démontrer qu'il a accédé à la demande de suppression d'une personne.

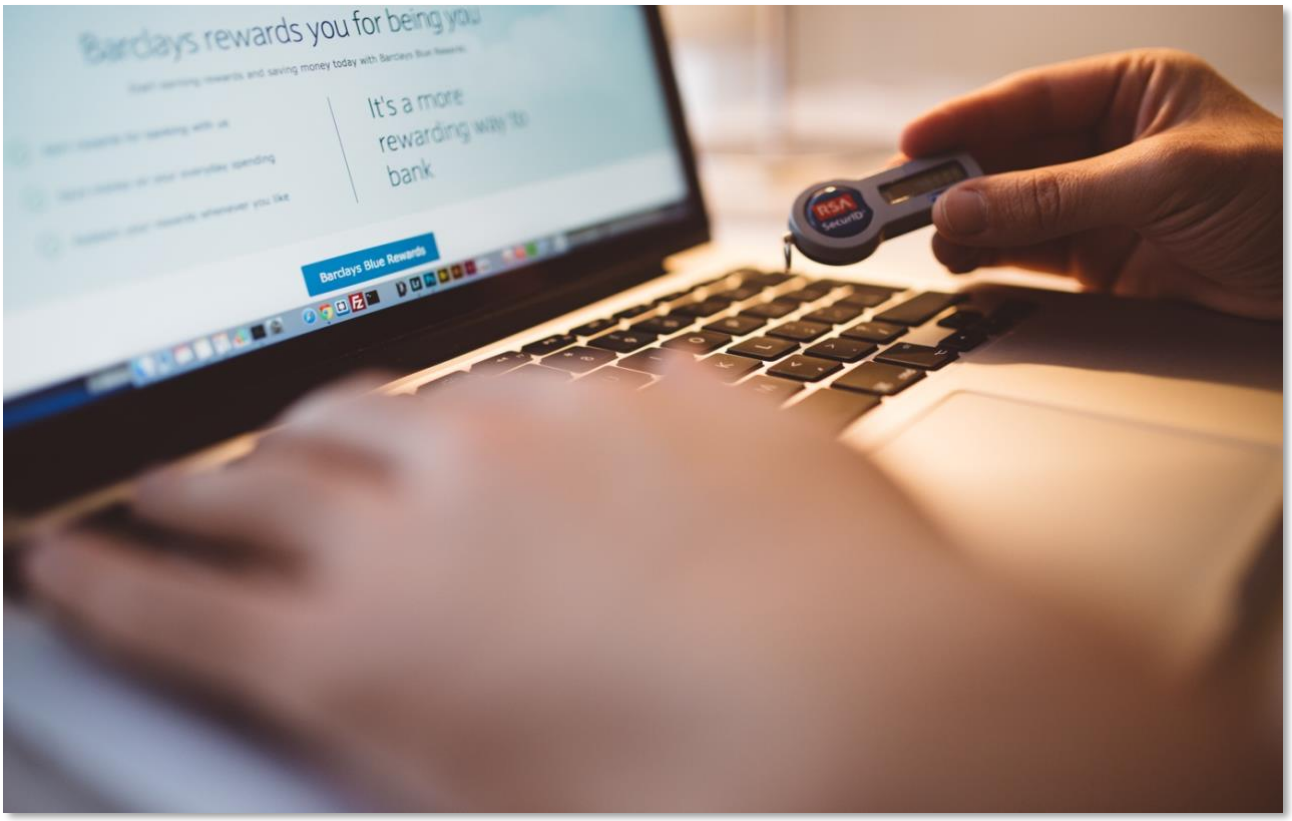
[27] Article 16-23 : Recital 65-73

De même, le droit de corriger les données est évidemment relatif. Un rapport d'évaluation validé ne peut être modifié sans raison à la demande d'un travailleur. Toutefois, il peut exercer ses droits en y ajoutant un commentaire. Les corrections ou les ajouts sont logiques – voire utiles – si les données sont par exemple obtenues via des tiers. Juridiquement, cela devient plus complexe s'il s'agit d'enrichissements apportés par le responsable lui-même, et qui sont peut-être sa valeur ajoutée.

De manière générale, de telles demandes de modification des données valent également pour tous les tiers auxquels ces données ont été transmises (par exemple des partenaires ou des sous-traitants). Le responsable doit veiller à ce que cela se passe aussi bien que possible. Quant à ce fameux « droit à l'oubli », il a déjà été mis en œuvre à grand bruit dans le secteur des réseaux sociaux. Comme nous le verrons, exécuter de telles demandes n'a rien de simple. Il s'agit d'un argument de taille, pour un responsable du traitement, pour indiquer clairement dans les contrats avec des sous-traitants que les données doivent être supprimées immédiatement après leur traitement.

Une personne concernée peut également **demander d'arrêter ou de suspendre tout traitement ultérieur de ses données**, tandis que les données restent quand même conservées. Cela peut être indiqué dans le cas d'une plainte en cours, pour laquelle les autorités ne se sont pas encore prononcées, par exemple si la personne concernée conteste le bien-fondé du traitement. Une telle demande ne peut évidemment pas être satisfaite si le traitement repose sur une obligation légale ou se déroule dans le cadre d'une mission des autorités. Comme nous l'avons déjà dit, un traitement effectué sur base de l'autorisation de la personne concernée peut toujours être arrêté par le **retrait de cette approbation**. Dans ce cas, le responsable est également tenu de supprimer les données.

Enfin, la personne concernée dispose du droit de « **portabilité de ses données** ». Il s'agit d'une disposition auparavant reprise dans la législation ePrivacy qui imposait des obligations aux fournisseurs de services électroniques. L'intention sous-jacente était d'éviter que les prestataires de services prennent les clients en « otage » sous prétexte qu'ils disposent de toutes leurs données et que celles-ci seraient perdues si l'utilisateur souhaitait changer de prestataire de services.



Personne ne veut en effet perdre ses photos, blogs ou e-mails conservés en ligne. Ce droit de la personne concernée est désormais repris dans le RGPD et applicable à tous les traitements des données à caractère personnel. Dans ce contexte beaucoup plus vaste, le transfert n'est souvent pas réalisable dans la pratique. En outre, cela entraîne des conflits avec d'autres droits. Un responsable qui a effectué des traitements complexes avec les données (avec parfois certains algorithmes qui sont la propriété intellectuelle de l'entreprise) ne souhaite pas vraiment renoncer à ces résultats. L'interprétation la plus suivie est que le droit à la portabilité des données vaut uniquement pour les données que la personne concernée a elle-même mises à la disposition du responsable.

Conseil:

Il est préférable que chaque organisation définisse dans une bonne procédure comment traiter toutes ces demandes.

- Pour commencer, il est nécessaire de signifier aux personnes concernées à quel interlocuteur elles doivent adresser leurs questions, et qui dans l'organisation en est responsable. Ceci peut par exemple être repris dans une déclaration de confidentialité.
- Au sein de l'organisation, les demandes doivent être transmises rapidement à la bonne personne afin d'être traitées. Chacun doit être au courant de la procédure.
- Il faut une méthode clairement décrite pour s'assurer que l'identité du demandeur correspond à celle de la personne concernée dont on demande les données. En général, il est suggéré de demander une copie de la carte d'identité du demandeur.
- Il doit également y avoir des règles déterminant quelles informations peuvent être données et quelles informations ne le peuvent éventuellement pas, parce qu'elles peuvent contenir par exemple des données confidentielles sur d'autres personnes ou des secrets d'entreprise. L'argumentation à suivre doit être documentée. Il convient ici de gérer les droits de chacun de manière équilibrée, car les droits de la personne concernée ne sont pas absolus.
- Un système de suivi doit permettre de traiter toutes les demandes dans les temps et de conserver de la documentation sur l'état d'avancement de la demande et les décisions prises.

Il est évident que l'exercice de ces droits occasionnera des problèmes pratiques dans le chef des responsables du traitement des données. Certains cercles craignent également que la loi soit utilisée par des activistes de la confidentialité des données pour harceler des entreprises bien précises avec des demandes organisées en masse. Le RGPD offre toutefois une certaine protection à cet égard, en précisant que les demandes doivent être motivées et ne peuvent être excessives (notamment en les répétant systématiquement). Si le responsable est en mesure de le démontrer, il n'est pas tenu d'accéder à de telles demandes.

Inversement, nous ne pouvons que louer le fait qu'avec le RGPD, en tant qu'individus, nous restons dans une certaine mesure maîtres des informations existant à notre sujet, et que les entreprises et organisations disposent d'un cadre pour gérer les données à caractère personnel avec soin et respect.

9. Responsabilité dans le cadre du RGPD

Maintenant que nous avons pour ainsi dire couvert l'ensemble du RGPD, il reste quelques sujets à aborder plus globalement. L'un d'eux est l'« accountability[28] » ou la responsabilité de ceux qui traitent les données et surtout des responsables pour le traitement. Toute personne qui traite des données à caractère personnel est tenue de respecter les prescriptions du RGPD et doit à tout moment pouvoir démontrer et prouver qu'elle le fait. Si vous êtes familier des audits, vous savez ce que cela signifie. Après vous avoir demandé comment vous vous organisiez pour respecter certaines obligations, vous devez toujours démontrer que vous suivez effectivement vos procédures et exercez un contrôle suffisant sur vos collaborateurs. C'est le sujet de ce chapitre.

Pour pouvoir démontrer que vous connaissez et comprenez tous les aspects du RGPD et en avez transposé les effets dans votre organisation, une certaine administration est nécessaire. Il convient de le faire de manière pragmatique mais en même temps complète, surtout pour une petite entreprise, organisation ou association. Nous avons déjà, dans ce texte, donné quelques conseils pour y parvenir. À l'avenir, vous devrez veiller à ce que votre documentation soit toujours à jour.

Pour commencer, vous devez veiller **à avoir suffisamment de connaissances en interne**. Les organisations qui disposent d'un Data Protection Officer lui confient (à lui et ses collaborateurs) cette responsabilité. Toutefois, même sans DPO, vous devez être informé(e) et former vos collaborateurs.

Le point central, pour attester de votre conformité, est le **registre des traitements des données à caractère personnel**. Le RGPD impose, en soi, la tenue d'un tel registre. Mais il s'agit également du point de départ idéal pour documenter votre maîtrise de la confidentialité des données. Pour chaque traitement décrit, vous y démontrez que vous avez réfléchi à l'objectif et au fondement juridique du traitement, envisagé les risques d'une fuite de données et développé une protection maximale pour l'éviter. Vous devez évidemment élaborer une bonne procédure pour garantir que ces informations restent complètes. Tout traitement supplémentaire doit être repris dans le registre. À cet égard, le rôle du Data Protection Officer est important, car il contribue à et supervise la bonne exécution de cette procédure.

[28] Article 5.2; Article 24 : Recital 74

Pour les projets importants, cette étude préliminaire peut être davantage formalisée. Il est alors question d'une Data Privacy Impact Analyse (DPIA). Il s'agit de la radiographie formelle d'un traitement en vue de définir tous les risques éventuels d'atteintes à la vie privée, d'énumérer toutes les mesures de protection et de confronter l'objectif et le fondement juridique pour s'assurer que le traitement compense les risques résiduels. Pour les traitements intensifs de catégories de données à caractère personnel particulières, une DPIA doit être soumise pour approbation à l'Autorité de protection des données.

Toutes les **mesures prises pour la protection** doivent évidemment être bien documentées. En cas de contrôle, vous êtes censé(e) être en mesure de montrer immédiatement quelles sont les procédures applicables, de quand date la dernière version, à qui chaque procédure est applicable et si vos collaborateurs sont informés des procédures et connaissent les instructions… Si certaines procédures vont de pair avec des actions de contrôle récurrentes, il est important de constater, d'une manière ou l'autre, que ces contrôles sont bien effectués. Il est préférable de conserver un certain temps les fichiers log ou les rapports techniques du contrôle. Dans le cas de contrôles manuels, vous devez en dresser un bref rapport ou une liste, afin de pouvoir démontrer qui a effectué ces contrôles à quel moment.

Tout le système de protection doit être évalué et adapté régulièrement – au moins une fois par an – en tenant compte des modifications au sein de l'organisation, des outils et des techniques utilisés et des solutions de sécurité disponibles.

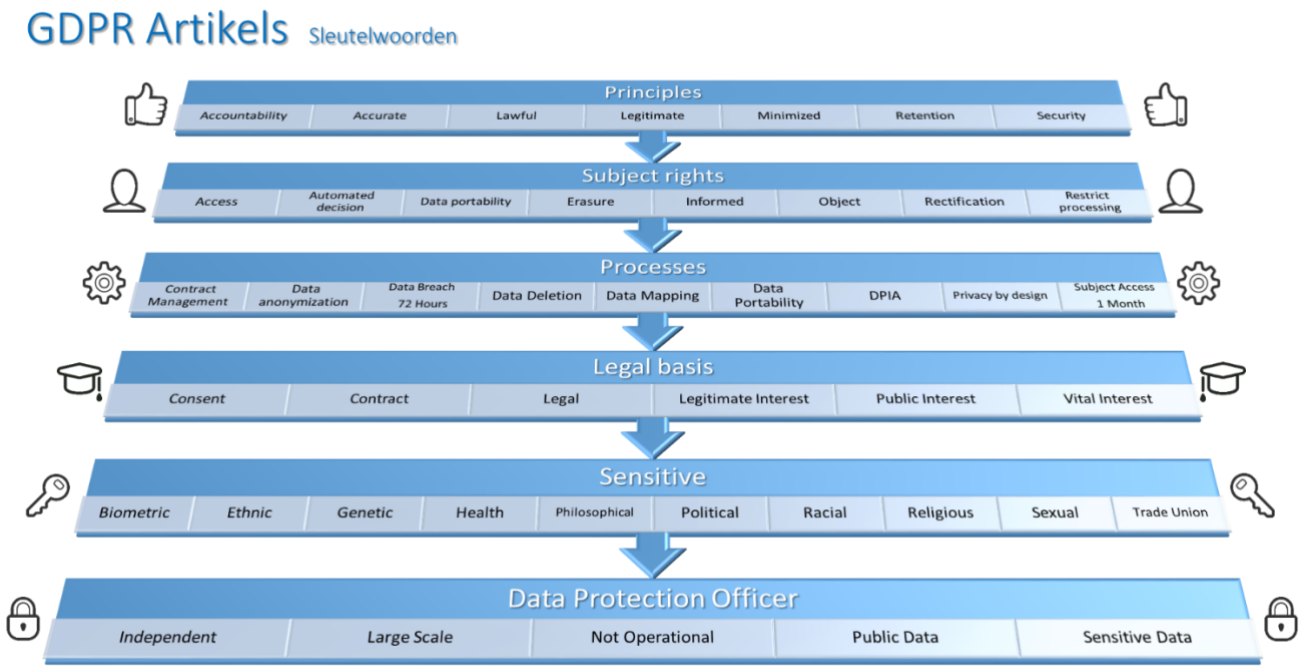
Dans ce contexte, vous devez accorder une grande attention à l'**enregistrement des incidents et surtout des fuites de données**. Tout incident à l'encontre des procédures normales de sécurité, toute constatation mettant en lumière un risque de fuite de données doivent être soigneusement consignés dans une liste d'incidents. Il convient évidemment d'examiner plus en détail les éléments de cette liste afin d'en connaître la cause sous-jacente. Il faut également définir des actions pour réduire le risque. Il peut s'agir de mesures de sécurité techniques supplémentaires, de procédures et de contrôles adaptés ou complémentaires, de nouveaux rapports ou journaux, etc. Afin de pouvoir attester de votre responsabilité, il est important que tout cela soit documenté. Il n'est pas obligatoirement nécessaire d'avoir un système de suivi complexe, mais vous avez au moins besoin de quelques listes synoptiques : tous les incidents avec leur analyse et les solutions convenues, ainsi que tous les points d'action, le responsable pour chacun d'entre eux et le statut.

Il convient d'accorder une attention particulière aux **accords contractuels avec les partenaires ou les fournisseurs**. Un contrat de responsable du traitement doit vous permettre de garantir le respect de la législation par vos sous-traitants également. Nous vous conseillons aussi de tenir un registre des sous-traitants auxquels vous confiez les traitements des données à caractère personnel, et de bien consigner leur mission et vos accords en la matière. Vous pouvez ensuite y coupler un accord spécifique. Inversement, vous devez veiller à ce que tout soit en ordre lorsque vous **intervenez comme responsable du traitement pour un client**. De tels traitements doivent être repris dans votre registre, même si moins de détails sont nécessaires que pour les traitements dont vous êtes responsable. Dans ce cas également, il est important que tous les accords cruciaux soient repris dans un contrat de traitement des données à caractère personnel.

Enfin, vous devez pouvoir démontrer que vous êtes **parfaitement en mesure de garantir les droits des personnes concernées**. Vous devez avoir de bons accords quant à la procédure à suivre lorsqu'une personne concernée pose des questions. Pour toutes les activités à cet égard, il est aussi préférable de tenir une sorte de registre. Si vous consignez toutes les demandes d'une personne individuelle, avec la date et l'heure de la demande, ainsi que les actions entreprises, vous pouvez vous assurer de réagir à temps et d'avoir fourni les réponses adéquates. En cas de contrôle par les autorités ou en cas de plainte, vous serez en mesure de prouver que vous avez fait tout ce qui était en votre pouvoir pour respecter la loi. Il est particulièrement important de conserver les arguments suivis si vous ne pouvez ou ne voulez pas donner suite à une requête.

Il ne suffit donc pas d'être légalement en ordre. Vous devez également documenter et attester de votre respect de la réglementation. Enfin, il est important, pour tous les projets à venir, d'anticiper les risques éventuels relatifs à la confidentialité des données. Ceci fera l'objet du prochain chapitre.

Pour ceux qui sont à la recherche pour plus de mots à la mode ci-dessous un aperçu de tous les mots clés qui sont dans l'99 articles sur la Protection des Données Générales de la Réglementation dans leur propre contexte.



10. L'avenir – Privacy by design

La « protection des données dès la conception » (mieux connue par la dénomination anglaise « *privacy by design*[29]») est un beau sujet pour clôturer en beauté notre exploration de la confidentialité des données. Le législateur souhaite en effet que tous les responsables de traitement de données tiennent compte du traitement des données à caractère personnel dès le début, dans leurs futurs projets. Les auteurs du RGPD partent du principe que nous allons acquérir une espèce de réflexe de protection de la vie privée. Les exigences de la législation deviendront alors une composante naturelle et évidente de l'élaboration d'une application ou de la création d'un site web, mais aussi de l'organisation d'une enquête ou d'une étude scientifique.

Si ce n'est pas nécessaire, il est préférable de ne pas collecter ou traiter de données à caractère personnel. Et s'il y a une bonne raison à leur collecte et leur traitement, nous devons **limiter les traitements au minimum strictement nécessaire**. Chaque nouvelle initiative devra donc faire l'objet d'un exercice de réflexion.

- Lors de l'analyse pour une nouvelle application ou lors de la conception d'une base de données, il était peut-être indiqué, dans le passé, d'ajouter davantage d'attributs ou de champs à un fichier (« au cas où »). Aujourd'hui, le nombre de données doit être aussi limité que possible, ciblant un objectif spécifique.
- Il est préférable d'enregistrer immédiatement dans une base de données lorsqu'une donnée particulière est désuète ou dépassée ou ne peut tout simplement plus être conservée. De la sorte, il n'est pas difficile de supprimer systématiquement des données lorsqu'elles ne sont plus nécessaires ou que leur exactitude ne peut plus être garantie.

[29] Article 25 : Recital 78

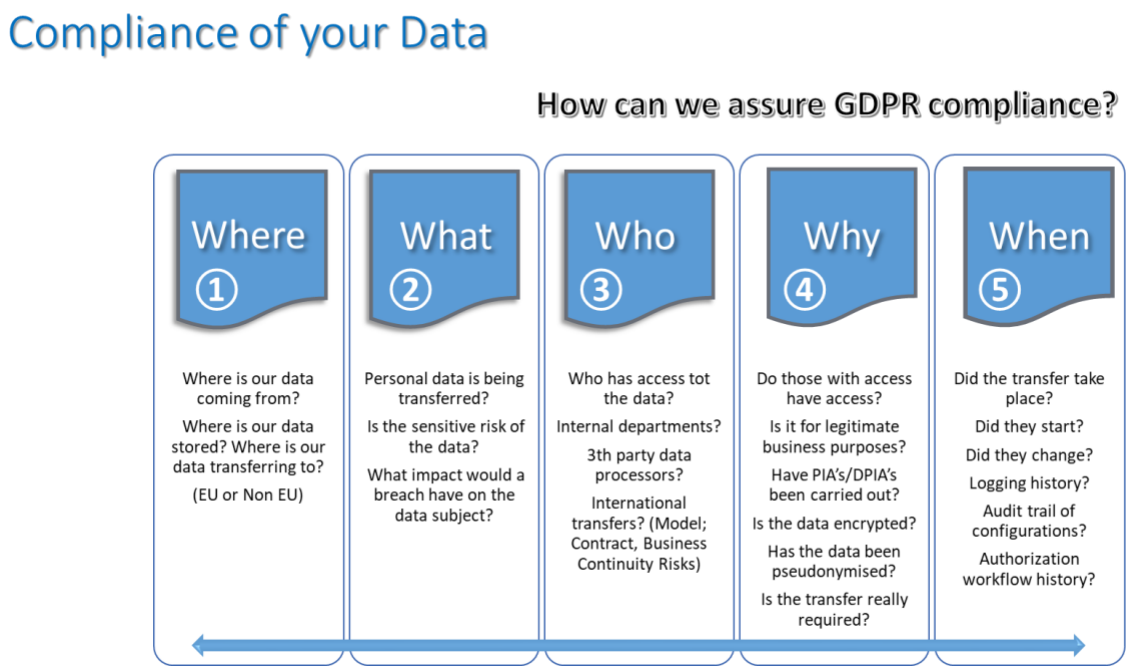
A l'avenir, une application peut comporter d'office une fonctionnalité visant à **garantir les droits des personnes concernées** et à en faciliter l'interprétation pratique.

- Partout où, dans une application, des données à caractère personnel sont demandées à des personnes concernées, il faut aussi que des informations soient disponibles sur le but, la durée du traitement, les risques et les mesures de protection. Une application pour smartphone qui enregistre par exemple les prestations sportives doit, avant la première utilisation, fournir à la personne concernée des informations suffisantes sur les données collectées et stockées en arrière-plan, ainsi que sur les intentions du concepteur de l'application. Cela doit pouvoir être aisément intégré dans l'interface utilisateur des applications.
- De même, toute personne essayant de récolter des informations sur un site doit fournir d'emblée une information de fond claire sur leur traitement. Cette information doit être fournie à temps. Les différents objectifs du traitement doivent être aussi distincts que possible les uns des autres.
- À l'avenir, une application devra idéalement comporter une fonctionnalité permettant aux personnes concernées de consulter leurs données et, si la situation le permet, de les corriger, compléter ou supprimer. Ceci n'est évidemment possible que s'il n'y a pas de conflit entre les droits de la personne concernée et d'autres intérêts.

La « protection de la vie privée dès la conception » implique également, dès la conception d'une application, une réflexion **quant aux façons de protéger au mieux les données**. Vous pouvez par exemple concevoir l'application en recourant systématiquement au cryptage. Un site web peut utiliser des protocoles de cryptage tels que https, l'échange de données peut se faire par des canaux cryptés et avec des fichiers cryptés. Si les données doivent être conservées un certain temps après leur traitement, cela peut également se faire sous forme cryptée, par exemple dans une archive numérique sécurisée. Grâce à ces mesures, le risque diminue que les données deviennent publiques ou tombent entre de mauvaises mains. Si tout cela est envisagé dès la conception, les frais sont bien moins élevés que dans le cas d'adaptations ultérieures. Une mesure pouvant être envisagée dans certains cas est la « pseudonimisation » des données. Comme nous l'avons déjà mentionné, cela implique de supprimer les références directes aux personnes concrètes dans les fichiers. Cela réduit également le risque d'infraction en cas de problème avec un fichier.

Enfin, signalons encore le concept de **« *privacy by default* »**. Il signifie que dans toutes les applications où l'utilisateur peut faire des choix visant à éventuellement rendre des données publiques, les partager avec d'autres ou les mettre à disposition pour certaines formes de traitement ou pour une communication ultérieure, les paramètres par défaut doivent toujours être les plus sûrs. Seule une intervention active de l'utilisateur (comme cocher une case ou cliquer sur un bouton pour donner son autorisation) permet de modifier ces paramètres.

Comme vous le voyez, il existe de nombreuses façons de garantir autant que possible la protection de la vie privée, et le RGPD encourage chacun à toujours les appliquer au maximum. La confidentialité des données n'est pas un thème unique pour un projet en cours, que l'on peut oublier ensuite. Il s'agit d'une préoccupation permanente.



11. RGPD – Les effets immédiats

Depuis le 25 mai 2018, c'est une réalité. Le Règlement Général sur la Protection des Données (RGPD) ou « General Data Protection Regulation » (GDPR) est entré en vigueur. La nouvelle loi européenne stipule désormais comment les entreprises, les administrations et les organisations doivent gérer les données à caractère personnel. Examinons d'un œil pragmatique tout ce qui s'est abattu sur nous comme un véritable tsunami au cours des derniers mois.

Une des premières constatations concerne la lenteur de la mise en route. Le RGPD n'est pourtant pas tombé du ciel. On savait depuis des années que cette législation était en préparation et le texte officiel était publié depuis avril 2016. Il est surprenant de constater qu'autant d'entreprises ne savaient (presque) rien à ce sujet et qu'elles n'ont massivement commencé à se mettre en ordre que début 2018. Cela prouve-t-il que la plupart des organisations prennent à la légère le respect de notre vie privée et la sécurité des données ? Ou s'agissait-il vraiment d'ignorance ?

Nous notons un pic d'activité dans deux domaines. De nombreux responsables du traitement des données à caractère personnel ont, sous l'élan du RGPD, contacté individuellement les destinataires repris dans leurs fichiers d'adresses ou d'autres personnes à propos desquelles leur organisation collecte des données. D'un autre côté, les négociations vont bon train entre les donneurs d'ordres et les entreprises qui traitent pour eux des données à caractère personnel. Examinons plus en détail les deux phénomènes.

11.1. Communication entre les responsables du traitement et les personnes concernées

Pendant la période qui a précédé et suivi le 25 mai, tout le monde a été submergé d'e-mails et de courriers relatifs à la confidentialité des données, envoyés par une multitude d'entreprises et d'organisations. Certaines demandaient l'autorisation d'utiliser vos données, d'autres signalaient simplement que leur déclaration de respect de la vie privée avait été modifiée, d'autres encore expliquaient ce qu'elles savaient et conservaient à votre sujet et pourquoi c'était légitime. Une chose est sûre : la date n'est pas passée inaperçue.

La conséquence inattendue est qu'aujourd'hui, notre mailbox est remplie de messages non sollicités qui, bien souvent, ne nous intéressent pas. Ils perturbent notre tranquillité, mais améliorent-ils aussi le respect de notre vie privée ?

À tout le moins, il est instructif de constater qui possède des données sur nous. Et cela donne indubitablement lieu à des surprises. Bien souvent, nous ne savons pas très bien comment nos coordonnées sont parvenues à un responsable du traitement. Si nous prenons la peine de lire toutes ces communications, nous sommes en tous cas au courant des traitements opérés par ces entreprises ou organisations. La transparence s'est améliorée – et c'était l'un des objectifs du RGPD.

Il est très intéressant de voir le nombre d'approches différentes utilisées. Beaucoup de campagnes ont pour objectif de **demander le consentement aux personnes concernées**.

- Cela se fait parfois de manière parfaitement inutile. Les entreprises écrivent aux personnes concernées parce qu'elles veulent obtenir leur consentement pour le traitement. Elles donnent quelques explications. Et elles terminent la communication en annonçant que ce consentement est donné sauf si la personne concernée les contacte pour se désinscrire. C'est tout simplement illégal dans le cadre du RGPD. Il n'est plus permis de se taire pour donner son consentement.
  Il est nécessaire d'agir, et le responsable du traitement doit également pouvoir démontrer qu'il a reçu une approbation délibérée. Sans réaction, il n'y a donc pas de fondement juridique.
- Il arrive aussi qu'en tant que personne concernée, on vous propose une belle application. Vous pouvez cliquer vers un site contenant plus d'informations. Vous retrouvez tous les éléments nécessaires à une déclaration de respect de la vie privée correcte : l'objet et le fondement juridique des traitements, le délai de conservation des données et les destinataires potentiels, les mesures de sécurité... Vous voyez même parfois aussi les données que l'entreprise conserve et avez la possibilité de les corriger ou de les compléter immédiatement. Et vos droits sont clairement expliqués, de même que la manière dont vous pouvez les exercer. Vous pouvez bien sûr aussi demander que vos données soient effacées. Il s'agit là d'initiatives emblématiques d'exemples à suivre.
- La grande question est de savoir ce qu'il advient concrètement des demandes de consentement auxquelles la personne concernée ne réagit pas. Sur le plan légal, la suite qui doit être donnée est une suppression des données et un arrêt de la communication – le fondement juridique qu'a choisi le responsable du traitement fait défaut. Les entreprises vont-elles réitérer encore plusieurs fois leur tentative de demande de consentement ? Jusque quand est-ce légitime ? L'avenir nous le dira. Et ne recevrons-nous effectivement plus aucune communication ?
- Serons-nous soumis à une campagne turbo de dégraissage et verrons-nous des mégas de données disparaître comme neige au soleil ? Nous craignons malheureusement que les choses ne se passeront pas comme cela. Les véritables activités commerciales continueront simplement, avec ou sans RGPD. On peut déjà en conclure que le RGPD n'est pas un filtre antispam.

D'autres responsables du traitement optent pour l'autre voie, en contactant les personnes concernées. Elles s'appuient sur l'**intérêt légitime**. Dans ce cas, aucun consentement de l'intéressé n'est nécessaire, mais la communication veille à ce que la transparence imposée par la loi soit bel et bien présente.

Si la campagne donne suffisamment d'informations sur le traitement spécifique et l'objet de celui-ci, et si la personne concernée est clairement informée de la manière dont elle peut exercer ses droits et surtout indiquer qu'elle s'oppose au traitement de ses données, c'est également acceptable pour le RGPD.

L'utilisation des données à caractère personnel pour la **communication par e-mail** est toutefois un axe de vigilance majeur. Le RGPD, mais aussi la **législation ePrivacy,** une autre Directive de l'UE (2002/58/ec et 2009/136/ec), s'appliquent à cette forme de communication. L'Union européenne avait l'intention de transposer la législation ePrivacy dans un nouveau règlement et de l'harmoniser avec le RGPD, mais cette révision est loin d'être terminée, notamment en raison des nombreuses discussions et du lobbying qu'elle suscite. On ne sait donc pas très bien quelle direction elle prendra.

L'actuelle Directive ePrivacy est plus stricte que le RGPD et stipule explicitement que le consentement de la personne concernée est nécessaire pour la communication par e-mail dans un contexte de marketing direct, à moins que l'intéressé ait une relation de client et que les produits ou services proposés soient très proches des biens ou services déjà fournis. Récemment, la fédération néerlandaise des professionnels du marketing pointait le danger qui menaçait leurs activités si cette législation devenait trop stricte.

Dans cette situation aussi, les droits de la personne concernée continuent à exister. Vous pouvez toujours demander à une entreprise de mettre fin au traitement de vos données, même si le responsable du traitement estime qu'il a un intérêt légitime. Si aucune obligation légale n'est en jeu ou si un délai de conservation légal est imposé, les données doivent être supprimées ou le traitement doit au moins être arrêté. Donc même si une organisation opte pour l'intérêt légitime comme fondement juridique, elle doit élaborer les mesures nécessaires afin de pouvoir réagir correctement à toute demande individuelle de mettre fin au traitement. C'est loin d'être une sinécure.

11.2. Contrats et accords entre entreprises

Les accords contractuels entre les responsables du traitement et les entreprises qu'ils utilisent en sous-traitance pour le traitement (ou des parties de celui-ci) sont également un domaine dans lequel les choses bougent. Le RGPD exige que le responsable du traitement reste légalement responsable et qu'il se porte garant qu'un fournisseur auquel il fait appel s'en tienne lui aussi à ses obligations juridiques. Cela doit être établi de manière démontrable.

L'expérience nous a appris que conclure un contrat de traitement avec tous les clients et fournisseurs est un travail titanesque.

Bien que de nombreuses organisations aient déjà commencé à le faire, beaucoup de contrats ne sont toujours pas signés.

Divers départements du gouvernement fédéral belge ont déjà tenté de regrouper les différents types de contrats de traitement afin de créer un canevas général et utile pour toutes les villes et communes de Belgique. Mais aucune solution universelle n'a encore été trouvée. Il est aussi particulièrement difficile d'utiliser un véritable standard. Impossible d'exiger cela des clients, surtout s'il s'agit de grandes organisations. Mais les grands fournisseurs favorisent eux aussi leurs propres textes. S'ensuit alors inévitablement la phase consistant à lire et analyser des dizaines de pièces juridiques en termes de complétude et d'équilibre.

Certains éléments de discussion reviennent à chaque fois.

- La responsabilité peut-elle être limitée ou pas ? Les amendes à elles seules peuvent être colossales, mais les dommages directs et surtout indirects en cas d'importante fuite de données coûtent aussi souvent très cher. Il semble raisonnable que le client ne veuille pas étrangler son fournisseur, mais il n'est pourtant pas simple, dans nombre de cas, de stipuler une limitation jusque, par exemple, le montant assuré par une assurance cybersécurité.
- Jusqu'où doit aller le droit à l'audit et qu'en est-il des coûts liés à la réception d'une délégation d'audit ?
- Dans quelle mesure est-il possible, dans la pratique, de charger le sous-traitant de répondre aux demandes des personnes concernées ? Est-ce réalisable chez un sous-traitant qui envoie par exemple des batchs de communication ?
- Est-il raisonnable, pour un client, d'imposer à son fournisseur de fournir gratuitement tout effort supplémentaire découlant du RGPD, juste parce que c'est la loi ?
- Comment gérer le fait qu'un responsable du traitement doive donner à un sous-traitant son approbation spécifique pour que ce dernier puisse à son tour engager un sous-traitant ? Ne peut-on pas décider soi-même comment gérer son entreprise ?

Pour certains de ces points, il faudra chercher un arrangement équilibré et rentable sur le plan économique. Il est en tout cas évident que toute négligence relative aux données à caractère personnel pourra être punie. Chaque responsable du traitement a tout intérêt à être en règle avec les grandes lignes de la nouvelle législation. La sécurité de l'information et la confidentialité des données seront dorénavant incontournables, au même titre que la qualité, pour toute entreprise qui fournit à des tiers des services dans lesquels le traitement des données à caractère personnel joue un rôle.

12. RGPD – Conséquences prévisibles

Dans le chapitre précédent, nous nous sommes penchés sur les effets immédiatement visibles de l'entrée en vigueur du RGPD. Ces deux dernières années, les juristes et les consultants ont épinglé d'autres conséquences majeures à cette entrée en vigueur, dans le but de créer du business, en pointant de grandes menaces : des amendes astronomiques, la déclaration obligatoire des incidents et des fuites de données, suite à quoi le déclarant serait probablement cloué au pilori, un afflux de demandes d'individus voulant faire valoir leurs droits sur leurs données... Jusqu'à présent, nous ne pouvons que constater que tout cela se passe encore bien, mais c'est peut-être parce que ces mécanismes ne se mettent que lentement en branle. Quoi qu'il en soit, jusqu'à présent, ce sont plutôt les effets positifs de la loi qui sont visibles.

12.1 Amendes

Qu'en est-il finalement des amendes en cas de non-respect du RGPD ? Posez-vous la question suivante : « vingt millions d'euros ou quatre pour cent des revenus mondiaux de votre entreprise », qu'est-ce que cela représente et lequel des deux montants est le plus élevé ?

Mettons cela en perspective : 4 % des revenus (en 2016) représentent 5,44 milliards de dollars pour Amazon, 3,6 milliards de dollars pour Google, 1,1 milliard de dollars pour Facebook et seulement 352 millions de dollars pour Netflix. Faites le calcul pour votre entreprise...

On entend souvent les sceptiques comparer le RGPD avec le fameux bug du millénaire, lors du passage de l'année 1999 à 2000, également appelé Y2K bug ou bug de l'an 2000. À l'époque aussi, le monde allait s'effondrer parce que plus aucun ordinateur ne continuerait à fonctionner à partir du 1er janvier 2000 et que nous nous retrouverions catapultés à l'âge de la pierre. Heureusement, les choses ne se sont pas passées comme cela et l'impact du changement de millénaire est resté relativement limité. Il est cependant quelque peu réducteur de comparer cette situation au RGPD.

Pourtant, le 25 mai 2018 est derrière nous et, pour autant que nous le sachions, aucune amende n'a encore été infligée. Jusqu'à présent, l'Autorité belge de protection des données (APD), à qui il appartient de déterminer et d'infliger les amendes, n'est pas encore prête en termes d'activités opérationnelles pour appliquer la nouvelle législation. Cela veut-il dire que vous pouvez dormir sur vos deux oreilles et que rien ne peut vous arriver en tant qu'entreprise ? Nous ne l'affirmerions certainement pas.

12.2 Obligation de notification des fuites de données

Depuis le 25 mai 2018, au sein de l'Union européenne, toutes les fuites de données à caractère personnel doivent être déclarées conformément au RGPD. L'obligation de notification des fuites de données implique que les organisations (tant les entreprises que les administrations) doivent déclarer toute fuite grave de données auprès de l'Autorité belge de protection des données (APD) ou de l'Autoriteit Persoonsgegevens néerlandaise (Autorité des données à caractère personnel - AP) au plus tard dans les 72 heures qui suivent la prise de connaissance de la fuite de données. En tant qu'entreprise, vous ne disposez donc que de trois jours pour déclarer les incidents aux autorités et faire constater une éventuelle atteinte à la vie privée.

Vous devrez expliquer dans cette déclaration : 1) comment la fuite de données a pu se produire ; 2) quelles mesures vous prendrez pour éviter que cela ne se reproduise ; 3) comment et quand vous allez communiquer vis-à-vis des parties concernées. En cas de risque grave de dommage, vous devez également signaler la perte de données aux intéressés (les personnes dont les données à caractère personnel ont été divulguées).

Aux Pays-Bas, cette obligation de notification existe depuis 2016. Il est donc intéressant de constater combien de fuites de données dans les organisations ont été signalées. La réalité nous apprend que quelque **10.000** notifications ont été faites en 2017, dont **47 pour cent** concernent la remise ou l'envoi de données à caractère personnel à un mauvais destinataire. Les données ayant le plus souvent fuité étaient : le nom, l'adresse, la commune, mais aussi le sexe, la date de naissance et/ou l'âge et le numéro de registre national.

Fait remarquable : **298** déclarations ont été retirées après constatation qu'il ne s'agissait pas vraiment d'une fuite de données. Pour les amateurs, le rapport complet peut être téléchargé en PDF sur le site web de l'Autoriteit Persoonsgegevens.

À présent, l'obligation de notification est obligatoire dans tous les États membres de l'Union européenne. Si le fonctionnement précis de cette obligation de notification a éveillé votre curiosité, jetez un coup d'œil au site web de l'Autorité belge de protection des données et essayez d'enregistrer une déclaration (fictive) de fuite de données. Je vous souhaite d'ores et déjà bonne chance. Aux Pays-Bas, l'Autoriteit Persoonsgegevens (AP) maîtrise bien mieux le sujet, mais le pays a un an et demi d'avance sur les autres en ce qui concerne cette obligation.

12.3 Exercice des droits des personnes concernées

Nous savons entre-temps quels sont les droits du *data subject* ou de la personne concernée. En tant que résident de l'Union européenne, vous pouvez demander à toute organisation une liste complète de toutes les données qu'elle possède à votre sujet. Vous pouvez en outre demander de vous transmettre cette information dans une forme transparente et lisible pour tous. Vous avez également le droit à l'oubli, sauf pour l'inspecteur des impôts ou si la législation générale de votre pays en décide autrement. Pensez par exemple aux informations comptables qui doivent être conservées au moins sept ans. Le responsable de la collecte et/ou du traitement des données dispose de 30 jours pour réagir à de telles demandes.

Mais je me demande parfois qui d'entre nous exercera ce droit dans la pratique. Sauf si vous trouvez du plaisir à donner du travail aux entreprises ou associations en leur faisant chercher (littéralement) où sont exactement conservées vos informations. Peut-être que vous avez des arguments valables et que certaines circonstances l'exigent. Mais ce seront toujours les exceptions qui confirment la règle.

J'avoue qu'il est un peu tôt pour tirer des conclusions depuis que le RGPD est entré en vigueur, mais allons-nous tous faire valoir nos droits pour que nos informations soient conservées correctement et en toute sécurité chez des tiers dans le cloud ? Et qui contrôlera cela en notre nom ? Certainement pas l'Autorité belge de protection des données (APD) ou l'Autoriteit Persoonsgegevens néerlandaise (AP), car elles ont déjà suffisamment de pain sur la planche.

Devez-vous engager un délégué à la protection des données (DPO) ? Cette question fait l'objet de nombreuses discussions. Et pouvons-nous, par facilité, donner au Chief Information Security Officer (CISO) le titre de DPO ? La réponse est non. Pouvons-nous alors externaliser le rôle de DPO ? C'est possible mais pas encore tout à fait sûr. Et où trouver une personne qui comprend la confidentialité des données, la sécurité de vos données et tous les aspects juridiques qui y sont liés ? Bonne question !

Un aspect souvent négligé du RGPD est qu'il n'y a que quelques expressions très isolées à propos de la sécurité adéquate relative à la confidentialité des données. Des termes comme « state of the art » sont controversés et ouvrent la voie à la discussion pour tout avocat.

12.4 Évolutions positives

Par ailleurs, nous ne pouvons oublier les côtés positifs du RGPD. La nouvelle législation est aussi une opportunité de mettre de l'ordre dans votre entreprise en termes de gestion des informations. Vous pouvez le faire en posant un regard critique sur la quantité d'informations au sein de votre organisation. Et en utilisant un système de classification des données. Des questions comme : « qui peut accéder à cette information ? » et « où se trouve cette information ? » sont les premières étapes à franchir sur la voie d'une modification réussie de votre politique d'information. La question « pourquoi conservons-nous ces données à caractère personnel spécifiques et qu'en faisons-nous en tant qu'entreprise ? » peut également contribuer à réduire le risque en cas d'éventuelle fuite de données. Il vaut toujours mieux prévenir que guérir...

Une fois que vous avez mis de l'ordre dans votre entreprise en ce qui concerne la sécurité de l'information, vous pouvez le faire savoir à l'aide d'une espèce de label de qualité. Cela vous permet de mettre davantage en lumière, vis-à-vis de vos clients mais aussi de vos propres collaborateurs, votre approche professionnelle des données à caractère personnel.

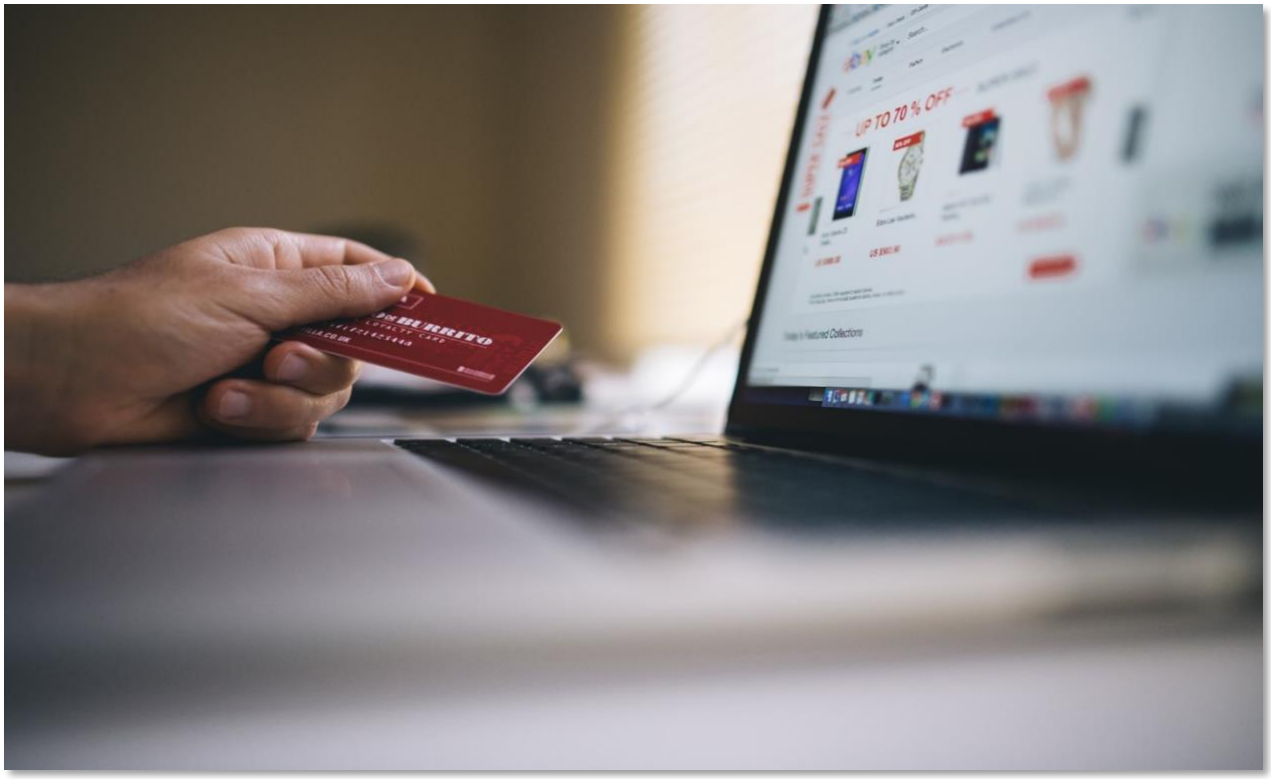
13. RGPD – Obstacle dans le développement technologique ?

Outre tous les autres effets du RGPD, l'imposition de cette nouvelle réglementation pourrait avoir des effets involontaires sur l'une des branches les plus rentables de l'industrie de notre économie mondiale, à savoir le secteur technologique.

13.1 Coûts et conditions supplémentaires pour les start-ups

Premièrement, les coûts augmenteront, ce qui fera baisser la rentabilité, avec pour conséquence moins de bénéfices et donc moins d'investissements, moins de start-ups et une croissance plus lente pour ce secteur.

Une autre conséquence pourrait être que le RGPD limite l'accès à la technologie pour les habitants et les entreprises en Europe. De nombreuses applications sont actuellement développées par de petites entreprises qui, à leur tour, collectent beaucoup d'informations personnelles. Toute start-up internet rêve d'attirer son premier million d'utilisateurs et tente d'y parvenir en mettant en place une opération virale avec des logiciels bon marché, voire gratuits. Leur business model est la collecte de vos données afin de créer de la valeur en utilisant les big data.



Mais elles relèvent désormais aussi du RGPD parce qu'elles possèdent et traitent des données personnelles sur des résidents de l'Union européenne. La définition des données personnelles comprend entre autres votre adresse IP, votre géolocalisation, l'adresse de votre domicile et votre adresse e-mail, qui sont assurément collectées. Les start-ups internet devront donc demander le consentement de chaque utilisateur.

13.2 Frontières digitales

Depuis 2017, l'adoption du cloud fait l'objet d'une croissance stable en Belgique (voir également notre Cloud Barometer). Une application sur cinq tourne d'ailleurs directement à partir du cloud. Et 2018 sera l'année au cours de laquelle quasiment toute PME qui se respecte explore davantage les solutions cloud ou charge son fournisseur informatique de la guider pour exploiter au maximum les avantages des solutions cloud. On nous demande souvent des conseils à ce sujet, car le cloud n'est pas encore évident pour tout le monde.

Une des questions les plus fréquentes est sans aucun doute : « le cloud est-il sûr et comment puis-je, en tant que chef d'entreprise, le vérifier ? ». La différence entre les solutions dans le cloud privé et public semble être un des éléments les plus nébuleux pour beaucoup d'entreprises. Sans le savoir, la plupart des PME sont depuis longtemps dans le cloud public.

De nombreux travailleurs ont une adresse e-mail privée ou un compte Dropbox et utilisent au moins une application de réseaux sociaux (Facebook, WhatsApp, LinkedIn...). Cela montre surtout que l'utilisation des applications du cloud est depuis longtemps ancrée dans les habitudes.

La plupart de ces applications – si pas toutes – proviennent de fournisseurs de cloud public aux États-Unis. J'ai un jour entendu ce qui suit dans les couloirs d'un fabricant :

« L'Amérique les invente (lisez Amazon, Facebook, Google), la Chine les copie (lisez Alibaba, TenCent) et l'Europe les régularise (lisez le RGPD) ».

C'est pour le moins approprié lorsque l'on voit que les plus grands fournisseurs de cloud public (Big 5) viennent d'Amérique et proposent leurs services depuis des décennies, mais qu'à présent l'Europe va y mettre le holà sous l'appellation RGPD.

Pourtant, en tant qu'entreprise, vous devez pouvoir prouver que vous respectez les obligations abordées dans les chapitres précédents. Le RGPD est un sujet brûlant, en particulier lorsqu'il s'agit de services cloud, car les données de votre entreprise et de ses utilisateurs seront sans cesse enregistrées « hors de portée ».

Le nouveau cadre impose non seulement des obligations au responsable du traitement, mais aussi aux parties qui, plus loin dans la chaîne, traitent les données à caractère personnel à des fins d'analyse, de stockage, de facturation... Et ce dernier élément fait figure d'importante nouveauté pour les prestataires de services ICT et plus précisément les fournisseurs de services cloud. Ce règlement sur le respect de la vie privée stipule qu'il faut modifier les contrats et transformer les politiques de protection des données, conformément au règlement. Toutes les entreprises devront en effet pouvoir démontrer qu'elles gèrent de manière responsable les données à caractère personnel de leurs collaborateurs, clients et sous-traitants.

S'ensuivent des défis à différents niveaux. Nombre d'entreprises ne se sont – soyons honnêtes – jamais penchées sur la sécurité des données. La technologie peut faire beaucoup, mais les applications et les processus devront être réexaminés à la lumière de ces changements législatifs.

Il est possible d'éviter ceci en ne collectant tout simplement plus aucune donnée sur des résidents de l'Union européenne. Pour cela, il suffit de demander aux utilisateurs, avant d'installer l'app, de cliquer sur un bouton pour confirmer qu'ils n'habitent pas dans l'Union européenne. Ou d'utiliser votre géolocalisation pour bloquer totalement l'app.

Cela pourrait avoir pour conséquence que chaque Européen se coupe lui-même des derniers développements logiciels. Vous voulez par exemple installer la dernière app de communication sécurisée ? Désolé, ce ne sera pas (ou plus) possible. Et cette nouvelle app professionnelle pour la gestion des contrats ou votre administration ? Pas disponible dans l'Union européenne, seuls ceux qui vivent hors d'Europe peuvent l'utiliser.

Cela pourrait être un gros problème pour l'Europe. Ne vous méprenez pas, car je suis moi-même un grand partisan de la gestion intelligente des données à caractère personnel et de la sécurité du stockage des données en général. Mais si les autorités belge ou néerlandaise de protection des données appliquent littéralement les règles du RGPD, de nouvelles frontières digitales – dont n'ont besoin ni internet ni le consommateur – pourraient faire leur apparition.

14. Conclusion « provisoire »

L'avenir nous dira comment les petites et moyennes entreprises, les personnes individuellement concernées (peut-être incitées par des organisations de consommateurs ou des syndicats), les autorités de contrôle et l'Union européenne elle-même appréhenderont le RGPD. Les tribunaux devront indubitablement se pencher sur des litiges complexes. Il est donc difficile de prévoir quelle sera la réponse aux nombreuses questions qui subsistent actuellement. C'est pourquoi nous parlons prudemment d'une conclusion « provisoire ». Mais une chose est sûre, la confidentialité des données est une notion dont il faut tenir compte et cela restera très probablement le cas.

Un objectif est en tout cas atteint. Au cours de l'année écoulée, la confidentialité des données a été un sujet à l'ordre du jour de toute association, institution publique et entreprise. Tout le monde a réfléchi à l'utilisation des données à caractère personnel. Dans de nombreux cas, cela a conduit à des décisions de réduire les fichiers de données ou d'y mettre peu à peu un terme, et à les conserver beaucoup moins longtemps. La gestion de ces données fait l'objet d'une véritable prise de conscience. Une ambiance d'ouverture s'est formée à propos de cette thématique. La transparence souhaitée a été créée à bien des endroits. Nous verrons si les résultats perdurent une fois que le battage médiatique et l'attention du management auront disparu. Mais nous avons l'impression que le droit des personnes concernées de savoir ce qui est fait des données qui les concernent est déjà un acquis. Ce droit n'est plus dissimulé dans les petits caractères d'interminables contrats, mais est clairement affiché sur les sites web, dans les e-mails et sur les apps.

De longues concertations sont cependant encore nécessaires pour éliminer progressivement tous les points manquant de clarté et parvenir à des règles et accords uniformes, des codes comportementaux équilibrés, des mesures de contrôle mesurables et des textes contractuels utilisables pour tous. Mais si nous poursuivons le travail déjà en cours dans maintes organisations, nous pouvons êtes sûrs que l'incertitude actuelle diminuera. La confidentialité des données deviendra probablement une évidence dans tout l'Espace économique européen, au même titre que la gestion de la qualité, l'environnement et la durabilité.

La question à laquelle il est le plus difficile de répondre est la suivante : le but premier du RGPD, à savoir créer un équilibre entre la protection de la vie privée et le droit à la liberté d'expression et à la libre circulation des biens et services, sera-t-il atteint ? Si la réglementation devait entraver le développement de nouvelles technologies dans le domaine de l'économie de la connaissance, voire même l'empêcher, la balance penchera plus dans un sens que dans l'autre. Si, dans la pratique, il ne ressort rien de la protection espérée des personnes concernées, il ne sera pas question d'équilibre non plus.

Tout l'art consiste donc à chercher la raison des deux côtés, entre les personnes concernées et les organisations ou entreprises, entre les institutions européennes et les grands acteurs du marché, entre les start-ups utilisatrices intensives de données, leurs investisseurs et leurs clients/utilisateurs. Et bien sûr entre l'Europe et les autres acteurs du marché – car nous vivons dans une économie mondiale.

Les raisons ne manquent donc pas pour continuer à suivre de près et avec beaucoup d'intérêt les développements à venir.

À propos de l'auteur

Après une brève carrière académique, Viktor D'Huys[30] a rejoint le secteur ICT il y a plus de 30 ans. Depuis 2003, il est CIO de Group Joos et il contribue à la transformation digitale du groupe, qui était autrefois une imprimerie et un printshop, et est aujourd'hui devenu un spécialiste de la communication hybride proposant aussi de nombreux services numériques.

Viktor s'est entre autres spécialisé dans la sécurité ICT. Il a mis en place l'Information Security Management System (ISMS) grâce auquel Group Joos a obtenu sa certification ISO 27001 en 2013. Il continue aujourd'hui à développer la politique de sécurité de l'information du groupe. Depuis 2016, la confidentialité des données s'est logiquement ajoutée à ses tâches. Viktor et le Data Protection Officer ont dirigé le projet préparé en temps opportun par Group Joos relatif au RGPD.

Viktor est Certified Information Security Officer (CISM) et Certified Information Privacy Professional (CIPP/E).

À propos du co-auteur

Au cours des dix dernières années, Peter Witsenburg[31] a eu l'occasion de travailler dans le domaine du cloud computing et de la sécurité de l'information. Dans ce dernier secteur, Peter a réalisé différents audits internes et externes reposant sur l'ISMS et le RGPD.

Chez Interxion, entre autres, il a collaboré à la mise en place de la norme ISO 27001 ISMS (Information Security Management System) en vue des évaluations des risques, de la politique de sécurité de l'information et du plan de continuité des activités (business continuity plan - BCP) en utilisant la méthodologie PDCA.

En plus de son activité professionnelle, Peter est aussi vice-président du comité de sélection de l'asbl '*Netwerk Ondernemen Vlaanderen'.* Pendant son temps libre, il écrit des articles et des blogs sur les dernières tendances ICT. Peter est en outre le fondateur de '*Belgium Cloud'* et de '*CloudMakelaar'.*

[30] Les chapitres 1 à 10 ont été écrits par Viktor D'Huys, avec de petites retouches de Peter Witsenburg, qui a également fourni les schémas destinés aux illustrations.

[31] Les chapitres 11 à 14 sont une révision approfondie de textes de Peter Witsenburg et de Viktor D'Huys. Peter Witsenburg s'est chargé de la composition et de la mise en page du livre.

Références

Le texte **légal officiel** le RGPD en anglais, Français et néerlandais se trouvent en PDF via les liens suivants :

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679

Plus, d'informations peuvent être trouvés partout. Je me limiterai ici à quelques canaux officiels.

La **Commission européenne** fournit plus d'informations via le lien suivant:

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_nl

Le site Web de **l'autorité de protection de données belge** a été adapté sur 25 mai 2018. Avec l'ancienne URL (https://www.privacycommission.be), vous pourrez toujours voir une page de transition, où vous trouverez le nouveau site en néerlandais, en anglais ou en Français. Le contenu et la structure du site est environ est resté le même, mais pas mis à jour en ce qui concerne l'organisation de l'autorité de protection des données.

https://www.gegevensbeschermingsautoriteit.be/)

Ce site contient beaucoup d'informations sur le RGPD. Vous pouvez trouver une feuille de route et toute une série de dossiers thématiques et la possibilité de télécharger les documents.

https://www.gegevensbeschermingsautoriteit.be/algemene-verordening-gegevensbescherming-avg

Les données personnelles de l'autorité (AP), l'autorité de protection des données néerlandaise et l'organe directeur indépendant qui a été nommé par la loi aux pays-bas en tant que superviseur pour surveiller le traitement des données à caractère personnel.

Ici, vous pouvez visiter le site des données personnelles d'autorité (AP) et vous trouverez un large éventail d'informations utiles, soigneusement classés par sujet.

RGPD - Les références des articles et des Considérants par chapitre*

1.1		Article 4.1 et 4.6 – Considérant 15, 26-27 et 30-31
1.2.		Article 4.13-15; Article 9-10 - Considérant 34-35 et 51-56
1.2	Pseudonymisation	Article 4.5; Article 25 - Considérant 78
1.3	Data processing	Article 2.1-2; Article 4.2
1.3	Homely atmosphere	Article 2.2c - Considérant 18
1.3	Responsible	Article 4.7
1.3	Processor	Article 4.8
1.3	Data subject	Article 12
1.4		Article 37-39 - Considérant 97
2		Article 5 - Considérant 39
3.1		Article 30 - Considérant 82
3.1	Who registry duty	Article 30.5 - Considérant 13
3.2		Article 30.1 - Considérant 39
4.1		Article 6 - Considérant 40-50
4.1	special categories	Article 9 - Considérant 51-56
4.2		Article 4.11; Article 7-8 - Considérant 32-33,38,42-43
4.3		Article 6-9 - Considérant 47-49
5.1		Article 13-14 - Considérant 60-62
5.2		Article 12.1 - Considérant 58
6.1		Article 24.2 et 25; Article 32
6.2		Article 32; Article 35-36 - Considérant 75-76, 84, 89-95
6.3		Article 32 - Considérant 77-78
6.4		Article 28-29 - Considérant 79 et 81
7.1		Article 4.12; Article 33-34 - Considérant 75 et 87-88
7.2		Article 33 et 34 - Considérant 85-88
8.1		Article 12-15; Article 23 - Considérant 58-64
8.2		Article 16-23 - Considérant 65-73
9		Article 5.2; Article 24 - Considérant 74
10		Article 25 - Considérant 78

**Des références à la GDPR Articles grâce à intersoft de consultation, voir aussi: gdpr-info.eu*

Tous les articles dans plus de détails se trouvent dans la publication suivante:

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

Postface: Group Joos et le RGPD

Le traitement des données à caractère personnel est l'une des activités principales de Group Joos. C'est la raison pour laquelle nous avons commencé à nous préparer dès avril 2016, bien avant la publication officielle du RGPD. Nous avons par exemple immédiatement nommé un Data Protection Officer (DPO). Nous estimions qu'il était de notre devoir, envers nos clients, d'acquérir aussi vite que possible les connaissances nécessaires et de préparer notre organisation au respect de cette nouvelle réglementation.

Pour Group Joos, la protection adéquate de toutes les données confidentielles est une priorité absolue. Cela englobe bien évidemment toutes les données à caractère personnel. Au cours des dernières années, nous avons consenti d'importants investissements dans la technologie et pris les mesures organisationnelles nécessaires pour amener la protection des informations au niveau le plus élevé. C'est ainsi que nous sommes certifiés ISO 27001 depuis 5 ans déjà.

Expertise et services de Group Joos

Nous sommes convaincus que Group Joos est un partenaire fiable, paré pour fournir à ses clients des services impliquant le traitement de données à caractère personnel.

Vous voulez être sûr(e) que les données à caractère personnel dont vous êtes responsable sont entre de bonnes mains ? Vous frappez à la bonne porte. Un mailing publicitaire, une campagne multicanaux pour atteindre des prospects, la composition de documents contenant des informations médicales ou financières très sensibles avec fourniture via le canal de votre choix... Group Joos vous propose toujours une solution appropriée qui respecte toutes les exigences de la nouvelle réglementation. Nous veillons à ce que les données puissent nous être fournies en toute sécurité, à ce qu'elles soient traitées de manière correcte et confidentielle, et à ce qu'elles soient délivrées au destinataire en toute sécurité sur papier ou via l'un des nombreux canaux numériques. Si vous le souhaitez, les données peuvent ensuite être conservées cryptées pendant une période déterminée.

Vous pouvez également faire appel à nous pour une archive numérique fiable. Group Joos se charge d'une solution technologique adaptée pour votre communication et propose un éventail de possibilités pour vous aider dans votre transformation numérique. Nous sommes prêts à réaliser tout cela de manière socialement responsable et conformément à toutes les dispositions légales.

Nous partageons volontiers avec nos clients et toute personne intéressée l'expertise acquise tout au long du trajet préparatoire. Nous espérons que les informations présentées dans cette publication seront utiles à tous ceux qui s'interrogent sur la bonne gestion des données à caractère personnel.

Group Joos nv

Everdongenlaan 14 -2300 Turnhout (B)

gdpr@groupjoos.com www.groupjoos.com

GUIDE

RGPD

PRATIQUE

Responsible Publisher: Group Joos in cooperation with Cloud Makelaar