**WEBSITES GDPR-DPO**

**V.1.0. dd April 29, 2018**

# FRENCH

## Qu'est-ce que le GDPR ?

Le *General Data Protection Regulation* (GDPR) ou *Règlement Général sur la Protection des Données* (RGPD) représente la plus importante mutation législative depuis 20 ans.

Directement applicable dans les 31 pays de l’Espace Économique Européen (les 28 États membres de l'[Union européenne](https://fr.wikipedia.org/wiki/Union_europ%C3%A9enne) (UE) et trois des quatre États membres de l'[Association européenne de libre-échange](https://fr.wikipedia.org/wiki/Association_europ%C3%A9enne_de_libre-%C3%A9change)), il s’impose de manière identique partout et sans intervention de chaque état membre pour l’insérer dans son arsenal législatif.

Il étend et renforce les droits des personnes concernées, nos clients si nous sommes acteurs des organismes à profit social ou privé, en termes de transparence dans le traitement de leurs données personnelles, surtout si elles sont sensibles ou si elles concernent des enfants.

L’internet, le cloud, hébergent nos données personnelles des plus « *ordinaires* » (nom, profession, résidence, téléphone, adresses email,…) au plus « *sensibles* » (opinions politiques, convictions religieuses ou philosophiques ou appartenance syndicale, données génétiques ou biométriques, relatives à la santé ou concernant la vie sexuelle ou l'orientation sexuelle).

Nous sommes demandeurs d’être, de devenir… ou de rester, maîtres de nos identités digitales qui doivent par ailleurs être adéquatement protégées de multiples personnes malveillantes.

Les données collectées sont à présent limitées de multiples manières : le consentement requis est ainsi caparaçonné (libre, spécifique, éclairé, univoque et strictement nécessaire aux prestations) et réellement cuirassé s’il concerne des catégories particulières de données à caractère personnel, des données génétiques ou biométriques (explicite).

Les finalités de la collecte et du traitement de ces données est circonscrite, les données sont d’ailleurs minimisées à ce qui doit impérativement être collecté pour atteindre ces objectifs. L’exactitude et la durée de conservation des données font également l’objet de mesure spécifiques et particulièrement contraignantes comme le droit au retrait du consentement, à l’effacement ou à la rectification.

La confidentialité et la sécurité doivent également être garanties dès la conception du bien ou service et par défaut, seules les données à caractère personnel qui sont strictement nécessaires au regard de chaque finalité spécifique du traitement sont proposées et traitées.

La « pseudonymisation » (ou **anonymization**) et le « chiffrement » (ou **cryptage)** sont encouragés et clairement définis tandis que de nouveaux droits voient le jour comme la portabilité des données qui doivent à présent être fournies dans un format structuré, couramment utilisé et lisible et sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées puisse y faire obstacle.

Les données personnelles bénéficient de protections supplémentaires en cas de traitement transfrontalier sous la stricte inspection des autorités de contrôle dotées de pouvoirs de sanctions jamais rencontré auparavant pouvant atteindre 20 Mo d’euros (ou 4% du chiffre d'affaire annuel mondial)!

La hantise de tout responsable du traitement des données et donc *in fine* de toute entreprise qui les collecte, est plus que jamais d’être victime d’une violation des données à caractère personnel.

La « personne physique identifiable » n’est autre que nous-même dans nos multiples interactions digitales, sur le net ou par mail, via des serveurs ou dans le cloud, par des procédés automatisés ou non,…

## Pourquoi devez-vous vous en soucier ?

Le RGPD concerne toute entreprise établie dans l’Union Européenne mais également :

1. l'offre de biens ou de services aux personnes concernées dans l’Union qu'un paiement soit exigé ou non desdites personnes; ou
2. le suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

De manière automatique, sans autre information, le règlement entre en vigueur le 25 mai 2018 : <http://www.eugdpr.org/>.

Chaque organisation qui ne s’est pas conformée à cette date s’expose à des amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Chaque entreprise – à buts lucratifs ou non - doit fournir à chaque personne concernée l’information qu’elle a le droit d'introduire une réclamation auprès d'une autorité de contrôle.

Puisque les violations de données à caractère personnel croissent de manière exponentielle plutôt que de se réduire ou s’éteindre, que l’information n’a jamais été aussi facile à partager entre un grand nombre de personnes sinon la planète entière, gageons que nos entreprises s’exposent à de nombreuses communications des données des personnes protégées par le RGPD aux autorités de contrôles…

## Quelles sont les opportunités offertes par le RGPD ?

Les opportunités sont pour nous plus nombreuses et inspirantes que les contraintes ou les obligations nouvelles ou intensifiées.

Les entreprises qui considèrent le RGPD comme un fardeau resteront à quai voire couleront tandis que celles qui le considèrent comme une chance apportant un souffle nouveau navigueront toutes voiles dehors (<http://www.cityam.com/268997/business-which-treat-gdpr-burden-get-left-behind)>.

La plupart des entreprises manquent actuellement de règles, techniques, personnes, pratiques et procédures pour garantir les droits et libertés des consommateurs digitaux.

Elles sont souvent indolentes et manquent de vision à moyen et long terme quant au traitement et à la conservation de ces données. Leurs équipes ne communiquent que peu sur le sujet et cette préoccupation n’est pas partagée par tous (mais au contraire limitée en règle aux services juridiques et informatiques).

Le RGPD repose tout entier sur la **CONFIANCE** qu’il fait naître ou grandir entre une entreprise et ses clients.

Le RGPD crée un nouvel environnement à l’origine d’expériences nouvelles pour les consommateurs : plus que jamais leur consentement doit être éclairé et l’usage qui est fait de leurs données, strictement réglementé.

Il permet également de rassembler une entreprise, de souder les membres de nombreux départements concernés, autour d’une vision commune de bonnes pratiques en termes de traitement des données personnelles.

Comme un phare dans la nuit glaciale des tsunami que nos économies modernes toujours plus digitales traversent, le RGPD brille et nous guide vers une nouvelle clarté et transparence.

Clairement, les objectifs de l’Union Européenne sont de créer un marché digital fort dans lequel la confiance des consommateurs dans les entreprises responsables du traitement, et leurs sous-traitants, est garantie… Et peut même devenir exemplaire et inspirante pour le reste du monde.

## Quand le Règlement européen est-t-il applicable ?

Le règlement est applicable à partir du 25 mai 2018 (article 99.2 du règlement) dans tous les pays de l'Union Européenne.

Les applications, manifestations de consentement, fichiers et autres traitements de données déjà mis en œuvre à cette date doivent, d'ici là, être mis en conformité avec les dispositions du règlement.

La conformité de votre entreprise impose souvent plus que de « cocher » des cases sans adoption de nouveaux outils, méthodes et politiques de gestion et de reporting. Le coût de ne PAS être conforme est extrêmement élevé.

## GDPR et DPO vous offrent des services de consultance

### AUDITS & CONSULTANCY

Les obligations de déclaration auprès des autorités de contrôle sont supprimées à compter du 25 mai 2018. Elles sont remplacées par des exigences de conformité, de responsabilité et sont accompagnées de (très) lourdes sanctions dissuasives.

Le Règlement accroit les droits des personnes concernées, multiplie les obligations de communication aux autorités de contrôles et aux personnes concernées en cas de violation des données et les assorti de sanctions plus sévères.

Évaluer le nombre, type et compétences de ressources humaines, matérielles, financières et d’information pour assurer le projet « GDPR compliance » est le point départ de toute démarche de conformité au RGPD.

[La déclaration préalable de traitement restera-t-elle obligatoire dès l’application du RGPD (25 mai 2018) ?](https://www.privacycommission.be/fr/la-d%C3%A9claration-pr%C3%A9alable-de-traitement-restera-t-elle-obligatoire-d%C3%A8s-l%E2%80%99application-du-rgpd-25-mai)

Non. Le RGPD supprime cette obligation préalable de déclaration des traitements à l’Autorité de Protection des Données mais impose de tenir un Registre des activités de traitement. Ce Registre est un outil interne et devra être fourni à l’autorité de contrôle à première demande. Cet outil permet aux responsables de traitement et sous-traitants d’identifier les traitements opérés et de faciliter la mise en conformité de ces traitements avec le RGPD.

*Source :*[*points 33 et s. de la recommandation 06/2017*](https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_06_2017_0.pdf)[***[1]***](applewebdata://16925669-0EAC-4C16-B9D2-6FAA9879FB0C#_ftn1)*.*

Nos entreprises GDPR SPRL et DPO SPRL ont donc pour objectif de vous accompagner tout au long des 3 étapes majeures du traitement des données : **1) la définition de données à collecte et l’évaluation de celles-ci 2) leur traitement licite 3) le reporting et la responsabilité à l’égard des autorités des contrôle.­­­**

*Assurez-vous qu'un programme complet de conformité est conçu pour votre organisation et qu'il intègre des fonctionnalités telles que:*

1. *des analyses d’impact relatives au traitement des données,*
2. *des audits réguliers,*
3. *des révisions et mises à jour des politiques et procédures, notamment en termes de RH,*
4. *des programmes de formation et de sensibilisation.*

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l’ensemble des événements qui peuvent survenir au cours de la vie d’un traitement de données (ex : faille de sécurité, gestion des demandes de rectification ou d’accès, modification des données collectées, changement de prestataire).

Organiser et DOCUMENTER les **processus** implique notamment :

* de prendre en compte la protection des données personnelles dès la conception (Article 25) d’une application ou d’un traitement (minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d’information, recueil du consentement, sécurité et confidentialité des données, s’assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données, …). Pour cela, appuyez-vous sur les conseils du délégué à la protection des données ;
* de sensibiliser et d'organiser la remontée d’information en construisant notamment un plan de formation et de communication auprès de vos collaborateurs ;
* de traiter les réclamations et les demandes des personnes concernées quant à l’exercice de leurs droits (droits d’accès, de rectification, d’opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen) (Articles 15-23) ;
* d'anticiper les violations de données en prévoyant, dans certains cas, la notification à l’autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais (Articles 33+34)[[2]](applewebdata://16925669-0EAC-4C16-B9D2-6FAA9879FB0C#_ftn2).

De vos déclarations de confidentialité ou de consentement jusqu’aux notifications de violation des données personnelles en passant par la tenue du registre des activités de traitement et à la désignation du délégué à la protection des données *ad hoc*, nous vous assistons dans l’ensemble des obligations imposées par le Règlement.

Nous adoptons l’approche la plus proche possible de celle recommandée par les autorités de protection des données et en particulier celle de la Commission de Protection de la Vie Privée :

### Avis et conseils juridiques pour la conformité au GDPR

#### Deux recommandations « qui valent de l’or »

1. Réalisez une analyse d’impact relative à la protection des données (« ***DPIA*** en anglais ») ; et
2. Désignez un ***Délégué à la Protection des Données*** avec tous les avantages que cela représente pour votre entreprise cf : [**https://www.linkedin.com/pulse/dpos-job-rockn-roll-christophe-boeraeve/?trackingId=CPPEMv9gSZ8N0Xd4gfsNMA%3D%3D**](https://www.linkedin.com/pulse/dpos-job-rockn-roll-christophe-boeraeve/?trackingId=CPPEMv9gSZ8N0Xd4gfsNMA%3D%3D)**&**<https://www.linkedin.com/pulse/le-d%C3%A9l%C3%A9gu%C3%A9-%C3%A0-la-protection-des-donn%C3%A9es-ou-dpd-christophe-boeraeve/>

#### 3 approches complémentaires

Il manque en règle dans les offres faites aux sociétés, autorités publiques et organismes à profit social deux fonctions non couvertes : celles de 1) **Gestion du projet** et 2) de **Cybersécurité** cf : <https://www.linkedin.com/pulse/les-paradise-papers-r%C3%A9v%C3%A8lent-des-montages-fiscale-une-boeraeve/>  & <https://www.linkedin.com/pulse/paradise-papers-reveal-international-arrangements-tax-boeraeve/>

Voici selon nous les **3 axes nécessaires et suffisants** pour assurer votre conformité :

*Comme toujours, le Règlement va requérir****3 approches distinctes****et convergentes pour atteindre cet objectif hautement désirable : la sauvegarde et la protection des données:*

1. ***Approche légale et juridique****. Des instructions, et autres articles de loi nous guident tout au long d’une voie qui ne comprend pas vraiment d’arrivée permanente et finale ; et*
2. ***Approche informatique/technologique****. Des moyens et ressources des technologies de l’information, des réseaux et de l’informatique articulent la réponse aux volontés de nuire des hackers ou aux simples incidents ou accidents qui peuvent aboutir à des pertes/altérations de données. Il s’agit autant de solutions en termes de matériels informatiques (« hardware ») que de logiciels (« software »); et*
3. ***Approche organisationnelle/humaine.****Les deux premières solutions, froides comme peuvent l’être des codes juridiques ou des machines électroniques, sont (encore à ce jour) toujours conçues et actionnées par des****êtres humains****. Les procédures, politiques et autres instructions ou check-lists organisent les solutions juridiques et techniques en****rassemblant les personnes concernées****par la protection des données dans l’entreprise.*

Nouer une relation avec l’Autorité de Protection des Données

Notre approche, basée sur la méthode des 6 c’s ou « *checks*» diffère également en ce que nous souhaitons entrer en contact et interroger sur base continue **l’Autorité de Protection des Données**(le « *gendarme*») cf : [http ://www.law-right.com/fr/notre-cabinet/6-checks-pour-optimiser-votre-dossier/](http://www.law-right.com/fr/notre-cabinet/6-checks-pour-optimiser-votre-dossier/) & [Law Right – La Méthode des 6C (6 checks) – YouTube](https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=video&cd=2&cad=rja&uact=8&ved=0ahUKEwjbnsS6m4PWAhWQaVAKHasNCqoQtwIILjAB&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DIA6gPmlriyo&usg=AFQjCNEUIKjrrmU8UnxXHqEXnqARr5s0Gg).

En l’attente de pouvoir **certifier** votre organisation (prévu par le Règlement mais faudra attendre que l’APD l’organise et nous sommes en Belgique), seul le « *gendarme*» - et aucun consultant – n’est en mesure de vous rassurer et vous garantir cette conformité.

Pour découvrir les nouvelles compositions, compétences et règles de fonctionnement de la nouvelle Autorité de Protection des données en Belgique :

<https://www.linkedin.com/pulse/quel-est-limpact-de-la-loi-cr%C3%A9ant-lautorit%C3%A9-des-donn%C3%A9es-boeraeve/> & <https://www.linkedin.com/pulse/loi-portant-cr%C3%A9ation-de-lautorit%C3%A9-protection-des-donn%C3%A9es-boeraeve/> .

Test d’Intrusion en collaboration avec l’Autorité de Protection des Données

Re : approche technologique, nous vous proposons de réaliser en premier lieu un « Penetration Test » ou « Test d’Intrusion » : <https://fr.wikipedia.org/wiki/Test_d%27intrusion>: méthode d'évaluation(" audit " en anglais) de la [sécurité](https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_du_syst%C3%A8me_d%27information) d'un [système](https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27information) ou d'un [réseau informatique](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique) ou [Système d'information](https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27information); il est réalisé par un testeur, ("pentester" en anglais ).

Les résultats sont toujours partagés, évalués et à la source des changements initiés, mis en place et testés régulièrement. Les solutions envisagées et décidées sont préalablement validées par l’Autorité de Protection des Données, jusqu’à 4 selon la méthode originale Conformité4[[1]](#footnote-1).

Nous vous accompagnons donc dans la conformité en vérifiant celle-ci durant 13 étapes (en Belgique) : <https://www.privacycommission.be/fr/preparez-vous-en-13-etapes> :

[[](https://www.privacycommission.be/fr/conscientisation)](https://www.privacycommission.be/fr/conscientisation)

**[1. Conscientisation](https://www.privacycommission.be/fr/conscientisation)**

[✅](https://www.privacycommission.be/fr/conscientisation)**[Informez](https://www.privacycommission.be/fr/conscientisation)**[les personnes clés et décideurs des changements.](https://www.privacycommission.be/fr/conscientisation)

[[](https://www.privacycommission.be/fr/registre-des-activites-de-traitement-0)](https://www.privacycommission.be/fr/registre-des-activites-de-traitement-0)

**[2. Registre de données](https://www.privacycommission.be/fr/registre-des-activites-de-traitement-0)**

[✅ Faites](https://www.privacycommission.be/fr/registre-des-activites-de-traitement-0)**[l'inventaire](https://www.privacycommission.be/fr/registre-des-activites-de-traitement-0)**[des traitement que vous effectuez.](https://www.privacycommission.be/fr/registre-des-activites-de-traitement-0)

[[](https://www.privacycommission.be/fr/delegue-a-la-protection-des-donnees-0)](https://www.privacycommission.be/fr/delegue-a-la-protection-des-donnees-0)

**[3. Délégué à la protection des données](https://www.privacycommission.be/fr/delegue-a-la-protection-des-donnees-0)**

[✅](https://www.privacycommission.be/fr/delegue-a-la-protection-des-donnees-0)**[Désignez un DPD](https://www.privacycommission.be/fr/delegue-a-la-protection-des-donnees-0)**[(si nécessaire) ou un représentant.](https://www.privacycommission.be/fr/delegue-a-la-protection-des-donnees-0)

[[](https://www.privacycommission.be/fr/communication)](https://www.privacycommission.be/fr/communication)

**[4. Communication](https://www.privacycommission.be/fr/communication)**

[✅](https://www.privacycommission.be/fr/communication)**[Évaluez](https://www.privacycommission.be/fr/communication)**[votre déclaration de confidentialité et](https://www.privacycommission.be/fr/communication)**[modifiez-là](https://www.privacycommission.be/fr/communication)**[si besoin est.](https://www.privacycommission.be/fr/communication)

[[](https://www.privacycommission.be/fr/droits-de-la-personne-concernee)](https://www.privacycommission.be/fr/droits-de-la-personne-concernee)

**[5. Droits de la personne concernée](https://www.privacycommission.be/fr/droits-de-la-personne-concernee)**

[✅](https://www.privacycommission.be/fr/droits-de-la-personne-concernee)**[Vérifiez](https://www.privacycommission.be/fr/droits-de-la-personne-concernee)**[si les procédures actuelles prévoiet tous les droits.](https://www.privacycommission.be/fr/droits-de-la-personne-concernee)

[[](https://www.privacycommission.be/fr/demande-dacces)](https://www.privacycommission.be/fr/demande-dacces)

**[6. Demande d'accès](https://www.privacycommission.be/fr/demande-dacces)**

[✅](https://www.privacycommission.be/fr/demande-dacces)**[Réflechissez](https://www.privacycommission.be/fr/demande-dacces)**[à la manière dont vous traiterez les demandes d'accès.](https://www.privacycommission.be/fr/demande-dacces)

[[](https://www.privacycommission.be/fr/fondement-legal-pour-le-traitement-de-donnees-a-caractere-personnel)](https://www.privacycommission.be/fr/fondement-legal-pour-le-traitement-de-donnees-a-caractere-personnel)

**[7. Fondement légal](https://www.privacycommission.be/fr/fondement-legal-pour-le-traitement-de-donnees-a-caractere-personnel)**

[✅](https://www.privacycommission.be/fr/fondement-legal-pour-le-traitement-de-donnees-a-caractere-personnel)**[Identifiez](https://www.privacycommission.be/fr/fondement-legal-pour-le-traitement-de-donnees-a-caractere-personnel)**[le fondement légal pour chaque traitement.](https://www.privacycommission.be/fr/fondement-legal-pour-le-traitement-de-donnees-a-caractere-personnel)

[[](https://www.privacycommission.be/fr/consentement)](https://www.privacycommission.be/fr/consentement)

**[8. Consentement](https://www.privacycommission.be/fr/consentement)**

[✅](https://www.privacycommission.be/fr/consentement)**[Évaluez](https://www.privacycommission.be/fr/consentement)**[la manière dont vous demandez et regristrez le consentement.](https://www.privacycommission.be/fr/consentement)

[[](https://www.privacycommission.be/fr/enfants)](https://www.privacycommission.be/fr/enfants)

**[9. Enfants](https://www.privacycommission.be/fr/enfants)**

[✅](https://www.privacycommission.be/fr/enfants)**[Développez](https://www.privacycommission.be/fr/enfants)**[des systèmes qui vérifient l'âge de la personne concernée.](https://www.privacycommission.be/fr/enfants)

[[](https://www.privacycommission.be/fr/fuites-de-donnees)](https://www.privacycommission.be/fr/fuites-de-donnees)

**[10. Fuites de données](https://www.privacycommission.be/fr/fuites-de-donnees)**

[✅](https://www.privacycommission.be/fr/fuites-de-donnees)**[Prévoyez des procédures](https://www.privacycommission.be/fr/fuites-de-donnees)**[pour détecter, rapport et analyser les fuites de données.](https://www.privacycommission.be/fr/fuites-de-donnees)

[[](https://www.privacycommission.be/fr/la-protection-des-donnees-des-la-conception-et-laipd)](https://www.privacycommission.be/fr/la-protection-des-donnees-des-la-conception-et-laipd)

**[11. Protection des données dès la conception et l'AIPD](https://www.privacycommission.be/fr/la-protection-des-donnees-des-la-conception-et-laipd)**

[✅](https://www.privacycommission.be/fr/la-protection-des-donnees-des-la-conception-et-laipd)**[Éxaminez](https://www.privacycommission.be/fr/la-protection-des-donnees-des-la-conception-et-laipd)**[la manière dont ces concepts pourront être mis en oeuvre.](https://www.privacycommission.be/fr/la-protection-des-donnees-des-la-conception-et-laipd)

[[](https://www.privacycommission.be/fr/international-0)](https://www.privacycommission.be/fr/international-0)

**[12. International](https://www.privacycommission.be/fr/international-0)**

[✅](https://www.privacycommission.be/fr/international-0)**[Déterminez](https://www.privacycommission.be/fr/international-0)**[de quelle autorité de contrôle vous relevez.](https://www.privacycommission.be/fr/international-0)

[[](https://www.privacycommission.be/fr/contrats-existants)](https://www.privacycommission.be/fr/contrats-existants)

**[13. Contrats existants](https://www.privacycommission.be/fr/contrats-existants)**

[✅](https://www.privacycommission.be/fr/contrats-existants)**[Évaluez vos contrats existants](https://www.privacycommission.be/fr/contrats-existants)**[et](https://www.privacycommission.be/fr/contrats-existants)**[apportez les changements](https://www.privacycommission.be/fr/contrats-existants)**[necessaires en temps utile.](https://www.privacycommission.be/fr/contrats-existants)

## DPO SPRL comme DPO intérimaire/externe dans votre organisation

La nomination d’un DPO (« Data Protection Officer ») est recommandé par les 3 autorités de protection des données et de la vie privée francophones : la CNIL (France), CNPD (Luxembourg) et CPVP (Belgique) : « Le Délégué à la protection des données : un nouvel intervenant!

Le nouveau Règlement européen relatif à la protection de la vie privée (RGPD) prévoit un nouvel intervenant : le délégué à la protection des données, également appelé Data Protection Officer (DPO).

Le délégué à la protection des données contrôle les traitements de données au sein de son organisation.

À partir du 25 mai 2018, certains responsables du traitement (et/ou sous-traitants) seront obligés de désigner un délégué à la protection des données. Ceux qui ne sont pas soumis à cette obligation ont quand même un intérêt à désigner un tel délégué. Celui-ci jouera en effet un rôle non négligeable dans la politique de protection des données de son organisation. »

<https://www.privacycommission.be/fr/dossier-thematique-delegue-a-la-protection-des-donnees>

« Dans quels cas un organisme doit-il obligatoirement désigner un délégué à la protection des données ?

## La désignation d’un délégué est obligatoire pour :

## Les autorités ou les organismes publics ; et

## Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ; et

## Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors des cas de désignation obligatoire, la désignation d’un délégué à la protection des données est encouragée par les membres du G29. Elle permet en effet de confier à un expert l’identification et la coordination des actions à mener en matière de protection des données personnelles. »

<https://www.cnil.fr/fr/le-cil-et-le-futur-delegue-la-protection-des-donnees>

"Développement de la fonction du délégué à la protection des données

Les organismes publics et les entreprises qui effectuent certains traitements de données à risques (par exemple, des traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ou des traitements à grande échelle de données sensibles) doivent obligatoirement désigner un délégué à la protection des données pour garantir le respect des règles dans le nouveau règlement. Les autres responsables de traitement sont encouragés à désigner eux aussi un délégué à la protection des données.

<https://cnpd.public.lu/fr/charge-protection.html> »

Creativity at its best : no censorship but soft-skills & tools

## DPD/DPO DESIGN

# Les 3 étapes transversales de TOUTE procédure de mise en conformité  et de mission de DPD : DD[[2]](#footnote-2)

L’approche originale  repose sur **3 fondations** :

1. « Legal & IT Design »
2. Intelligence Artificielle ou « IA »
3. Ethique et « Human by Design »

Qui transcendent 3 étapes de toute mission que nous accomplissons :

**Étape 1 : TABLETTE GRAPHIQUE & INTERACTION**

**Les 3 profils de nos équipes (Expert IT/cybersecurity - Juriste – Chef de projet) font l’usage des outils modernes de communication EN INTERNE et EXTERNE : avec les clients et partenaires extérieurs.**

Nous utilisons des tablettes tactiles et des applications graphiques de dessin, mind-mapping, visualisation, advanced natural language generation (advanced NLG), vidéo, story-telling[[3]](#footnote-3),...

There are loads of opportunities but MONEY is not the only goal

Nous dessinons et « sketchons » donc DES REGLES DE DROITS ET DE SECURITE DES SYSTEMES D’INFORMATION – sans la moindre intention que le résultat soit esthétique et communicable tel quel et à ce stade aux différents destinataires (voir étape 3 pour atteindre ce résultat).

La forme de ces compte-rendu de réunions, discussions et réflexions ?

Un schéma, un graphique, une icône, des étapes, un processus, des sanctions ou non selon les choix posés, des avantages financiers mesurables et chiffrés, des gains en termes de réputation, d’analyse des données et d’opérations de marketing ou de communication,…

**Étape 2 : HUMAN BY DESIGN**

Nous appliquons la règle de l’impératif catégorique d’Emmanuel Kant[[4]](#footnote-4) à toute solution proposée et en particulier nous appliquons ce **double test :**

1. Agis seulement d'après la maxime grâce à laquelle tu peux vouloir en même temps qu'elle devienne une **loi universelle**
2. Agis de façon telle que tu traites **l'humanité**, aussi bien dans ta personne que dans toute autre, toujours en même temps **comme fin**, et jamais simplement comme moyen.

Nous passons donc chaque option et - plus encore solution – au crible de cette inévitable - et génératrice de valeurs - évaluation éthique.

En d’autres termes, TOUTE solution JURIDICO/TECHNOLOGIQUE retenue nous satisfait doublement :

1. **Comme DPO/consultant et conseil d’entreprises** commerciales ou organisations à but non lucratif mais entrant nécessairement dans une relation impliquant des flux financiers avec les personnes concernées ; et
2. **Comme personne concernée** : cible des actions envisagées, parent, enfant, citoyen et avatar dans nos vies numériques.

Nous mettons les données personnelles au centre de nos projets et de nos réunions internes, et avec les clients, poursuivons donc l’étape de remue-méninges, de recherche et de visualisation des idées en interaction avec le Règlement, par une analyse des conséquences éthiques de chaque option.

Nous faisons le choix de ne retenir que des solutions qui sont applicables au plus grand nombre et nous satisfont donc comme citoyen d’un univers toujours plus connecté et digital. Nous percevons également le Règlement comme une opportunité commerciale et marketing pour valoriser les données à caractère personnel et développer la confiance des personnes concernées par le respect et la sécurité dans le traitement de celles-ci[[5]](#footnote-5).

Notre test ultime : nous nous mettons à la place de nos enfants pour tester l’option envisagée puis la commentons et l’évaluons comme parent.

NON AUX TERMES JURIDIQUES ET IT INCOMPREHENSIBLES… C’est simplement interdit dès le 25 mai pour toutes les informations à communiquer aux personnes concernées par le Règlement!

Human & Artificial intelligence assists us in delivering state-of-the-art designs

**Étape 3 : VISUALISATION ET REDACTION**

Nous avons préparé durant les deux premières étapes un objectif souhaitable : **Communiquer visuellement après un check éthique**.

Deux solutions externes (humaines et artificielles) vont nous aider à finaliser la communication de manière professionnelle et optimale :

1. Outsourcing graphique design

Nous faisons des appels d’offre en ligne de réalisations graphiques pour professionnaliser la dernière étape du Legal design, les productions visuelles, web, vidéo,… :

<https://www.designcrowd.com> & <https://99designs.fr/> & <https://www.upwork.com/> & <https://www.freelancer.com>

Nos « *sketchs* » sont numériques cf usage de tablettes (si sur papier nous les numérisons) et les partageons donc à nos partenaires designers.

Nos partenaires dans le monde – choisis via les plateformes web de mise en concurrence - finalisent l’objectif du Règlement de « communiquer d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant » (article 12 RGPD : application du principe de TRANSPARENCE). Nous accordons une attention toute particulière à l’iconisation puisque le RGPD l’encourage[[6]](#footnote-6).

1. Intelligence artificielle

Lire : <https://www.dropbox.com/sh/57ucgvg83eg7esf/AABXFs-yGaHX-E_JPcvtrIbPa?dl=0>

“*Tout comme l'électricité a transformé un secteur industriel après l'autre il y a une siècle, l'Intelligence artificielle fera de même à présent.”* Andrew Ng, ancien responsable scientifique du groupe chinois Baidu (en 2017)

Nous invitons l’AI dans le processus de REDACTION des différents documents et textes destinés aux personnes concernées et destinataires cf : https://textio.com/.

Nous utilisons des outils de rédaction AI qui transforment le langage juridique en langage clair cf dossiers Harvard Business Review et La libre Belgique[[7]](#footnote-7) sur le sujet reprenant de très beaux exemples de sociétés la proposant.

L’AI est par ailleurs développée et utilisée dans les processus de formation des DPO, de solutions augmentée de DPO (Data Privacy Box[[8]](#footnote-8) Dfakto[[9]](#footnote-9) et DPObots[[10]](#footnote-10)), de marketing et prospection commerciale[[11]](#footnote-11) et de communication interne (Dfakto est une solution data analytique pour gérer de projets de grande envergure en grand nombre[[12]](#footnote-12)).

1. « Délivrables » optimisés selon les 3 étapes et les 2 solutions externes de la 3ème

Nous paraphrasons l’article 32 du Règlement relatif à la Sécurité du traitement des données[[13]](#footnote-13) pour en faire notre objectif de communication légale :

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte, des finalités et des destinataires de la communication légale et de sa conformité optimale au Règlement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques concernées par la communication, nous mettons en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de communication adapté au risque et le plus conforme au Règlement, y compris entre autres, selon les besoins du client.

## Comment créer de la valeur ensemble ?

### Un regard neuf

Porter un regard neuf sur la relation que vous nouez avec vos clients et voir dans le RGPD une opportunité de construire une nouvelle relation de **confiance**, de **transparence** et **d'ouverture** affecte positivement l'expérience client et développe leur fidélité (et permet d’éviter des amende administratives pour non-respect du Règlement qui se chiffrent en dizaines de millions d'euros!).

Steve Wood, sous-commissaire de l’autorité de contrôle de Grande-Bretagne, a déclaré:

"Les informations personnelles devenant la monnaie par laquelle nos société font des affaires, les organisations doivent faire des droits des consommateurs à la protection des données une priorité. Mettre la protection des données au centre des stratégies des entreprises numériques est la clé de l'amélioration de la **confiance** et de la croissance numérique. "

Il ajouta:

"Les changements apportés à la législation sur la protection des données, qui incluent l'introduction du GDPR, offrent aux organisations une opportunité de se réengager vis-à-vis de leurs clients à propos des données. Les nouvelles réglementations exigent que les organisations soient plus responsables de la protection des données, ce qui constitue un réel engagement à placer le consommateur au cœur des affaires. "**[[14]](#footnote-14)**

Cette relation unique que seules les plus grandes entreprises, ou les meilleures… ou agiles… ou évolutives, ont pu construire, résulte d’une vision commune partagée par tous les membres de votre entreprise : **« Nous mettons tout en œuvre pour protéger vos données, les traiter de manière loyale et transparente et vous informer en permanence. »**

Un traitement loyal des données collectées auprès des particuliers signifie aussi que les responsables du traitement sont prêts à aller au-delà des obligations légales minimales de service envers la personne concernée, si les intérêts légitimes de celle-ci le requièrent.

En termes de marketing direct, cela implique de veiller à ce que les personnes dont vous utilisez les données sont conscientes qu'elles peuvent recevoir des offres marketing de votre part. Vous devez également les informer si vous prévoyez de partager vos bases de données à d'autres organisations et comment vous allez contacter ces personnes : par courrier, téléphone, courrier électronique,...

La FEDERATION EUROPEENNE DE MARKETING DIRECT défini le MARKETING DIRECT comme « La communication par quel moyen que ce soit (comprenant de manière non limitative le courrier, la télécopie, le téléphone, les services en ligne, etc.) de toute offre de publicité ou marketing, qui est réalisée par le professionnel même ou sous sa responsabilité et qui s'adresse à des particuliers. »

La définition de marketing direct couvre donc tous les moyens de communication et ne se limite pas aux formes traditionnelles de commercialisation telles que la télévente ou les mailshots, et s'étend au marketing en ligne, aux réseaux sociaux ou d'autres canaux émergents de communication.

Examinez les listes utilisées pour vos opérations de marketing direct et les processus de suppression des personnes concernées de ces listes (y compris celles qui sont exploitées au nom et/ou pour compte de votre organisation par des partenaires et fournisseurs de services) pour vous assurer qu'ils respectent le RGPD.

Bien que le RGPD vise clairement des appels téléphoniques, courriels et textes, il peut s'appliquer à tout type de marketing direct.

**Voici la nouvelle culture suggérée dans nos entreprises : « Le consommateur est au centre de nos préoccupations et nous considérons son identité digitale comme le plus important actif de sa personnalité à l’ère digitale. »**

[https://iconewsblog.files.wordpress.com/2013/12/sw.jpg?resize=64%2C64](https://iconewsblog.files.wordpress.com/2013/12/sw.jpg?resize=64%2C64%20)

“Whatever the size of your organisation, GDPR is essentially about trust.  Building trusted relationships with the public will enable you to sustainably build your use of data and gain more value. Through changing their data handling culture, organisations can derive new value from customer relationships”.

[**Steve Wood**](http://iconewsblog.wordpress.com/category/steve-wood/) is Deputy Commissioner for Policy and responsible for the ICO’s policy position on the proper application of information rights law and good practice, through lines to take, guidance, internal training, advice and specific projects.

S’agissant de services internet, les caractéristiques des systèmes de traitement de données doivent permettre aux personnes concernées de véritablement comprendre ce qu’il va advenir de leurs données.

« La pierre angulaire du nouveau règlement européen est (en effet) la notion de **confiance**: **confiance** dans le responsable de traitement à traiter les informations personnelles de façon responsable et **confiance** que les règles seront efficacement appliquées. Il incombe à la CNPD ensemble avec les autres autorités de contrôle européennes de générer cette **confiance**. »*[[15]](#footnote-15)*

C’est pour cela que le **GDPR** pourrait aussi se référer à **une Grande Dame qui Protège et Rassure**… dans nos activités les plus intimes et essentielles : internet, cloud compting, big data, réseaux sociaux, Internet of Things, uberisation, les sites de rencontre, les clubs privés, nos vies et orientations sexuelles, nos choix politiques et syndicaux, notre santé,…

L'INTERNET que vous expérimentez est aussi unique que votre empreinte digitale.

Les sites Web qui se sont imposés dans nos vies ordinaires et notre vocabulaires ont commencé à comprendre quel genre de personnes nous sommes. En développant des algorithmes qui tracent (« suivent ») nos comportements en ligne, les entreprises technologiques ont créé des expériences en ligne qui sont profondément personnelles et autodéterminées.[[16]](#footnote-16)

### réunion en vie reelle

Nous renonçons à toute offre de prix « standard » et donc détachée des réalités de votre organisation.

Nous avons mis au point divers outils informatiques qui permettent de réaliser dès notre première réunion :

1. Un diagnostic complet de votre organisation en termes de conformité au GDPR et de son niveau de maturité Cybersécurité ; et
2. Un rapport précis des tâches à accomplir ; et
3. Un projet de lettre de missions ; et
4. Un devis scindé selon votre demande en fonction de :
   1. Consultance/Assistance conformité au GDPR et/ou assistance à un DPO interne
   2. Mission de DPO
   3. Taille de votre organisation
   4. Risques isolés
   5. Préférence pour un paiement « frontal » (« one-shot ») ou un abonnement qui « lisse » les coûts de l’intervention ; et
5. Des actions concrètes à développer afin de valoriser les traitement des données révélés grâce aux points 1 à 4 à des fins de création de valeur pour votre organisation (prospection, information, marketing, recrutement, fidélisation, récolte de fonds,…)

Cette réunion et ses 5 services livrables (« *deliverables* »), réalisés en votre entreprise, sont facturés au prix de 850 euros HTVA et sont imputés sur les premiers honoraires convenus en cas de mission.

Vous pouvez également solliciter une première réunion en nos bureaux (Avenue Brugmann 183 à 1190 Forest) pour une simple discussion ouverte et sans engagement ni facturation en fixant rdv en ligne : *Pour fixer rendez-vous/ To Book online:* [*http://ow.ly/PqGw30a5Zyo*](http://ow.ly/PqGw30a5Zyo) *&* [*https://www.facebook.com/lawrightallright/*](https://www.facebook.com/lawrightallright/)ou en appelant le 02 643 11 00 ou TELEPHONE de KRISTINA.

# ENGLISH

1. What is the GDPR?

The General Data Protection Regulation (GDPR) represents the most significant legislative change in 20 years. Directly applicable in the 31 countries of the European Economic Area (the 28 Member States of the European Union (EU) and three of the four Member States of the European Free Trade Association), it is imposed in an identical way everywhere and without intervention of each Member State to insert it into its legislative arsenal.

It extends and reinforces the rights of the persons concerned, our clients if we are actors of social or private profit organizations, in terms of transparency in the treatment of their personal data, especially if they are sensitive or if they concern children.

The Internet, the cloud, host our personal data from the most "ordinary" (name, profession, residence, telephone, email addresses,...) to the most "sensitive" (political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data, relating to health or concerning sexual life or sexual orientation).

We are asking to be, to become... or to remain, masters of our digital identities which must also be adequately protected from multiple malicious people.

The data collected are now limited in many ways: the consent required is thus caparisoned (free, specific, informed, unambiguous and strictly necessary for the services) and really armoured if it concerns particular categories of personal data, genetic or biometric data (explicit).

The purposes of collecting and processing this data are limited, and the data are minimised to what must be collected to achieve these objectives. The accuracy and retention period of data are also subject to specific and particularly binding measures such as the right to withdrawal of consent, erasure or rectification.

Confidentiality and security must also be guaranteed from the design of the good or service and, by default, only personal data that are strictly necessary for each specific purpose of processing are proposed and processed.

Pseudonymisation" (or anonymisation) and "encryption" are encouraged and clearly defined, while new rights are emerging such as the portability of data which must now be provided in a structured, commonly used and readable format and without the controller to whom the personal data have been communicated being able to prevent it.

Personal data benefit from additional protection in the event of cross-border processing under strict inspection by supervisory authorities with previously unheard of powers of sanctions of up to 20 MB euros (or 4% of annual worldwide turnover)!

The fear of any data controller, and therefore ultimately of any company that collects data, is more than ever to be a victim of a violation of personal data.

The "identifiable natural person" is none other than ourselves in our multiple digital interactions, on the net or by e-mail, via servers or in the cloud, by automated processes or not,...

1. Why should you care?

The DGPS concerns any company established in the European Union but also:

(A) the supply of goods or services to the persons concerned in the Union whether or not payment is required from such persons; or

B) the monitoring of the conduct of such persons, in so far as it is conduct which takes place within the Union.

Automatically, without further information, the Regulation enters into force on 25 May 2018: <http://www.eugdpr.org/>.

Each organisation which has not complied by that date is liable to administrative fines of up to EUR 20 000 000 or, in the case of an undertaking, up to 4 % of the previous year's total worldwide annual turnover, whichever is the higher.

Each undertaking - for profit or not - must provide each person concerned with the information that it has the right to lodge a complaint with a supervisory authority.

Since violations of personal data are growing exponentially rather than diminishing or becoming extinct, and information has never been so easy to share between a large number of people if not the entire planet, let's bet that our companies are exposed to numerous communications of data from people protected by the GPDM to control authorities...

3. What are the opportunities offered by the DGMP?

For us, opportunities are more numerous and inspiring than constraints or new or intensified obligations.

Companies that see the RGPD as a burden will stay docked or even sink while those that see it as an opportunity to bring a breath of fresh air will sail all out (http://www.cityam.com/268997/business-which-treat-gdpr-burden-get-left-behind).

Most companies currently lack rules, techniques, people, practices and procedures to guarantee the rights and freedoms of digital consumers.

They are often indolent and lack vision in the medium and long term regarding the processing and storage of these data. Their teams communicate little on the subject and this concern is not shared by all (but on the contrary limited to legal and IT services).

The DGMP is based entirely on the TRUST that it creates or grows between a company and its customers.

The DSMP creates a new environment that creates new experiences for consumers: more than ever their consent must be informed and the use of their data strictly regulated.

It also makes it possible to bring a company together, to unite the members of many departments concerned, around a common vision of good practices in terms of personal data processing.

Like a beacon in the icy night of the tsunami that our increasingly digital modern economies are passing through, the DGMP shines and guides us towards a new clarity and transparency.

Clearly, the objectives of the European Union are to create a strong digital market in which consumer confidence in the companies responsible for processing, and their subcontractors, is guaranteed... And can even become exemplary and inspiring for the rest of the world.

4. When is the European Regulation applicable?

The Regulation is applicable from 25 May 2018 (Article 99.2 of the Regulation) in all European Union countries.

The applications, expressions of consent, files and other data processing already implemented on that date must, by that date, be brought into line with the provisions of the Regulation.

Your company's compliance often requires more than "checking" boxes without adopting new management and reporting tools, methods and policies. The cost of NOT complying is extremely high.

5. GDPR and DPO offer you consultancy services

A. AUDITS & CONSULTANCY

The reporting obligations to the supervisory authorities are abolished as of 25 May 2018. They are replaced by compliance and liability requirements and are accompanied by (very) heavy dissuasive sanctions.

The Regulation increases the rights of data subjects, increases the reporting obligations to supervisory authorities and data subjects in the event of data breaches and imposes more severe sanctions.

Assessing the number, type and skills of human, material, financial and information resources to ensure the "GDPR compliance" project is the starting point of any compliance approach to the DGMP.

Will prior declaration of treatment remain mandatory upon application of the DSAR (May 25, 2018)?

No. The DGPS removes this prior obligation to declare processing operations to the Data Protection Authority but requires that a Register of processing activities be kept. This Register is an internal tool and should be provided to the supervisory authority on first request. This tool enables data controllers and processors to identify the processing operations carried out and to facilitate compliance of these operations with the DGPS.

Source: points 33 et seq. of recommendation 06/2017[1].

Our companies GDPR SPRL and DPO SPRL therefore aim to accompany you throughout the 3 major stages of data processing: 1) the definition of data to be collected and the evaluation of these 2) their lawful processing 3) reporting and responsibility towards the supervisory authorities.

Ensure that a comprehensive compliance program is designed for your organization and incorporates features such as:

1. impact assessments relating to data processing,

2. regular audits,

3. Revisions and updates to policies and procedures, including HR,

4. training and awareness programs.

To guarantee a high level of personal data protection at all times, set up internal procedures that guarantee data protection at all times, taking into account all events that may occur during the life of a data processing operation (e.g. security breach, management of requests for rectification or access, modification of data collected, change of provider).

Organizing and DOCUMENTING processes involves in particular:

1. to take into account the protection of personal data from the design stage (Article 25) of an application or processing (minimisation of data collection with regard to the purpose, cookies, storage period, information mentions, collection of consent, data security and confidentiality, ensuring the role and responsibility of the actors involved in the implementation of data processing, etc.). To do this, rely on the advice of the Data Protection Officer;
2. to raise awareness and organize the feedback by building a training and communication plan with your employees;
3. to deal with complaints and requests from data subjects concerning the exercise of their rights (rights of access, rectification, opposition, right to portability, withdrawal of consent) by defining the actors and procedures (the exercise of rights must be possible by electronic means, if the data have been collected by this means) (Articles 15-23);
4. anticipate data breaches by providing, in certain cases, for notification to the data protection authority within 72 hours and to the persons concerned as soon as possible (Articles 33+34)[2].

From your declarations of confidentiality or consent to notifications of violations of personal data, including the keeping of the register of processing activities and the appointment of the appropriate data protection officer, we assist you in all the obligations imposed by the Regulation.

We adopt the approach as close as possible to that recommended by the data protection authorities and in particular that of the Commission de Protection de la Vie Privée :

### LEGAL ADVICE AND COUNSEL FOR COMPLIANCE WITH THE GDPR

Two "worth the gold" recommendations

1. Conduct a data protection impact assessment ("DPIA"); and

2. Appoint a Data Protection Officer with all the advantages this represents for your company cf : https://www.linkedin.com/pulse/dpos-job-rockn-roll-christophe-boeraeve/?trackingId=CPPEMv9gSZ8N0Xd4gfsNMA%3D%3D & https://www.linkedin.com/pulse/le-d%C3%A9l%C3%A9gu%C3%A9-%C3%A0-data-protection%C3%A9es-ou-dpd-christophe-boeraeve/

3 complementary approaches

Two functions not covered are missing in the offers made to companies, public authorities and social profit organizations: 1) Project management and 2) Cybersecurity cf: https://www.linkedin.com/pulse/les-paradise-papers-r%C3%A9v%C3%A8lent-des-montages-fiscale-une-boeraeve/ & <https://www.linkedin.com/pulse/paradise-papers-reveal-international-arrangements-tax-boeraeve/>

According to us, here are the 3 necessary and sufficient axes to ensure your conformity:

As always, the Regulation will require 3 distinct and convergent approaches to achieve this highly desirable objective: data backup and protection:

1. Legal and legal approach. Instructions, and other articles of law guide us along a path that does not really include a permanent and final arrival; and

2. Computer/technological approach. Information technology, network and computer means and resources articulate the response to hackers' wishes to harm or to simple incidents or accidents that can lead to data loss/alterations. These are both hardware and software solutions; and

3. Organizational/human approach. The first two solutions, cold as legal codes or electronic machines can be, are (still today) always designed and operated by human beings. Procedures, policies and other instructions or checklists organise legal and technical solutions by bringing together those concerned with data protection in the company.

Establish a relationship with the Data Protection Authority

Our approach, based on the 6 c's or "checks" method also differs in that we wish to contact and question the Data Protection Authority (the "gendarme") on an ongoing basis cf : http /www.law-right.com/fr/notre-cabinet/6-checks-pour-optimiser-votre-dossier/ & Law Right - La Méthode des 6C (6 checks) - YouTube.

While waiting to be able to certify your organisation (provided for by the Regulation but we will have to wait until the APD organises it and we are in Belgium), only the "gendarme" - and no consultant - is able to reassure you and guarantee you this conformity.

To discover the new composition, competences and operating rules of the new Data

Protection Authority in Belgium :

https://www.linkedin.com/pulse/quel-est-limpact-de-la-loi-cr%C3%A9ant-lautorit%C3%A9-des-donn%C3%A9es-boeraeve/ & https://www.linkedin.com/pulse/loi-portant-cr%C3%A9ation-de-lautorit%C3%A9-protection-des-donn%C3%A9es-boeraeve/ .

Intrusion Testing in collaboration with the Data Protection Authority

Re: technological approach, we propose that you first carry out a "Penetration Test" or "Intrusion Test": https://fr.wikipedia.org/wiki/Test\_d%27intrusion: method of evaluation ("audit" in English) of the security of a computer system or network or Information System; it is carried out by a tester, ("pentester" in English).

The results are always shared, evaluated and at the source of the changes initiated, implemented and tested regularly. The envisaged and decided solutions are validated in advance by the Data Protection Authority, up to 4 according to the original Conformity4 method.

We therefore accompany you in your compliance journey by verifying it during 13 steps (in Belgium): https://www.privacycommission.be/fr/preparez-vous-en-13-etapes :

1. Awareness raising

✅ Inform key people and decision-makers of the changes.

2. Data register

✅ Make an inventory of the treatments you perform.

3. Data Protection Officer

✅ Appoint a DPO (if necessary) or representative.

4. Communication

✅ Assess your privacy statement and modify it if necessary.

5. Rights of the data subject

✅ Check if current procedures provide for all rights.

6. Request for access

✅ Think about how you will handle access requests.

7. Legal basis

✅ Identify the legal basis for each treatment.

8. Consent

✅ Assess how you seek and record consent.

9. Children

✅ Develop systems that check the age of the person concerned.

10. Data Leaks

✅ Plan procedures for detecting, reporting and analyzing data leaks.

11. Data protection from design and AIPD

✅ Consider how these concepts can be implemented.

12. International

✅ Determine which control authority you report to.

13. Existing contracts

✅ Evaluate your existing contracts and make the necessary changes in a timely manner.

6. DPO SPRL as interim/external DPO in your organisation

The appointment of a DPO ("Data Protection Officer") is recommended by the 3 French-speaking data protection and privacy authorities: the CNIL (France), CNPD (Luxembourg) and CPVP (Belgium): "The Data Protection Officer: a new speaker!

The new European Data Protection Regulation (EDPR) provides for a new actor: the Data Protection Officer (DPO).

The Data Protection Officer supervises data processing within his organisation.

From 25 May 2018, some controllers (and/or processors) will be obliged to appoint a Data Protection Officer. Those who are not subject to this obligation still have an interest in appointing such a delegate. The latter will indeed play a significant role in his organisation's data protection policy.

https://www.privacycommission.be/fr/dossier-thematique-delegue-a-la-protection-des-donnees

"In what cases must an organization appoint a data protection officer?

The appointment of a delegate is mandatory for:

1. Public authorities or agencies; and

2. Organizations whose core activities involve regular and systematic monitoring of people on a large scale; and

3. Organizations whose core activities require them to process on a large scale so-called "sensitive" data or data relating to criminal convictions and offences.

Apart from mandatory appointments, the appointment of a Data Protection Officer is encouraged by G29 members. It makes it possible to entrust an expert with the identification and coordination of the actions to be taken with regard to the protection of personal data.

https://www.cnil.fr/fr/le-cil-et-le-futur-delegue-la-protection-des-donnees

"Development of the function of the Data Protection Officer

Public bodies and undertakings which carry out certain processing operations involving data at risk (for example, processing operations requiring regular and systematic large-scale monitoring of data subjects or large-scale processing of sensitive data) must appoint a data protection officer to ensure compliance with the rules in the new Regulation. Other controllers are also encouraged to appoint a Data Protection Officer.

https://cnpd.public.lu/fr/charge-protection.html".

4. DPD/DPO DESIGN

The 3 transversal stages of ANY compliance and DPO mission procedure: DD

The original approach is based on 3 foundations:

1) Legal & IT Design

2) Artificial Intelligence or "AI

3) Ethics and Human by Design

That transcend 3 stages of any mission we accomplish:

Step 1: GRAPHIC TABLE & INTERACTION

The 3 profiles of our teams (IT/cybersecurity Expert - Lawyer - Project Manager) make use of modern tools of communication INTERNAL and EXTERNAL: with external clients and partners.

We use tactile tablets and graphic applications for drawing, mind-mapping, visualization, advanced natural language generation (advanced NLG), video, storytelling,...

We therefore draw and "sketch" RULES OF RIGHTS AND SECURITY OF INFORMATION SYSTEMS - without the slightest intention that the result be aesthetic and communicable as it is and at this stage to the various recipients (see step 3 to achieve this result).

The form of these minutes of meetings, discussions and reflections?

A diagram, a graph, an icon, steps, a process, sanctions or not depending on the choices made, measurable and quantified financial benefits, gains in terms of reputation, data analysis and marketing or communication operations,...

Step 2: HUMAN BY DESIGN

We apply Emmanuel Kant's categorical imperative rule to any proposed solution and in particular we apply this double test:

1. Act only according to the maxim by which you can want it to become a universal law at the same time.

2. Act in such a way that you treat humanity, as well in your person as in any other, always at the same time as an end, and never simply as a means.

We therefore pass each option and - even more so - through the sieve of this inevitable - and values-generating - ethical evaluation.

In other words, EVERY JURIDICO/TECHNOLOGICAL solution chosen satisfies us doubly:

1. As a DPO/consultant and advisor to commercial enterprises or non-profit organisations but necessarily entering into a relationship involving financial flows with the persons concerned; and

2. As concerned person: target of the actions envisaged, parent, child, citizen and avatar in our digital lives.

We put personal data at the centre of our projects and internal meetings, and with clients, we therefore continue the stage of brainstorming, researching and visualising ideas in interaction with the Regulation, by analysing the ethical consequences of each option.

We choose only solutions that are applicable to the greatest number and therefore satisfy us as citizens of an increasingly connected and digital world. We also see the Regulation as a commercial and marketing opportunity to enhance the value of personal data and develop the confidence of those concerned by respect and security in the processing of such data.

Our ultimate test: we put ourselves in our children's shoes to test the option considered, then comment on it and evaluate it as a parent.

NO TO LEGAL TERMS AND INCOMPREHENSIVE IT... It is simply prohibited from 25 May for all information to be communicated to the persons concerned by the Regulation!

Step 3: VISUALIZATION AND REDACTION

During the first two stages, we prepared a desirable objective: Communicate visually after an ethical check.

Two external solutions (human and artificial) will help us to finalize the communication in a professional and optimal way:

1. Graphic design outsourcing

We make online tenders of graphic creations to professionalize the last stage of Legal design, visual, web, video productions,... :

https://www.designcrowd.com & https://99designs.fr/ & https://www.upwork.com/ & https://www.freelancer.com

Our "sketches" are digital cf use of tablets (if on paper we digitize them) and therefore share them with our designer partners.

Our partners around the world - chosen via web-based competition platforms - finalise the Regulation's objective of "communicating in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms, in particular for any information specifically intended for a child" (Article 12 GSR: application of the principle of TRANSPARENCY). We pay particular attention to iconization since the DGMP encourages it.

2. Artificial intelligence

Read: https://www.dropbox.com/sh/57ucgvg83eg7esf/AABXFs-yGaHX-E\_JPcvtrIbPa?dl=0

"Just as electricity transformed one industrial sector after another a century ago, so will artificial intelligence now." Andrew Ng, former Chief Scientist of the Chinese Baidu Group (in 2017)

We invite the IA in the process of REDACTION of the various documents and texts intended for the persons concerned and recipients cf : https://textio.com/.

We use AI writing tools that transform legal language into plain language, see Harvard Business Review and La libre Belgique dossiers on the subject, which include very good examples of companies offering it.

AI is also developed and used in DPO training processes, enhanced DPO solutions (Data Privacy Box Dfakto and DPObots), marketing and sales prospecting and internal communication (Dfakto is an analytical data solution to manage large scale projects in large numbers).

3. « Deliverables " optimized according to the 3 steps and 2 external solutions of the 3rd

We paraphrase Article 32 of the Data Processing Security Regulation to make it our legal communication objective:

Taking into account the state of knowledge, the implementation costs and the nature, scope, context, purposes and recipients of the legal communication and its optimal compliance with the Regulation, as well as the risks, the probability and seriousness of which vary, for the rights and freedoms of the natural persons concerned by the communication, we implement the appropriate technical and organisational measures in order to guarantee a level of communication adapted to the risk and most in conformity with the Regulation, including among others, according to the client's needs.

8. How to create value together?

A. A FRESH LOOK

Taking a fresh look at the relationship you build with your customers and seeing in the RGPD an opportunity to build a new relationship of trust, transparency and openness positively affects the customer experience and develops their loyalty (and helps avoid administrative fines for non-compliance with the Regulation which amount to tens of millions of euros!).

Steve Wood, Deputy Commissioner of the British Supervisory Authority, said:

"As personal information becomes the currency through which our societies do business, organizations must make consumer rights to data protection a priority. Putting data protection at the centre of digital business strategies is the key to improving trust and digital growth.

He added:

"Changes to data protection legislation, including the introduction of the GDPR, offer organizations an opportunity to re-engage with their customers about data. New regulations require organizations to be more responsible for data protection, which is a real commitment to putting the consumer at the heart of business.

This unique relationship that only the largest companies, or the best... or agile... or evolving, have been able to build, results from a common vision shared by all members of your company: "We do everything possible to protect your data, treat them fairly and transparently and keep you constantly informed.

Fair processing of data collected from individuals also means that data controllers are prepared to go beyond the minimum legal service obligations towards the data subject, if the data subject's legitimate interests so require.

In terms of direct marketing, this means ensuring that the people whose data you use are aware that they may receive marketing offers from you. You should also inform them if you plan to share your databases with other organizations and how you will contact these people: by mail, phone, e-mail,...

The EUROPEAN DIRECT MARKETING FEDERATION defines DIRECT MARKETING as "the communication by whatever means (including but not limited to mail, fax, telephone, online services, etc.) of any advertising or marketing offer, which is made by the professional himself or under his responsibility and which is addressed to individuals".

The definition of direct marketing therefore covers all means of communication and is not limited to traditional forms of marketing such as telemarketing or mailshots, and extends to online marketing, social networks or other emerging communication channels.

Review the lists used for your direct marketing operations and the processes for removing individuals from these lists (including those operated on behalf and/or on behalf of your organization by partners and service providers) to ensure that they comply with the PDR.

While the PDNMR clearly targets telephone calls, e-mails and text, it can be applied to any type of direct marketing.

Here is the new culture suggested in our companies: "The consumer is at the centre of our concerns and we consider his digital identity as the most important asset of his personality in the digital age.

https://iconewsblog.files.wordpress.com/2013/12/sw.jpg?resize=64%2C64

"Whatever the size of your organisation, GDPR is essentially about trust. Building trusted relationships with the public will enable you to sustainably build your use of data and gain more value. Through changing their data handling culture, organisations can derive new value from customer relationships".

Steve Wood is Deputy Commissioner for Policy and responsible for the ICO's policy position on the proper application of information rights law and good practice, through lines to take, guidance, internal training, advice and specific projects.

As Internet services, the characteristics of the data processing systems must enable the data subjects to truly understand what will happen to their data.

"The cornerstone of the new European regulation is (indeed) the notion of trust: trust in the controller to handle personal information responsibly and trust that the rules will be effectively applied. It is up to the NCDP together with the other European supervisory authorities to generate this confidence.

This is why the GDPR could also refer to a Great Lady who Protects and Reassure... in our most intimate and essential activities: internet, cloud counting, big data, social networks, Internet of Things, uberisation, dating sites, private clubs, our lives and sexual orientations, our political and trade union choices, our health,...

The INTERNET you experience is as unique as your fingerprint.

The websites that have imposed themselves in our ordinary lives and our vocabularies have begun to understand what kind of people we are. By developing algorithms that track ("track") our online behaviours, technology companies have created online experiences that are deeply personal and self-determined.

B. MEETING IN REAL LIFE

We renounce any "standard" price offer and thus detached from the realities of your organization.

We have developed various computer tools that make it possible to carry out from our first meeting:

1) A complete diagnosis of your organization in terms of GDPR compliance and maturity level Cybersecurity; and

2) A precise report of the tasks to be accomplished; and

3) A draft engagement letter; and

4) An estimate split according to your request according to :

a. Consultancy/Assistance with GDPR compliance and/or assistance to an internal DPO

b. DPO's mission

c. Size of your organization

d. Isolated risks

e. Preference for a "one-shot" payment or subscription that "smoothes" intervention costs; and

5) Concrete actions to develop in order to enhance the processing of the data revealed thanks to points 1 to 4 for purposes of creating value for your organization (prospecting, information, marketing, recruitment, loyalty, fundraising,...)

This meeting and its 5 deliverable services, performed in your company, are invoiced at the price of 850 euros excluding VAT and are deducted from the first agreed fees in case of mission.

You can also request a first meeting in our offices (Avenue Brugmann 183 to 1190 Forest) for a simple open discussion and without obligation or billing by booking an appointment online: To Book online: http://ow.ly/PqGw30a5Zyo & https://www.facebook.com/lawrightallright/ or by calling 02 643 11 00 or TELEPHONE from KRISTINA.

# DUTCH

1. Wat is het BBPR?

De algemene verordening gegevensbescherming (GDPR) is de belangrijkste wetswijziging in 20 jaar. De richtlijn is rechtstreeks van toepassing in de 31 landen van de Europese Economische Ruimte (de 28 lidstaten van de Europese Unie (EU) en drie van de vier lidstaten van de Europese Vrijhandelsassociatie) en wordt overal en zonder tussenkomst van elke lidstaat op identieke wijze opgelegd om in zijn wetgevingsarsenaal te worden opgenomen.

Het breidt de rechten uit en versterkt die van de betrokken personen, onze klanten als wij actoren zijn van sociale of private profit organisaties, in termen van transparantie in de behandeling van hun persoonlijke gegevens, vooral als ze gevoelig zijn of als het kinderen betreft.

Het internet, de wolk, host onze persoonlijke gegevens van de meest "gewone" (naam, beroep, verblijf, telefoon, e-mailadressen,...) tot de meest "gevoelige" (politieke opvattingen, religieuze of filosofische overtuigingen of vakbondslidmaatschap, genetische of biometrische gegevens, met betrekking tot gezondheid of met betrekking tot seksueel leven of seksuele geaardheid).

We vragen om meesters van onze digitale identiteiten te zijn, te worden... of te blijven, die ook adequaat moeten worden beschermd tegen meerdere kwaadwillige mensen.

De verzamelde gegevens zijn nu op velerlei manieren beperkt: de vereiste toestemming is dus gecaparonneerd (gratis, specifiek, geïnformeerd, ondubbelzinnig en strikt noodzakelijk voor de diensten) en echt gepantserd als het gaat om bepaalde categorieën van persoonsgegevens, genetische of biometrische gegevens (expliciet).

De doeleinden van het verzamelen en verwerken van deze gegevens zijn beperkt, en de gegevens zijn geminimaliseerd tot wat moet worden verzameld om deze doelstellingen te bereiken. De nauwkeurigheid en de bewaartermijn van gegevens zijn ook onderworpen aan specifieke en bijzonder bindende maatregelen, zoals het recht om toestemming in te trekken, te wissen of te corrigeren.

Vertrouwelijkheid en veiligheid moeten ook worden gegarandeerd vanaf het ontwerp van het goed of de dienst en, standaard, worden alleen persoonsgegevens voorgesteld en verwerkt die strikt noodzakelijk zijn voor elk specifiek doel van de verwerking.

Pseudonimisering" (of anonimisering) en "encryptie" worden aangemoedigd en duidelijk gedefinieerd, terwijl zich nieuwe rechten aandienen, zoals de meeneembaarheid van gegevens, die nu in een gestructureerd, algemeen gebruikt en leesbaar formaat moeten worden verstrekt, zonder dat de voor de verwerking verantwoordelijke aan wie de persoonsgegevens zijn verstrekt, deze kan voorkomen.

Persoonsgegevens genieten extra bescherming bij grensoverschrijdende verwerking onder strenge controle van toezichthoudende instanties met tot nu toe ongekende sanctiebevoegdheden tot 20 MB euro (of 4% van de jaarlijkse wereldwijde omzet)!

De angst van elke verantwoordelijke voor de verwerking, en dus uiteindelijk van elk bedrijf dat gegevens verzamelt, is meer dan ooit het slachtoffer van een schending van persoonsgegevens.

De "identificeerbare natuurlijke persoon" is niemand minder dan wijzelf in onze meervoudige digitale interacties, op het net of via e-mail, via servers of in de cloud, al dan niet geautomatiseerd,...

2. Waarom zou je geven?

Het DGPS heeft betrekking op elke onderneming die in de Europese Unie is gevestigd, maar ook op ondernemingen die in de Europese Unie zijn gevestigd:

A) goederenleveringen of diensten verricht voor de betrokkenen in de Unie, ongeacht of daarvoor al dan niet een vergoeding verlangd wordt; of

B) het toezicht op het gedrag van deze personen, voor zover dit gedrag binnen de Unie plaatsvindt.

De verordening treedt automatisch, zonder verdere informatie, in werking op 25 mei 2018: http://www.eugdpr.org/.

Elke organisatie die op die datum nog niet aan de eisen heeft voldaan, wordt bestraft met administratieve geldboeten van maximaal 20 000 000 EUR of, in het geval van een onderneming, maximaal 4 % van de totale wereldwijde jaaromzet van het voorgaande jaar, waarbij het hoogste bedrag in aanmerking wordt genomen.

1. Iedere onderneming moet, al dan niet met winstoogmerk, aan iedere betrokkene de inlichtingen verstrekken waarover zij beschikt om bij een toezichthoudende autoriteit een klacht in te dienen.

Aangezien schendingen van persoonsgegevens exponentieel toenemen in plaats van afnemen of uitsterven, en informatie nog nooit zo gemakkelijk te delen is geweest tussen een groot aantal mensen, zo niet de hele planeet, wedden we dat onze bedrijven worden blootgesteld aan talloze communicatie van gegevens van mensen die beschermd worden door de GPDM aan de controle-instanties ...

3. Welke mogelijkheden biedt het DGMP?

Voor ons zijn de kansen talrijker en inspirerender dan beperkingen of nieuwe of aangescherpte verplichtingen.

Bedrijven die de RGPD als een last zien, zullen in het dok blijven of zelfs zinken, terwijl bedrijven die de RGPD als een kans zien om een frisse wind te laten waaien, zullen uitzeilen (http://www.cityam.com/268997/business-which-treat-gdpr-burden-get-left-behind).

De meeste bedrijven hebben momenteel een gebrek aan regels, technieken, mensen, praktijken en procedures om de rechten en vrijheden van digitale consumenten te garanderen.

Zij zijn vaak indolent en hebben op middellange en lange termijn geen visie op de verwerking en opslag van deze gegevens. Hun teams communiceren weinig over het onderwerp en deze zorg wordt niet gedeeld door iedereen (maar in tegendeel beperkt tot juridische en IT-diensten).

Het DGMP is volledig gebaseerd op het TRUST dat het opricht of groeit tussen een bedrijf en zijn klanten.

Het DSMP creëert een nieuwe omgeving die nieuwe ervaringen creëert voor consumenten: meer dan ooit moet hun toestemming worden geïnformeerd en moet het gebruik van hun gegevens strikt worden gereguleerd.

Het maakt het ook mogelijk om een bedrijf samen te brengen, om de leden van vele betrokken afdelingen te verenigen, rond een gemeenschappelijke visie van goede praktijken op het gebied van de verwerking van persoonsgegevens.

Als een baken in de ijzige nacht van de tsunami die onze steeds digitaler wordende moderne economieën doormaken, schittert en begeleidt het DGMP ons naar een nieuwe helderheid en transparantie.

Het is duidelijk dat de Europese Unie tot doel heeft een sterke digitale markt tot stand te brengen waarin het vertrouwen van de consument in de verwerkingsbedrijven en hun onderaannemers gewaarborgd is... En zelfs tot voorbeeld kan strekken en inspirerend kan zijn voor de rest van de wereld.

4. Wanneer is de Europese verordening van toepassing?

De verordening is van toepassing met ingang van 25 mei 2018 (artikel 99, lid 2, van de verordening) in alle landen van de Europese Unie.

De aanvragen, kennisgevingen van toestemming, dossiers en andere gegevensverwerkingen die op die datum reeds ten uitvoer zijn gelegd, moeten uiterlijk op die datum in overeenstemming zijn gebracht met de bepalingen van de verordening.

Voor de compliance van uw bedrijf is vaak meer nodig dan het "aanvinken" van vakjes, zonder dat u nieuwe beheer- en rapportagetools, -methoden en -beleidslijnen hoeft in te voeren. De kosten om NIET aan de eisen te voldoen zijn extreem hoog.

5. GDPR en DPO bieden u adviesdiensten aan

A. AUDITS & ADVISERING

De rapportageverplichtingen aan de toezichthouders worden per 25 mei 2018 afgeschaft. Zij worden vervangen door nalevings- en aansprakelijkheidsvoorschriften en gaan vergezeld van (zeer) zware afschrikkende sancties.

De verordening versterkt de rechten van de betrokkenen, versterkt de meldingsplicht aan de toezichthoudende autoriteiten en de betrokkenen bij inbreuken op de gegevensbescherming en legt strengere sancties op.

Het beoordelen van het aantal, het type en de vaardigheden van de personele, materiële, financiële en informatiemiddelen om ervoor te zorgen dat het GDPR-conformiteitsproject het uitgangspunt vormt van elke nalevingsaanpak van het DGMP.

Blijft voorafgaande verklaring van behandeling verplicht bij toepassing van het DSAR (25 mei 2018)?

Nee. Het DGPS schaft deze voorafgaande verplichting om verwerkingen aan te melden bij de gegevensbeschermingsautoriteit af, maar eist dat een register van verwerkingen wordt bijgehouden. Dit register is een intern instrument en dient op eerste verzoek aan de toezichthoudende autoriteit te worden verstrekt. Met dit hulpmiddel kunnen de voor de verwerking verantwoordelijken en de verwerkers de verrichte verwerkingen identificeren en de naleving van het DGPS bij deze verwerkingen vergemakkelijken.

Bron: punten 33 e.v. van aanbeveling 06/2017[1].

Onze bedrijven GDPR SPRL en DPO SPRL streven er daarom naar om u te begeleiden in de 3 belangrijkste stadia van de gegevensverwerking: 1) de definitie van de te verzamelen gegevens en de evaluatie van deze 2) hun rechtmatige verwerking 3) rapportage en verantwoordelijkheid naar de toezichthoudende autoriteiten.

Zorg ervoor dat er een uitgebreid complianceprogramma is ontworpen voor uw organisatie en dat het functies bevat zoals:

1. effectbeoordelingen met betrekking tot gegevensverwerking,

2. regelmatige audits,

3. Herzieningen en actualiseringen van beleidslijnen en procedures, met inbegrip van HR,

4. opleidings- en bewustmakingsprogramma's.

Om te allen tijde een hoog niveau van bescherming van persoonsgegevens te waarborgen, moeten interne procedures worden ingevoerd die te allen tijde gegevensbescherming garanderen, waarbij rekening wordt gehouden met alle gebeurtenissen die zich tijdens de levensduur van een gegevensverwerking kunnen voordoen (bv. inbreuk op de beveiliging, beheer van verzoeken om rectificatie of toegang, wijziging van verzamelde gegevens, verandering van aanbieder).

Bij het organiseren en DOCUMENTING-processen gaat het met name om:

rekening te houden met de bescherming van persoonsgegevens vanaf het ontwerpstadium (artikel 25) van een aanvraag of verwerking (minimalisering van de gegevensverzameling met betrekking tot het doel, cookies, opslagtermijn, vermelding van informatie, verzameling van toestemming, gegevensbeveiliging en vertrouwelijkheid, waarborging van de rol en verantwoordelijkheid van de actoren die betrokken zijn bij de uitvoering van de gegevensverwerking, enz. Vertrouw hiervoor op het advies van de functionaris voor gegevensbescherming;

om het bewustzijn te verhogen en de feedback te organiseren door een trainings- en communicatieplan op te stellen met uw medewerkers;

klachten en verzoeken van betrokkenen in verband met de uitoefening van hun rechten (recht van toegang, rectificatie, verzet, recht van meeneembaarheid, intrekking van toestemming) te behandelen door de actoren en procedures vast te stellen (de uitoefening van rechten moet langs elektronische weg mogelijk zijn indien de gegevens op deze wijze zijn verzameld) (artikelen 15-23);

te anticiperen op gegevensinbreuken door in bepaalde gevallen de gegevensbeschermingsautoriteit binnen 72 uur en de betrokken personen zo spoedig mogelijk in kennis te stellen (artikelen 33+34)2 .

Vanaf uw verklaringen van vertrouwelijkheid of toestemming tot kennisgevingen van schendingen van persoonsgegevens, met inbegrip van het bijhouden van het register van verwerkingsactiviteiten en de aanstelling van de geschikte functionaris voor gegevensbescherming, helpen wij u bij alle verplichtingen die door de verordening worden opgelegd.

We kiezen voor een aanpak die zo dicht mogelijk ligt bij de aanpak die wordt aanbevolen door de gegevensbeschermingsautoriteiten en in het bijzonder die van de Commission de Protection de la Vie Privée :

B. JURIDISCH ADVIES EN RAAD VOOR DE NALEVING VAN DE GDPR

Twee gouden aanbevelingen

1. een effectbeoordeling inzake gegevensbescherming ("DPIA") uit te voeren; en

2. Benoem een functionaris voor gegevensbescherming met alle voordelen die dit voor uw bedrijf betekent, cf. https://www.linkedin.com/pulse/dpos-job-rockn-roll-christophe-boeraeve/?trackingId=CPPEMv9gSZ8N0Xd4gfsNMA%3D%3D & https://www.linkedin.com/pulse/le-d%C3%A9l%C3%A9gu%C3%A9-%C3%A0-dataprotectie%C3%A9es-ou-dpd-christophe-boeraeve/

3 complementaire benaderingen

In de aanbiedingen aan bedrijven, overheden en social profit-organisaties ontbreken twee functies: 1) projectmanagement en 2) cyberbeveiliging, zie: https://www.linkedin.com/pulse/les-paradise-papers-r%C3%A9v%C3%A8lent-des-montages-fiscale-une-boeraeve/ & https://www.linkedin.com/pulse/paradise-papers-reveal-international-arrangements-tax-boeraeve/

Volgens ons zijn hier de 3 noodzakelijke en voldoende assen om uw conformiteit te waarborgen:

Zoals altijd vereist de verordening drie verschillende en convergerende benaderingen om dit zeer wenselijke doel te bereiken: gegevensback-up en -bescherming:

1. Juridische en juridische benadering. Instructies en andere artikelen van de wet leiden ons langs een pad dat niet echt een permanente en definitieve aankomst omvat; en

2. Computer-technologische benadering. Informatietechnologie, netwerk- en computermiddelen en -hulpmiddelen verwoorden de reactie op hackers' wensen om schade te berokkenen of op eenvoudige incidenten of ongevallen die kunnen leiden tot gegevensverlies/wijzigingen. Dit zijn zowel hardware- als softwareoplossingen; en

3. Organisatorische/humane aanpak. De eerste twee oplossingen, hoe koud wetboeken of elektronische machines ook mogen zijn, worden (nog steeds) altijd door mensen ontworpen en bediend. Procedures, beleidsregels en andere instructies of controlelijsten organiseren juridische en technische oplossingen door degenen die betrokken zijn bij gegevensbescherming in het bedrijf samen te brengen.

Totstandbrenging van een relatie met de gegevensbeschermingsautoriteit.

Onze aanpak, gebaseerd op de 6 c's of "controles" methode verschilt ook in dat we willen contact opnemen met en vraagtekens plaatsen bij de autoriteit voor gegevensbescherming (de "gendarme") op een continue basis zie: http /www.law-right.com/fr/notre-cabinet/6-checks-pour-optimiser-votre-dossier/ & Recht - La Méthode des 6C (6 controles) - YouTube.

In afwachting van de certificering van uw organisatie (zoals voorzien in de verordening, maar we zullen moeten wachten tot de APD deze organiseert en we in België zijn), kan alleen de "gendarme" - en geen enkele consultant - u deze conformiteit garanderen.

De nieuwe samenstelling, bevoegdheden en werkingsregels van de nieuwe Gegevensbeschermingsautoriteit in België ontdekken:

https://www.linkedin.com/pulse/quel-est-limpact-de-la-loi-cr%C3%A9ant-lautorit%C3%A9-des-donn%C3%A9es-boeraeve/ & https://www.linkedin.com/pulse/loi-portant-cr%C3%A9ation-de-lautorit%C3%A9-bescherming-des-donn%C3%A9es-boeraeve/ .

Intrusietests in samenwerking met de gegevensbeschermingsautoriteit

Wat de technologische aanpak betreft, stellen wij voor dat u eerst een "Penetration Test" of "Intrusion Test" uitvoert: https://fr.wikipedia.org/wiki/Test\_d%27 inbraak: evaluatiemethode ("audit" in het Engels) van de veiligheid van een computersysteem, netwerk of informatiesysteem; deze wordt uitgevoerd door een tester ("pentester" in het Engels).

De resultaten worden altijd gedeeld, geëvalueerd en aan de bron van de veranderingen geïnitieerd, geïmplementeerd en regelmatig getest. De beoogde en overeengekomen oplossingen worden vooraf gevalideerd door de gegevensbeschermingsautoriteit, maximaal 4 volgens de oorspronkelijke conformiteitsmethode4.

Wij begeleiden u daarom in naleving door het te controleren in 13 stappen (in België): https://www.privacycommission.be/fr/preparez-vous-en-13-etapes :

1. Bewustmaking

✅ Belangrijke personen en besluitvormers informeren over de veranderingen.

2. Dataregister

✅ Inventariseer de behandelingen die u uitvoert.

3. Functionaris voor gegevensbescherming

✅ Benoem een DPO (indien nodig) of vertegenwoordiger.

4. Communicatie

✅ Beoordeel uw privacyverklaring en wijzig deze indien nodig.

5. Rechten van de betrokkene

✅ Controleer of de huidige procedures alle rechten toestaan.

6. Verzoek om toegang

✅ Denk na over hoe u toegangsverzoeken gaat afhandelen.

7. Rechtsgrondslag

✅ Vermeld de rechtsgrondslag voor elke behandeling.

8. Toestemmen

✅ Beoordelen hoe u toestemming vraagt en vastleggen.

9. Kinderen

✅ Ontwikkelen van systemen die de leeftijd van de betrokkene controleren.

10. Datalekken

✅ Plan procedures voor het detecteren, rapporteren en analyseren van datalekken.

11. Gegevensbescherming tegen ontwerp en AIPD

✅ Denk na over hoe deze concepten kunnen worden geïmplementeerd.

12. Internationaal

✅ Bepaal aan welke controlerende instantie u rapporteert.

13. Bestaande contracten

✅ Evalueer uw bestaande contracten en breng tijdig de nodige wijzigingen aan.

6. DPO SPRL als interim/externe DPO in uw organisatie

De benoeming van een DPO ("Gegevensbeschermingsfunctionaris") wordt aanbevolen door de 3 Franstalige gegevensbeschermings- en privacybeschermingsautoriteiten: de CNIL (Frankrijk), CNPD (Luxemburg) en CPVP (België): "De Gegevensbeschermingsfunctionaris: een nieuwe spreker!

De nieuwe Europese verordening inzake gegevensbescherming (EDPR) voorziet in een nieuwe actor: de functionaris voor gegevensbescherming (DPO).

De functionaris voor gegevensbescherming houdt toezicht op de gegevensverwerking binnen zijn organisatie.

Vanaf 25 mei 2018 zullen sommige voor de verwerking verantwoordelijken (en/of verwerkers) verplicht zijn een functionaris voor gegevensbescherming aan te wijzen. Degenen die niet onder deze verplichting vallen, hebben er nog steeds belang bij een dergelijke afgevaardigde te benoemen. Dit laatste zal inderdaad een belangrijke rol spelen in het gegevensbeschermingsbeleid van zijn organisatie.

https://www.privacycommission.be/fr/dossier-thematique-delegue-a-la-protection-des-donnees

"In welke gevallen moet een organisatie een functionaris voor gegevensbescherming aanstellen?

De aanstelling van een afgevaardigde is verplicht voor:

1. overheidsinstanties of -agentschappen; en

2. Organisaties die zich richten op het regelmatig en systematisch monitoren van mensen op grote schaal; en

3. Organisaties die voor hun kernactiviteiten op grote schaal zogenaamde "gevoelige" gegevens of gegevens in verband met strafrechtelijke veroordelingen en strafbare feiten moeten verwerken.

Afgezien van verplichte benoemingen wordt de benoeming van een functionaris voor gegevensbescherming door G29-leden aangemoedigd. Het maakt het mogelijk een deskundige te belasten met de identificatie en coördinatie van de maatregelen die moeten worden genomen met betrekking tot de bescherming van persoonsgegevens.

https://www.cnil.fr/fr/le-cil-et-le-futur-delegue-la-protection-des-donnees

"Ontwikkeling van de functie van de functionaris voor gegevensbescherming

Overheidsinstanties en ondernemingen die bepaalde verwerkingen met betrekking tot risicovolle gegevens uitvoeren (bijvoorbeeld verwerkingen die een regelmatige en systematische grootschalige controle van de betrokkenen of een grootschalige verwerking van gevoelige gegevens vereisen), moeten een functionaris voor gegevensbescherming aanstellen om ervoor te zorgen dat de regels van de nieuwe verordening worden nageleefd. Andere voor de verwerking verantwoordelijken worden ook aangemoedigd een functionaris voor gegevensbescherming aan te stellen.

https://cnpd.public.lu/fr/charge-protection.html".

4. DPD/DPO DESIGN

De 3 transversale fasen van de procedure voor naleving door de ANY's en de DPO-missie: DD

De oorspronkelijke aanpak is gebaseerd op 3 fundamenten:

1) Juridisch & IT-ontwerp

2) Kunstmatige intelligentie of "AI

3) Ethiek en menselijk ontwerp

Dat overstijgt 3 stadia van elke missie die we volbrengen:

Stap 1: GRAFISCHE TABEL & INTERACTIE

De 3 profielen van onze teams (IT/cybersecurity Expert - Advocaat - Project Manager) maken gebruik van moderne communicatiemiddelen INTERNAL en EXTERNAL: met externe klanten en partners.

We gebruiken tactiele tablets en grafische toepassingen voor tekenen, mind-mapping, visualisatie, geavanceerde natuurlijke taalgeneratie (geavanceerde NLG), video, storytelling,...

Daarom tekenen en "schetsen" we de REGLEMENTEN van de RECHTEN EN BEVEILIGINGSYSTEMEN - zonder de geringste bedoeling dat het resultaat esthetisch zou zijn en op dit moment overdraagbaar aan de verschillende ontvangers (zie stap 3 om dit resultaat te bereiken).

De vorm van deze notulen van vergaderingen, discussies en beschouwingen?

Een diagram, een grafiek, een icoon, stappen, een proces, sancties of niet afhankelijk van de gemaakte keuzes, meetbare en gekwantificeerde financiële voordelen, voordelen op het gebied van reputatie, data-analyse en marketing- of communicatieactiviteiten, ....

Stap 2: HUMAN BY DESIGN

We passen de categoriale dwingende regel van Emmanuel Kant toe op elke voorgestelde oplossing en in het bijzonder passen we deze dubbele test toe:

1. Handel alleen volgens de stelregel waarmee je wilt dat het tegelijkertijd een universele wet wordt.

2. Handel zo dat je de mensheid, zowel in je persoon als in ieder ander, altijd tegelijk als doel en nooit simpelweg als middel behandelt.

We passeren daarom elke optie en - nog meer - door de zeef van deze onvermijdelijke - en waarden genererende - ethische evaluatie.

Met andere woorden, de gekozen EVERY JURIDICO/TECHNOLOGICAL-oplossing voldoet in twee opzichten aan onze verwachtingen:

1. 1. Als functionaris voor gegevensbescherming/adviseur en adviseur van handelsondernemingen of non-profitorganisaties die noodzakelijkerwijs een relatie met de betrokken personen aangaan waarbij geldstromen betrokken zijn; en

2. Als betrokken persoon: doelwit van de geplande acties, ouder, kind, burger en avatar in ons digitale leven.

We plaatsen persoonsgegevens centraal in onze projecten en interne vergaderingen en met klanten zetten we daarom de fase van brainstormen, onderzoeken en visualiseren van ideeën in wisselwerking met de verordening voort, door de ethische gevolgen van elke optie te analyseren.

We kiezen alleen oplossingen die voor zoveel mogelijk mensen toepasbaar zijn en die ons als burgers van een steeds meer verbonden en digitale wereld tevreden stellen. We zien de verordening ook als een commerciële en marketingkans om de waarde van persoonsgegevens te vergroten en het vertrouwen van degenen die betrokken zijn bij het respect voor en de veiligheid van de verwerking van dergelijke gegevens te ontwikkelen.

Onze ultieme test: we zetten onszelf in de schoenen van onze kinderen om de optie in kwestie te testen, er commentaar op te geven en het te evalueren als een ouder.

GEEN WIJZIGINGSTOFFEN EN INCOMPREHENSIT... Het is ten strengste verboden om vanaf 25 mei alle inlichtingen te verstrekken aan de personen die betrokken zijn bij de verordening!

Stap 3: VISUALIZATIE EN REDACTIE

In de eerste twee fasen hebben we een wenselijke doelstelling voorbereid: visueel communiceren na een ethische toetsing.

Twee externe oplossingen (menselijk en kunstmatig) zullen ons helpen om de communicatie op een professionele en optimale manier af te ronden:

1. Grafisch ontwerp uitbesteden

Wij maken online offertes van grafische creaties om de laatste fase van Legal design, visual, web, video producties, ... te professionaliseren :

https://www.designcrowd.com & https://99designs.fr/ & https://www.upwork.com/ & https://www.freelancer.com

Onze "schetsen" zijn digitaal cf gebruik van tablets (als we ze op papier digitaliseren) en delen ze daarom met onze ontwerperpartners.

Onze partners over de hele wereld - geselecteerd via webgebaseerde concurrentieplatforms - leggen de laatste hand aan de doelstelling van de verordening om "op beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke wijze, in duidelijke en eenvoudige bewoordingen te communiceren, in het bijzonder voor alle informatie die specifiek voor een kind is bestemd" (artikel 12 van de GSR: toepassing van het beginsel van TRANSPARENCY). We besteden bijzondere aandacht aan de iconisering, aangezien het DGMP dit aanmoedigt.

2. Kunstmatige intelligentie

Lees: https://www.dropbox.com/sh/57ucgvg83eg7esf/AABXFs-yGaHX-E\_JPcvtrIbPa?dl=0

"Net zoals elektriciteit een eeuw geleden de ene industriële sector na de andere transformeerde, zal kunstmatige intelligentie dat nu ook zijn. Andrew Ng, voormalig wetenschappelijk hoofd van de Chinese Baidu-groep (in 2017)

Wij nodigen de effectbeoordelingsautoriteit uit om in de procedure van REDACTIE de verschillende documenten en teksten voor de betrokken personen en ontvangers te raadplegen (zie: https://textio.com/.

We gebruiken AI-schrijfwaren om juridische taal om te zetten in gewone taal, zie de dossiers van Harvard Business Review en La libre Belgique over dit onderwerp, die zeer goede voorbeelden bevatten van bedrijven die het aanbieden.

AI wordt ook ontwikkeld en gebruikt in DPO-opleidingsprocessen, verbeterde DPO-oplossingen (Data Privacy Box Dfakto en DPObots), marketing- en verkoopprospectie en interne communicatie (Dfakto is een oplossing voor analytische gegevens om grootschalige projecten in grote aantallen te beheren).

3. « Deliverables " geoptimaliseerd volgens de 3 stappen en 2 externe oplossingen van de 3e

We parafraseren artikel 32 van de verordening betreffende de beveiliging van gegevensverwerking om er onze juridische communicatiedoelstelling van te maken:

Rekening houdend met de stand van de kennis, de uitvoeringskosten, de aard, de omvang, de context, de doeleinden en de ontvangers van de juridische communicatie en de optimale naleving van de verordening, alsook met de risico's waarvan de waarschijnlijkheid en de ernst variëren, nemen wij voor de rechten en vrijheden van de bij de communicatie betrokken natuurlijke personen de nodige technische en organisatorische maatregelen om een communicatieniveau te waarborgen dat is aangepast aan het risico en dat het meest in overeenstemming is met de verordening, onder meer overeenkomstig de behoeften van de cliënt.

8. Hoe creëert u samen waarde?

A. EEN FRISSE UITSTRALING

Een frisse blik op de relatie die u opbouwt met uw klanten en het zien in het RGPD van een kans om een nieuwe relatie van vertrouwen, transparantie en openheid op te bouwen heeft een positief effect op de klantervaring en ontwikkelt hun loyaliteit (en helpt administratieve boetes voor niet-naleving van de verordening, die oplopen tot tientallen miljoenen euro's te voorkomen!).

Steve Wood, adjunct-commissaris van de Britse toezichthoudende autoriteit, zei hierover:

"Naarmate persoonlijke informatie het betaalmiddel wordt waarmee onze samenlevingen zaken doen, moeten organisaties prioriteit geven aan de rechten van de consument op gegevensbescherming. Gegevensbescherming centraal stellen in digitale bedrijfsstrategieën is de sleutel tot het verbeteren van het vertrouwen en de digitale groei.

Hij voegde eraan toe:

"Veranderingen in de wetgeving op het gebied van gegevensbescherming, met inbegrip van de invoering van het GDPR, bieden organisaties de mogelijkheid om opnieuw met hun klanten in gesprek te gaan over gegevens. Nieuwe regelgeving vereist dat organisaties verantwoordelijker zijn voor gegevensbescherming, wat een echte verplichting is om de consument centraal te stellen in het bedrijfsleven.

Deze unieke relatie die alleen de grootste bedrijven, of de beste ... of wendbare ... of in ontwikkeling, hebben kunnen opbouwen, vloeit voort uit een gemeenschappelijke visie die door alle leden van uw bedrijf wordt gedeeld: "Wij doen er alles aan om uw gegevens te beschermen, eerlijk en transparant te behandelen en u voortdurend op de hoogte te houden.

Eerlijke verwerking van bij natuurlijke personen verzamelde gegevens betekent ook dat de voor de verwerking verantwoordelijken bereid zijn verder te gaan dan de minimale wettelijke dienstverplichtingen jegens de betrokkene, indien de gerechtvaardigde belangen van de betrokkene dit vereisen.

Op het gebied van direct marketing betekent dit dat u ervoor moet zorgen dat de mensen van wie u de gegevens gebruikt weten dat ze marketingaanbiedingen van u kunnen ontvangen. U dient hen ook te informeren als u van plan bent om uw databases te delen met andere organisaties en hoe u deze mensen zult contacteren: per post, telefoon, e-mail,...

In de RICHTLIJN VAN DE EUROPESE RICHTLIJN wordt RICHTLIJNSMARKETERING gedefinieerd als "de mededeling met welk middel dan ook (met inbegrip van, maar niet beperkt tot, post, fax, telefoon, on-linediensten, enz.) van elk reclame- of marketingaanbod dat door de beroepsbeoefenaar zelf of onder zijn verantwoordelijkheid wordt gedaan en dat tot individuele personen is gericht".

De definitie van direct marketing omvat derhalve alle communicatiemiddelen en is niet beperkt tot traditionele vormen van marketing zoals telemarketing of mailshots, en strekt zich uit tot onlinemarketing, sociale netwerken of andere opkomende communicatiekanalen.

Controleer de lijsten die worden gebruikt voor uw directmarketingactiviteiten en de processen om personen van deze lijsten te verwijderen (met inbegrip van de lijsten die namens en/of namens uw organisatie worden beheerd door partners en serviceproviders) om te verzekeren dat deze in overeenstemming zijn met de PDR.

Hoewel het PDNMR zich duidelijk richt op telefoongesprekken, e-mails en tekst, kan het worden toegepast op elke vorm van direct marketing.

Hier is de nieuwe cultuur die in onze bedrijven wordt gesuggereerd: "De consument staat in het middelpunt van onze zorgen en wij beschouwen zijn digitale identiteit als de belangrijkste troef van zijn persoonlijkheid in het digitale tijdperk.

https://iconewsblog.files.wordpress.com/2013/12/sw.jpg?resize=64%2C64

"Wat de grootte van uw organisatie ook is, GDPR draait in wezen om vertrouwen. Het opbouwen van vertrouwensrelaties met het publiek stelt u in staat uw gebruik van gegevens duurzaam op te bouwen en meer waarde te creëren. Door hun dataverwerkingscultuur te veranderen, kunnen organisaties nieuwe waarde ontlenen aan klantrelaties".

Steve Wood is Plaatsvervangend Commissaris voor Beleid en verantwoordelijk voor het beleidsstandpunt van het ICO inzake de correcte toepassing van de wetgeving inzake informatierechten en goede praktijken, via te volgen lijnen, begeleiding, interne opleiding, advies en specifieke projecten.

Als internetdiensten moeten de kenmerken van de gegevensverwerkingssystemen de betrokkenen in staat stellen werkelijk te begrijpen wat er met hun gegevens zal gebeuren.

"De hoeksteen van de nieuwe Europese verordening is (inderdaad) het begrip vertrouwen: vertrouwen in de voor de verwerking verantwoordelijke om op verantwoorde wijze met persoonsgegevens om te gaan en vertrouwen dat de regels effectief worden toegepast. Het is aan het NCDP om samen met de andere Europese toezichthouders dit vertrouwen te wekken.

Daarom zou het GDPR ook kunnen verwijzen naar een dame die beschermt en motiveert... in onze meest intieme en essentiële activiteiten: internet, wolkentelling, big data, sociale netwerken, internet van de dingen, uberisatie, datingsites, privé-clubs, ons leven en onze seksuele geaardheid, onze politieke en vakbondskeuzes, onze gezondheid,...

Het INTERNET dat u ervaart is net zo uniek als uw vingerafdruk.

De websites die zich hebben opgedrongen in ons gewone leven en onze vocabulaires zijn beginnen te begrijpen wat voor mensen we zijn. Door algoritmen te ontwikkelen die ons online gedrag volgen ("track"), hebben technologiebedrijven online ervaringen gecreëerd die diep persoonlijk en zelfbepaald zijn.

B. ONTMOETING IN HET ECHTE LEVEN

Wij zien af van een "standaard" prijsaanbieding en staan daarmee los van de realiteit van uw organisatie.

We hebben verschillende informatica-instrumenten ontwikkeld die het mogelijk maken om vanaf onze eerste vergadering uit te voeren:

1) Een volledige diagnose van uw organisatie in termen van GDPR-compliance en volwassenheidsniveau Cybersecurity; en

2) een nauwkeurig verslag van de uit te voeren taken; en

3) een ontwerp-toezeggingsbrief; en

4) Een uitsplitsing van de schatting volgens uw verzoek volgens :

a. Consultancy/Asistentie bij de naleving van GDPR en/of bijstand aan een interne functionaris voor gegevensbescherming

b. Missie van de functionaris voor gegevensbescherming

c. Omvang van uw organisatie

d. Geïsoleerde risico's

e. Voorkeur voor een eenmalige betaling of abonnement waarmee de interventiekosten worden "afgevlakt"; en

5) Concrete acties om de verwerking van de in de punten 1 tot 4 geopenbaarde gegevens te verbeteren met het oog op het creëren van waarde voor uw organisatie (prospectie, informatie, marketing, rekrutering, loyaliteit, fondsenwerving,...)

Deze vergadering en zijn 5 te leveren diensten, uitgevoerd in uw bedrijf, worden gefactureerd aan de prijs van 850 euro exclusief BTW en worden afgetrokken van de eerste overeengekomen kosten in geval van dienstreizen.

U kunt ook vragen om een eerste vergadering in onze kantoren (Brugmannlaan 183 tot 1190 Vorst) voor een eenvoudige open discussie en zonder verplichting of facturering door het boeken van een afspraak online: Om online te boeken: http://ow.ly/PqGw30a5Zyo & https://www.facebook.com/lawrightallright/ of door te bellen naar 02 643 11 00 of TELEPHONE van KRISTINA.

# GERMAN

1. Was ist die GDPR?

Die Allgemeine Datenschutzverordnung (GDPR) stellt die bedeutendste Gesetzesänderung seit 20 Jahren dar. Direkt anwendbar in den 31 Ländern des Europäischen Wirtschaftsraums (den 28 Mitgliedstaaten der Europäischen Union (EU) und drei der vier Mitgliedstaaten der Europäischen Freihandelsassoziation), wird sie überall und ohne Eingreifen jedes Mitgliedstaates in gleicher Weise auferlegt, um sie in sein legislatives Arsenal aufzunehmen.

Sie erweitert und stärkt die Rechte der Betroffenen, unserer Kunden, wenn wir Akteure sozialer oder privater Profit-Organisationen sind, hinsichtlich der Transparenz im Umgang mit ihren persönlichen Daten, insbesondere wenn sie sensibel sind oder Kinder betreffen.

Das Internet, die Wolke, beherbergt unsere persönlichen Daten von den "gewöhnlichsten" (Name, Beruf, Wohnort, Telefon, E-Mail-Adressen,....) bis zu den "sensibelsten" (politische Meinungen, religiöse oder philosophische Überzeugungen oder Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, die sich auf die Gesundheit oder das Sexualleben oder die sexuelle Orientierung beziehen).

Wir fordern, Herr unserer digitalen Identitäten zu sein, zu werden.... oder zu bleiben, die auch vor mehreren böswilligen Menschen angemessen geschützt werden müssen.

Die gesammelten Daten sind nun in vielerlei Hinsicht begrenzt: Die erforderliche Einwilligung ist somit gekapselt (kostenlos, spezifisch, informiert, eindeutig und für die Dienste unbedingt erforderlich) und wirklich gepanzert, wenn es sich um bestimmte Kategorien von personenbezogenen Daten, genetischen oder biometrischen Daten handelt (explizit).

Die Zwecke der Erhebung und Verarbeitung dieser Daten sind begrenzt, und die Daten werden auf das zur Erreichung dieser Ziele erforderliche Maß beschränkt. Auch die Richtigkeit und Aufbewahrungsfrist der Daten unterliegt besonderen und besonders verbindlichen Maßnahmen wie dem Recht auf Widerruf, Löschung oder Berichtigung.

Vertraulichkeit und Sicherheit müssen auch bei der Gestaltung der Ware oder Dienstleistung gewährleistet sein, und standardmäßig werden nur personenbezogene Daten vorgeschlagen und verarbeitet, die für den jeweiligen Verarbeitungszweck unbedingt erforderlich sind.

Pseudonymisierung" (oder Anonymisierung) und "Verschlüsselung" werden gefördert und klar definiert, während neue Rechte wie die Übertragbarkeit von Daten entstehen, die nun in einem strukturierten, allgemein verwendeten und lesbaren Format bereitgestellt werden müssen, ohne dass der für die Verarbeitung Verantwortliche, dem die personenbezogenen Daten übermittelt wurden, dies verhindern kann.

Personenbezogene Daten genießen zusätzlichen Schutz bei grenzüberschreitender Verarbeitung unter strenger Kontrolle durch Aufsichtsbehörden mit bisher nicht gekannten Sanktionsbefugnissen von bis zu 20 MB Euro (oder 4% des weltweiten Jahresumsatzes)!

Die Angst vor einem Datenverantwortlichen und damit letztlich vor jedem Unternehmen, das Daten sammelt, ist mehr denn je ein Opfer einer Verletzung personenbezogener Daten.

Die "identifizierbare natürliche Person" ist niemand anders als wir selbst in unseren vielfältigen digitalen Interaktionen, im Netz oder per E-Mail, über Server oder in der Cloud, durch automatisierte Prozesse oder nicht,....

2. Warum sollten Sie sich sorgen?

Die DGPS betrifft alle in der Europäischen Union ansässigen Unternehmen, aber auch:

(A) die Lieferung von Waren oder Dienstleistungen an die betroffenen Personen in der Union, unabhängig davon, ob von diesen Personen eine Zahlung verlangt wird oder nicht, oder

B) die Überwachung des Verhaltens dieser Personen, soweit es sich um ein Verhalten innerhalb der Union handelt.

Ohne weitere Informationen tritt die Verordnung automatisch am 25. Mai 2018 in Kraft: http://www.eugdpr.org/.

Jede Organisation, die sich bis zu diesem Zeitpunkt nicht daran gehalten hat, muss mit Geldbußen von bis zu 20 000 000 EUR oder, im Falle eines Unternehmens, bis zu 4 % des gesamten weltweiten Jahresumsatzes des Vorjahres rechnen, je nachdem, welcher Betrag höher ist.

Jedes Unternehmen - ob mit oder ohne Gewinn - muss jedem Betroffenen mitteilen, dass es das Recht hat, eine Beschwerde bei einer Aufsichtsbehörde einzureichen.

Da Verstöße gegen personenbezogene Daten exponentiell zunehmen und nicht abnehmen oder aussterben, und es noch nie so einfach war, Informationen zwischen einer großen Anzahl von Menschen, wenn nicht gar dem gesamten Planeten, auszutauschen, sollten wir wetten, dass unsere Unternehmen einer Vielzahl von Datenübertragungen von Personen ausgesetzt sind, die durch den GPDM geschützt sind....

3. Welche Möglichkeiten bietet die DGMP?

Für uns sind die Möglichkeiten zahlreicher und inspirierender als Zwänge oder neue oder verschärfte Verpflichtungen.

Unternehmen, die das RGPD als Belastung sehen, bleiben angedockt oder sinken sogar, während diejenigen, die es als Chance sehen, frischen Wind zu bringen, alles ausfahren (http://www.cityam.com/268997/business-which-treat-gdpr-burden-get-left-behind).

Den meisten Unternehmen fehlen derzeit Regeln, Techniken, Personen, Praktiken und Verfahren zur Gewährleistung der Rechte und Freiheiten der digitalen Verbraucher.

Sie sind oft träge und haben mittel- und langfristig keine Vision für die Verarbeitung und Speicherung dieser Daten. Ihre Teams kommunizieren wenig über das Thema und dieses Anliegen wird nicht von allen geteilt (im Gegenteil, es beschränkt sich auf Rechts- und IT-Dienstleistungen).

Die DGMP basiert vollständig auf dem Vertrauen, das sie zwischen einem Unternehmen und seinen Kunden schafft oder wächst.

Das DSMP schafft ein neues Umfeld, das neue Erfahrungen für die Verbraucher schafft: Mehr denn je muss ihre Zustimmung eingeholt und die Verwendung ihrer Daten streng geregelt werden.

Sie ermöglicht es auch, ein Unternehmen zusammenzubringen, um die Mitglieder vieler betroffener Abteilungen um eine gemeinsame Vision von guten Praktiken in Bezug auf die Verarbeitung personenbezogener Daten zu vereinen.

Wie ein Leuchtturm in der eisigen Nacht des Tsunami, den unsere zunehmend digitalisierten modernen Volkswirtschaften durchlaufen, glänzt die DGMP und führt uns zu einer neuen Klarheit und Transparenz.

Die Ziele der Europäischen Union sind eindeutig die Schaffung eines starken digitalen Marktes, auf dem das Vertrauen der Verbraucher in die für die Verarbeitung verantwortlichen Unternehmen und ihre Subunternehmer gewährleistet ist.... und der sogar für den Rest der Welt beispielhaft und inspirierend sein kann.

4. Wann ist die Europäische Verordnung anwendbar?

Die Verordnung gilt ab dem 25. Mai 2018 (Artikel 99.2 der Verordnung) in allen Ländern der Europäischen Union.

Die zu diesem Zeitpunkt bereits durchgeführten Anträge, Zustimmungserklärungen, Dateien und sonstigen Datenverarbeitungen müssen bis zu diesem Zeitpunkt mit den Bestimmungen der Verordnung in Einklang gebracht werden.

Die Konformität Ihres Unternehmens erfordert oft mehr als nur das "Ankreuzen" von Kästchen, ohne neue Management- und Reporting-Tools, -Methoden und -Richtlinien einzuführen. Die Kosten der Nichteinhaltung sind extrem hoch.

5. GDPR und DPO bieten Ihnen Beratungsleistungen an

A. PRÜFUNGEN & BERATUNG

Die Meldepflicht gegenüber den Aufsichtsbehörden wird zum 25. Mai 2018 aufgehoben. Sie werden durch Compliance- und Haftungsanforderungen ersetzt und sind mit (sehr) schweren abschreckenden Sanktionen verbunden.

Die Verordnung stärkt die Rechte der betroffenen Personen, erhöht die Meldepflichten gegenüber den Kontrollbehörden und den betroffenen Personen im Falle von Datenschutzverletzungen und sieht strengere Sanktionen vor.

Die Bewertung der Anzahl, Art und Kompetenz der personellen, materiellen, finanziellen und informationellen Ressourcen zur Sicherstellung der "GDPR-Compliance" ist der Ausgangspunkt eines jeden Compliance-Ansatzes der DGMP.

Bleibt die vorherige Erklärung der Behandlung bei Anwendung des DSAR (25. Mai 2018) verbindlich?

Nein. Die DGPS hebt diese vorherige Verpflichtung zur Meldung von Verarbeitungen an die Datenschutzbehörde auf, verlangt jedoch, dass ein Register der Verarbeitungstätigkeiten geführt wird. Dieses Register ist ein internes Instrument und sollte der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden. Dieses Tool ermöglicht es den für die Verarbeitung Verantwortlichen und Verarbeitern, die durchgeführten Vorgänge zu identifizieren und die Übereinstimmung dieser Vorgänge mit dem DGPS zu erleichtern.

Quelle: Punkte 33 ff. der Empfehlung 06/2017[1].

Unsere Unternehmen GDPR SPRL und DPO SPRL sind daher bestrebt, Sie durch die 3 wichtigsten Phasen der Datenverarbeitung zu begleiten: 1) die Definition der zu erhebenden Daten und deren Auswertung 2) ihre rechtmäßige Verarbeitung 3) die Berichterstattung und die Verantwortung gegenüber den Aufsichtsbehörden.

Stellen Sie sicher, dass ein umfassendes Compliance-Programm für Ihr Unternehmen konzipiert ist und Funktionen wie:

1. Folgenabschätzungen im Zusammenhang mit der Datenverarbeitung,

2. regelmäßige Audits,

3. die Überarbeitung und Aktualisierung von Richtlinien und Verfahren, einschließlich HR,

4. Schulungs- und Sensibilisierungsprogramme.

Um jederzeit ein hohes Maß an Schutz personenbezogener Daten zu gewährleisten, sollten interne Verfahren eingerichtet werden, die den Datenschutz jederzeit gewährleisten, wobei alle Ereignisse zu berücksichtigen sind, die während der Dauer einer Datenverarbeitung auftreten können (z.B. Sicherheitsverletzung, Verwaltung von Berichtigungs- oder Zugriffsanfragen, Änderung der erfassten Daten, Providerwechsel).

Das Organisieren und Dokumentieren von Prozessen beinhaltet insbesondere:

den Schutz personenbezogener Daten bereits in der Entwurfsphase (Artikel 25) eines Antrags oder einer Verarbeitung zu berücksichtigen (Minimierung der Datenerhebung in Bezug auf den Zweck, Cookies, Speicherdauer, Erwähnung von Informationen, Einholung der Einwilligung, Datensicherheit und Vertraulichkeit, Gewährleistung der Rolle und Verantwortung der an der Durchführung der Datenverarbeitung beteiligten Akteure usw.). Verlassen Sie sich dabei auf den Rat des Datenschutzbeauftragten;

Sensibilisierung und Organisation des Feedbacks durch Erstellung eines Schulungs- und Kommunikationsplans mit Ihren Mitarbeitern;

Behandlung von Beschwerden und Anträgen von Betroffenen über die Ausübung ihrer Rechte (Zugangsrechte, Berichtigung, Widerspruch, Recht auf Portabilität, Widerruf der Einwilligung) durch Festlegung der Akteure und Verfahren (die Ausübung der Rechte muss auf elektronischem Wege möglich sein, wenn die Daten auf diesem Wege erhoben wurden) (Artikel 15-23);

Datenschutzverletzungen vorzubeugen, indem sie in bestimmten Fällen der Datenschutzbehörde innerhalb von 72 Stunden und den betroffenen Personen so bald wie möglich Mitteilung machen (Artikel 33+34)[2].

Von Ihren Vertraulichkeitserklärungen oder Einwilligungen bis hin zu Mitteilungen über Verstöße gegen personenbezogene Daten, einschließlich der Führung des Registers der Verarbeitungstätigkeiten und der Ernennung des zuständigen Datenschutzbeauftragten, unterstützen wir Sie bei allen Verpflichtungen, die sich aus der Verordnung ergeben.

Wir orientieren uns so weit wie möglich an den Empfehlungen der Datenschutzbehörden und insbesondere der Commission de Protection de la Vie Privée :

B. RECHTSBERATUNG UND BERATUNG BEI DER EINHALTUNG DES GDPR

Zwei "worth the gold"-Empfehlungen

1. Durchführung einer Datenschutzfolgenabschätzung ("DPIA"); und

2. Benennen Sie einen Datenschutzbeauftragten mit allen Vorteilen, die dies für Ihr Unternehmen bedeutet: https://www.linkedin.com/pulse/dpos-job-rockn-roll-christophe-boeraeve/?trackingId=CPPEMv9gSZ8N0Xd4gfsNMA%3D%3D%3D & https://www.linkedin.com/pulse/le-d%C3%A9l%C3%A9gu%C3%A9-%C3%A0-data-protection%C3%A9es-ou-dpd-christophe-boeraeve/

3 komplementäre Ansätze

Zwei nicht abgedeckte Funktionen fehlen in den Angeboten an Unternehmen, Behörden und gemeinnützige Organisationen: 1) Projektmanagement und 2) Cybersecurity siehe: https://www.linkedin.com/pulse/les-paradise-papers-r%C3%A9v%C3%A8lent-des-montages-fiscale-une-boeraeve/ & https://www.linkedin.com/pulse/paradise-papers-reveal-international-arrangements-tax-boeraeve/

Unserer Meinung nach sind hier die 3 notwendigen und ausreichenden Achsen, um Ihre Konformität zu gewährleisten:

Wie immer erfordert die Verordnung drei unterschiedliche und konvergente Ansätze, um dieses höchst wünschenswerte Ziel zu erreichen: Datensicherung und -schutz:

1. Rechtlicher und juristischer Ansatz. Anweisungen und andere Gesetzesartikel führen uns auf einem Weg, der nicht wirklich eine dauerhafte und endgültige Ankunft beinhaltet; und

2. Computer/technologischer Ansatz. Informationstechnologie, Netzwerk- und Computermittel und -ressourcen artikulieren die Reaktion auf den Wunsch von Hackern nach Schaden oder auf einfache Vorfälle oder Unfälle, die zu Datenverlusten/-veränderungen führen können. Dies sind sowohl Hardware- als auch Softwarelösungen; und

3. Organisatorisch/menschlicher Ansatz. Die ersten beiden Lösungen, so kalt wie gesetzliche Vorschriften oder elektronische Maschinen sein können, werden (noch heute) immer von Menschen entworfen und bedient. Verfahren, Richtlinien und andere Anweisungen oder Checklisten organisieren rechtliche und technische Lösungen, indem sie die mit dem Datenschutz im Unternehmen befassten Personen zusammenführen.

Aufbau einer Beziehung mit der Datenschutzbehörde

Unser Ansatz, der auf der 6 c's oder "checks"-Methode basiert, unterscheidet sich auch darin, dass wir die Datenschutzbehörde (den "Gendarmen") laufend kontaktieren und befragen möchten, siehe: http /www.law-right.com/fr/notre-cabinet/6-checks-pour-optimiser-votre-dossier/ & Law Right - La Méthode des 6C (6 checks) - YouTube.

Während wir darauf warten, Ihre Organisation zertifizieren zu können (in der Verordnung vorgesehen, aber wir müssen warten, bis der APD sie organisiert und wir in Belgien sind), kann nur der "Gendarm" - und kein Berater - Sie beruhigen und Ihnen diese Konformität garantieren.

Die neue Zusammensetzung, Zuständigkeiten und Betriebsvorschriften der neuen Datenschutzbehörde in Belgien kennenzulernen :

https://www.linkedin.com/pulse/quel-est-limpact-de-la-loi-cr%C3%A9ant-lautorit%C3%A9-des-donn%C3%A9es-boeraeve/ & https://www.linkedin.com/pulse/loi-portant-cr%C3%A9ation-de-lautorit%C3%A9-protection-des-donn%C3%A9es-boeraeve/ .

Intrusion Testing in Zusammenarbeit mit der Datenschutzbehörde

Re: technologischen Ansatz, schlagen wir vor, dass Sie zunächst einen "Penetration Test" oder "Intrusion Test": https://fr.wikipedia.org/wiki/Test\_d%27intrusion: Methode der Bewertung ("Audit" in Englisch) der Sicherheit eines Computersystems oder Netzwerkes oder Informationssystems; es wird von einem Tester durchgeführt, ("Pentester" in Englisch).

Die Ergebnisse werden immer geteilt, bewertet und an der Quelle der Veränderungen initiiert, umgesetzt und regelmäßig getestet. Die vorgesehenen und beschlossenen Lösungen werden von der Datenschutzbehörde vorab validiert, bis zu 4 nach der ursprünglichen Conformity4-Methode.

Deshalb begleiten wir Sie in 13 Schritten (in Belgien): https://www.privacycommission.be/fr/preparez-vous-en-13-etapes :

1. Bewusstseinsbildung

✅ Informieren Sie Schlüsselpersonen und Entscheidungsträger über die Veränderungen.

2. Datenregister

✅ Machen Sie eine Bestandsaufnahme der von Ihnen durchgeführten Behandlungen.

3. Datenschutzbeauftragter

✅ Benennen Sie einen DSB (falls erforderlich) oder einen Vertreter.

4. Kommunikation

✅ Überprüfen Sie Ihre Datenschutzerklärung und ändern Sie sie gegebenenfalls.

5. Rechte des Betroffenen

✅ Überprüfen Sie, ob die aktuellen Verfahren alle Rechte vorsehen.

6. Antrag auf Zugang

✅ Denken Sie darüber nach, wie Sie mit Zugriffsanfragen umgehen werden.

7. Rechtliche Grundlagen

✅ Identifizieren Sie die rechtlichen Grundlagen für jede Behandlung.

8. Einwilligung

✅ Beurteilen Sie, wie Sie die Einwilligung einholen und aufzeichnen.

9. Kinder

✅ Entwickeln Sie Systeme, die das Alter der betroffenen Person überprüfen.

10. Datenlecks

✅ Planen Sie Verfahren zur Erkennung, Meldung und Analyse von Datenlecks.

11. Datenschutz vor Design und AIPD

✅ Überlegen Sie, wie diese Konzepte umgesetzt werden können.

12. International

✅ Bestimmen Sie, an welche Kontrollstelle Sie sich wenden.

13. Bestehende Verträge

✅ Bewerten Sie Ihre bestehenden Verträge und nehmen Sie rechtzeitig die notwendigen Änderungen vor.

6. DPO SPRL als vorläufiger/externer DPO in Ihrer Organisation

Die Ernennung eines DSB ("Datenschutzbeauftragten") wird von den drei französischsprachigen Datenschutzbehörden CNIL (Frankreich), CNPD (Luxemburg) und CPVP (Belgien) empfohlen: "Der Datenschutzbeauftragte: ein neuer Sprecher!

Die neue europäische Datenschutzverordnung (EDPR) sieht einen neuen Akteur vor: den Datenschutzbeauftragten (DSB).

Der Datenschutzbeauftragte überwacht die Datenverarbeitung innerhalb seiner Organisation.

Ab dem 25. Mai 2018 sind einige für die Verarbeitung Verantwortliche verpflichtet, einen Datenschutzbeauftragten zu ernennen. Diejenigen, die dieser Verpflichtung nicht unterliegen, haben weiterhin ein Interesse an der Ernennung eines solchen Delegierten. Letzterer wird in der Tat eine wichtige Rolle in der Datenschutzpolitik seiner Organisation spielen.

https://www.privacycommission.be/fr/dossier-thematique-delegue-a-la-protection-des-donnees

"In welchen Fällen muss eine Organisation einen Datenschutzbeauftragten ernennen?

Die Ernennung eines Delegierten ist obligatorisch für:

1. Behörden oder Agenturen; und

2. Organisationen, deren Haupttätigkeit die regelmäßige und systematische Überwachung von Menschen in großem Umfang ist; und

3. Organisationen, deren Kernaufgaben es erfordern, in großem Umfang so genannte "sensible" Daten oder Daten zu strafrechtlichen Verurteilungen und Straftaten zu verarbeiten.

Abgesehen von den obligatorischen Ernennungen wird die Ernennung eines Datenschutzbeauftragten von den G29-Mitgliedern unterstützt. Sie ermöglicht es, einen Experten mit der Identifizierung und Koordinierung der Maßnahmen zum Schutz personenbezogener Daten zu beauftragen.

https://www.cnil.fr/fr/le-cil-et-le-futur-delegue-la-protection-des-donnees

"Entwicklung der Funktion des Datenschutzbeauftragten

Öffentliche Stellen und Unternehmen, die bestimmte Verarbeitungen mit gefährdeten Daten durchführen (z. B. Verarbeitungen, die eine regelmäßige und systematische umfassende Überwachung der betroffenen Personen oder eine umfassende Verarbeitung sensibler Daten erfordern), müssen einen Datenschutzbeauftragten benennen, um die Einhaltung der Vorschriften der neuen Verordnung zu gewährleisten. Auch andere für die Verarbeitung Verantwortliche werden aufgefordert, einen Datenschutzbeauftragten zu ernennen.

https://cnpd.public.lu/fr/charge-protection.html".

4. DPD/DPO DESIGN

Die 3 transversalen Stufen JEDER Compliance- und DPO-Missionsprozedur: DD

Der ursprüngliche Ansatz basiert auf 3 Fundamenten:

1) Rechtliches & IT-Design

2) Künstliche Intelligenz oder "AI

3) Ethik und Mensch durch Design

Das übersteigt 3 Stufen jeder Mission, die wir erfüllen:

Schritt 1: GRAFIK-TISCH & INTERAKTION

Die 3 Profile unserer Teams (IT/cybersecurity Expert - Lawyer - Project Manager) nutzen moderne Kommunikationsmittel INTERNAL und EXTERN: mit externen Kunden und Partnern.

Wir verwenden taktile Tabletts und grafische Anwendungen für das Zeichnen, Mind-mapping, Visualisierung, erweiterte natürliche Sprachgenerierung (advanced NLG), Video, Storytelling,....

Wir zeichnen und "skizzieren" daher RECHTS- UND INFORMATIONSSYSTEME - ohne die geringste Absicht, dass das Ergebnis so ästhetisch und kommunizierbar ist, wie es ist, und zu diesem Zeitpunkt an die verschiedenen Empfänger (siehe Schritt 3, um dieses Ergebnis zu erreichen).

Die Form dieser Sitzungsprotokolle, Diskussionen und Überlegungen?

Ein Diagramm, ein Diagramm, ein Symbol, Schritte, ein Prozess, Sanktionen oder nicht abhängig von den getroffenen Entscheidungen, messbare und quantifizierte finanzielle Vorteile, Gewinne in Bezug auf Reputation, Datenanalyse und Marketing oder Kommunikationsmaßnahmen,....

Schritt 2: HUMAN BY DESIGN

Wir wenden die kategorische Imperativregel von Emmanuel Kant auf jeden Lösungsvorschlag an und wenden insbesondere diesen Doppeltest an:

1. Handeln Sie nur nach der Maxime, nach der Sie wollen, dass es gleichzeitig ein universelles Gesetz wird.

2. Handeln Sie so, dass Sie die Menschheit, sowohl in Ihrer Person als auch in jeder anderen Person, immer zur gleichen Zeit als Zweck und niemals einfach als Mittel behandeln.

Wir gehen daher jede Option und - noch mehr - durch das Sieb dieser unvermeidlichen - und wertschöpfenden - ethischen Bewertung.

Mit anderen Worten, JEDE gewählte JURIDICO/TECHNOLOGISCHE Lösung erfüllt uns doppelt:

1. als DPO/Berater und Berater von Wirtschaftsunternehmen oder Non-Profit-Organisationen, die jedoch notwendigerweise mit den betroffenen Personen in eine Beziehung treten; und

2. Als betroffene Person: Ziel der geplanten Aktionen, Eltern, Kind, Bürger und Avatar in unserem digitalen Leben.

Wir stellen personenbezogene Daten in den Mittelpunkt unserer Projekte und internen Treffen und setzen daher die Phase des Brainstormings, der Recherche und der Visualisierung von Ideen im Zusammenspiel mit der Verordnung fort, indem wir die ethischen Konsequenzen jeder Option analysieren.

Wir wählen nur Lösungen, die auf die größte Zahl anwendbar sind und uns als Bürger einer zunehmend vernetzten und digitalen Welt zufrieden stellen. Wir sehen die Verordnung auch als eine Möglichkeit, den Wert personenbezogener Daten zu steigern und das Vertrauen der Betroffenen in die Verarbeitung dieser Daten zu stärken.

Unser ultimativer Test: Wir versetzen uns in die Lage unserer Kinder, die in Betracht gezogene Option zu testen, sie dann zu kommentieren und als Elternteil zu bewerten.

NO TO LEGAL TERMS AND INCOMPREHENSIVE IT.... Es ist einfach verboten, ab dem 25. Mai alle Informationen an die von der Verordnung betroffenen Personen weiterzugeben!

Schritt 3: VISUALISIERUNG UND REDUKTION

In den ersten beiden Phasen haben wir ein erstrebenswertes Ziel vorbereitet: die visuelle Kommunikation nach einer ethischen Prüfung.

Zwei externe Lösungen (menschlich und künstlich) helfen uns, die Kommunikation professionell und optimal abzuschließen:

1. Grafik-Design-Outsourcing

Wir machen Online-Ausschreibungen von grafischen Kreationen zur Professionalisierung der letzten Phase der rechtlichen Gestaltung, visuelle, Web-, Video-Produktionen,.... .:

https://www.designcrowd.com & https://99designs.fr/ & https://www.upwork.com/ & www.freelancer.com & https://www.freelancer.com

Unsere "Skizzen" sind digitale Vorlagen (wenn wir sie auf Papier digitalisieren) und teilen sie daher mit unseren Designern.

Unsere Partner auf der ganzen Welt - die über webbasierte Wettbewerbsplattformen ausgewählt werden - vervollständigen das Ziel der Verordnung, "in knapper, transparenter, verständlicher und leicht zugänglicher Form, insbesondere für alle Informationen, die speziell für ein Kind bestimmt sind" (Artikel 12 GSR: Anwendung des Grundsatzes der TRANSPARENZ). Besonderes Augenmerk legen wir auf die Ikonisierung, da sie von der DGMP gefördert wird.

2. Künstliche Intelligenz

Lesen Sie: https://www.dropbox.com/sh/57ucgvg83eg7esf/AABXFs-yGaHX-E\_JPcvtrIbPa?dl=0

"So wie die Elektrizität vor einem Jahrhundert einen Industriesektor nach dem anderen veränderte, so wird es jetzt auch die künstliche Intelligenz sein." Andrew Ng, ehemaliger Chefwissenschaftler der chinesischen Baidu-Gruppe (2017)

Wir laden die IA in den Prozess der REDAKTION der verschiedenen Dokumente und Texte für die betroffenen Personen und Empfänger ein: https://textio.com/.

Wir verwenden KI-Schreibwerkzeuge, die Rechtssprache in Klartext umwandeln, siehe Harvard Business Review und La libre Belgique Dossiers zu diesem Thema, die sehr gute Beispiele von Unternehmen enthalten, die sie anbieten.

AI wird auch in DPO-Schulungsprozessen, erweiterten DPO-Lösungen (Data Privacy Box Dfakto und DPObots), Marketing und Verkaufsprospektion und interner Kommunikation (Dfakto ist eine analytische Datenlösung zur Verwaltung großer Projekte in großer Zahl) entwickelt und eingesetzt.

3. « Leistungen " optimiert nach den 3 Schritten und 2 externen Lösungen des 3.

Wir paraphrasieren Artikel 32 der Datenschutzverordnung, um sie zu unserem rechtlichen Kommunikationsziel zu machen:

Unter Berücksichtigung des Kenntnisstandes, der Umsetzungskosten und der Art, des Umfangs, des Kontextes, der Zwecke und der Empfänger der Rechtsmitteilung und ihrer optimalen Einhaltung der Verordnung sowie der Risiken, deren Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten der von der Mitteilung betroffenen natürlichen Personen unterschiedlich sind, ergreifen wir die geeigneten technischen und organisatorischen Maßnahmen, um ein dem Risiko angepasstes und der Verordnung am besten entsprechendes Kommunikationsniveau zu gewährleisten, unter anderem auch entsprechend den Bedürfnissen des Kunden.

8. Wie kann man gemeinsam Werte schaffen?

A. EIN FRISCHES AUSSEHEN

Ein neuer Blick auf die Beziehung, die Sie zu Ihren Kunden aufbauen, und die Möglichkeit, im RGPD eine neue Beziehung von Vertrauen, Transparenz und Offenheit aufzubauen, wirkt sich positiv auf das Kundenerlebnis aus und fördert deren Loyalität (und hilft, Verwaltungsstrafen wegen Nichteinhaltung der Verordnung in Höhe von mehreren zehn Millionen Euro zu vermeiden!).

Steve Wood, stellvertretender Kommissar der britischen Aufsichtsbehörde, sagte:

"Da persönliche Informationen die Währung werden, durch die unsere Gesellschaften Geschäfte machen, müssen Organisationen die Rechte der Verbraucher auf Datenschutz zu einer Priorität machen. Datenschutz in den Mittelpunkt der digitalen Geschäftsstrategien zu stellen, ist der Schlüssel zu mehr Vertrauen und digitalem Wachstum.

Er fügte hinzu:

"Änderungen in der Datenschutzgesetzgebung, einschließlich der Einführung des GDPR, bieten Unternehmen die Möglichkeit, sich wieder mit ihren Kunden über Daten auszutauschen. Neue Vorschriften verlangen von den Unternehmen mehr Verantwortung für den Datenschutz, was eine echte Verpflichtung ist, den Verbraucher in den Mittelpunkt des Geschäfts zu stellen.

Diese einzigartige Beziehung, die nur die größten Unternehmen oder die besten.... oder agilen... oder sich entwickelnden Unternehmen aufbauen konnten, resultiert aus einer gemeinsamen Vision, die alle Mitglieder Ihres Unternehmens teilen: "Wir tun alles, um Ihre Daten zu schützen, sie fair und transparent zu behandeln und Sie ständig auf dem Laufenden zu halten.

Eine faire Verarbeitung der von Einzelpersonen erhobenen Daten bedeutet auch, dass die für die Verarbeitung Verantwortlichen bereit sind, über die gesetzlichen Mindestverpflichtungen gegenüber der betroffenen Person hinauszugehen, wenn die berechtigten Interessen der betroffenen Person dies erfordern.

Für das Direktmarketing bedeutet dies, dass die Personen, deren Daten Sie verwenden, wissen, dass sie Marketingangebote von Ihnen erhalten können. Sie sollten sie auch informieren, wenn Sie planen, Ihre Datenbanken mit anderen Organisationen zu teilen und wie Sie diese Personen kontaktieren: per Post, Telefon, E-Mail,....

Die EUROPEAN DIRECT MARKETING FEDERATION definiert DIRECT MARKETING als "die Kommunikation mit allen Mitteln (einschließlich, aber nicht beschränkt auf Post, Fax, Telefon, Online-Dienste usw.) von Werbe- oder Marketingangeboten, die vom Fachmann selbst oder unter seiner Verantwortung gemacht werden und die sich an Einzelpersonen richten".

Die Definition von Direktmarketing umfasst daher alle Kommunikationsmittel und beschränkt sich nicht auf traditionelle Marketingformen wie Telemarketing oder Mailings, sondern erstreckt sich auch auf Online-Marketing, soziale Netzwerke oder andere neu entstehende Kommunikationskanäle.

Überprüfen Sie die für Ihre Direktmarketing-Aktivitäten verwendeten Listen und die Verfahren zur Entfernung von Personen aus diesen Listen (einschließlich derjenigen, die im Namen und/oder im Namen Ihrer Organisation von Partnern und Dienstleistern betrieben werden), um sicherzustellen, dass sie der PDR entsprechen.

Während das PDNMR klar auf Telefonate, E-Mails und Text ausgerichtet ist, kann es auf jede Art von Direktmarketing angewendet werden.

Hier ist die neue Kultur in unseren Unternehmen: "Der Konsument steht im Mittelpunkt unseres Interesses und wir betrachten seine digitale Identität als das wichtigste Kapital seiner Persönlichkeit im digitalen Zeitalter.

https://iconewsblog.files.wordpress.com/2013/12/sw.jpg?resize=64%2C64

"Unabhängig von der Größe Ihrer Organisation geht es bei GDPR im Wesentlichen um Vertrauen. Der Aufbau vertrauenswürdiger Beziehungen mit der Öffentlichkeit ermöglicht es Ihnen, Ihre Daten nachhaltig zu nutzen und mehr Wert zu gewinnen. Durch die Veränderung ihrer Datenverarbeitungskultur können Unternehmen neue Werte aus Kundenbeziehungen ableiten.

Steve Wood ist stellvertretender Kommissar für Politik und verantwortlich für den politischen Standpunkt der ICO zur ordnungsgemäßen Anwendung des Rechts auf Informationsrechte und bewährter Verfahren, durch Leitlinien, interne Schulungen, Beratung und spezifische Projekte.

Als Internetdienste müssen die Merkmale der Datenverarbeitungssysteme es den Betroffenen ermöglichen, wirklich zu verstehen, was mit ihren Daten geschieht.

"Der Eckpfeiler der neuen europäischen Regelung ist (in der Tat) der Begriff des Vertrauens: Vertrauen in den verantwortlichen Umgang mit personenbezogenen Daten und Vertrauen in die effektive Anwendung der Regeln. Es ist Aufgabe der NCDP, gemeinsam mit den anderen europäischen Aufsichtsbehörden dieses Vertrauen zu schaffen.

Deshalb könnte sich die GDPR auch auf eine Große Dame beziehen, die schützt und beruhigt.... in unseren intimsten und wichtigsten Aktivitäten: Internet, Wolkenzählung, große Daten, soziale Netzwerke, Internet der Dinge, Uberfischung, Dating-Sites, private Clubs, unser Leben und unsere sexuelle Orientierung, unsere politischen und gewerkschaftlichen Entscheidungen, unsere Gesundheit,....

Das Internet, das Sie erleben, ist so einzigartig wie Ihr Fingerabdruck.

Die Websites, die sich in unserem normalen Leben und unseren Vokabularen durchgesetzt haben, haben begonnen zu verstehen, was für eine Art von Menschen wir sind. Durch die Entwicklung von Algorithmen, die unser Online-Verhalten verfolgen ("verfolgen"), haben Technologieunternehmen Online-Erfahrungen geschaffen, die zutiefst persönlich und selbstbestimmt sind.

B. TREFFEN IM WIRKLICHEN LEBEN

Wir verzichten auf jedes "Standard"-Preisangebot und damit losgelöst von den Realitäten Ihrer Organisation.

Wir haben verschiedene Computer-Tools entwickelt, die es ermöglichen, von unserem ersten Treffen an zu arbeiten:

1) Eine vollständige Diagnose Ihrer Organisation in Bezug auf GDPR-Compliance und Reifegrad Cybersecurity; und

2) einen genauen Bericht über die zu erfüllenden Aufgaben; und

3) einen Entwurf eines Verlobungsschreibens; und

4) Ein Kostenvoranschlag aufgeteilt nach Ihrer Anfrage nach :

a. Beratung/Unterstützung bei der GDPR-Konformität und/oder Unterstützung eines internen DSB

b. Auftrag des DSB

c. Größe Ihrer Organisation

d. Isolierte Risiken

e. Präferenz für eine "einmalige" Zahlung oder ein Abonnement, das die Interventionskosten "glättet"; und

5) Konkrete Maßnahmen zu entwickeln, um die Verarbeitung der Daten zu verbessern, die dank der Punkte 1 bis 4 zum Zweck der Wertschöpfung für Ihre Organisation (Prospektion, Information, Marketing, Rekrutierung, Loyalität, Fundraising,....) aufgedeckt wurden.

Dieses Treffen und seine 5 in Ihrem Unternehmen erbrachten Leistungen werden zum Preis von 850 Euro zzgl. MwSt. in Rechnung gestellt und im Falle eines Einsatzes von den ersten vereinbarten Honoraren abgezogen.

Sie können auch ein erstes Treffen in unseren Büros (Avenue Brugmann 183 bis 1190 Forest) für ein einfaches, unverbindliches und kostenfreies Gespräch vereinbaren, indem Sie einen Termin online buchen: http://ow.ly/PqGw30a5Zyo & https://www.facebook.com/lawrightallright/ oder telefonisch unter 02 643 11 00 oder TELEFON von KRISTINA.

**\* \***

**\***

1. Selon la méthode originale Conformité4, nos conseils sont basés UNIQUEMENT sur les pratiques admises par les 3 autorités de surveillance francophones (France, Belgique et Luxembourg) + Groupe29.

   Respecter scrupuleusement les recommandations, avis et opinions des autorités judiciaires - dans 3 juridictions pour commencer - en se référant clairement à la jurisprudence administrative du Groupe29 lorsqu'elle est disponible. Nous pensons qu'il n'existe pas de meilleur moyen de garantir la conformité en l'absence de certifications et de codes de conduite officiels de l'UE. [↑](#footnote-ref-1)
2. La procédure « GDPR annoté avec actions DD » applique la présente procédure. [↑](#footnote-ref-2)
3. Voir mon storytelling droits d’auteur via Storybird :  -   <https://storybird.s3.amazonaws.com/commerce/assets/2015/7/PJ4VZ/il-y-a-la-si-lon-pre_standard_100671_PJ4VZ.pdf> et - <http://storybird.com/books/il-y-a-la-si-lon-prenait-le-temps-si-lon-prenait-l/?token=4qua2ygbf9> [↑](#footnote-ref-3)
4. <http://www.larousse.fr/encyclopedie/divers/imp%C3%A9ratif_cat%C3%A9gorique/31430> [↑](#footnote-ref-4)
5. Nous multiplions notre connaissance du marché des entreprises actives dans le Data Analytics et Management cf Dfakto, Ucatchit,… et l’AI cf Easyvest.Bisnode,… [↑](#footnote-ref-5)
6. Considérant 7 du même article 12 du Règlement : « *Les informations à communiquer aux personnes concernées en application des articles 13 et 14 peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles sont lisibles par machine* » et pour un exemple : http://sketchlex.com/06/12/2017/icones/pack-icones-communication-droit/ PACK D’ICÔNES RELATIVES À LA COMMUNICATION DU DROIT. [↑](#footnote-ref-6)
7. <https://www.dropbox.com/sh/57ucgvg83eg7esf/AABXFs-yGaHX-E_JPcvtrIbPa?dl=0> [↑](#footnote-ref-7)
8. <http://dataprivacybox.be/> [↑](#footnote-ref-8)
9. <https://www.dropbox.com/sh/xa8wm436iqui2zj/AAC_9x1jlxRIKI046gC1ONXGa?dl=0> [↑](#footnote-ref-9)
10. TRANSFORMER LA RELATION DIGITALE EN RELATION HUMAINE avec des avatars digitaux – des "chatbots":  <http://www.davi.ai/fr/&#technologie> & <https://www.france.tv/france-2/telematin/405667-nouveau-un-avatar-a-votre-service.html> [↑](#footnote-ref-10)
11. <http://www.clari.com/> [↑](#footnote-ref-11)
12. https://www.dfakto.com/ [↑](#footnote-ref-12)
13. « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins » [↑](#footnote-ref-13)
14. Steve Wood, Deputy Commissioner said:

    “As personal information becomes the currency by which society does business, organisations need to start making people’s data protection rights a priority. P utting data protection at the centre of digital businesses strategies is the key to improving trust and digital growth. ”

    He added:

    “Changes to data protection legislation, which include the introduction of the GDPR, offer organisations an opportunity to re-engage with their customers about data. The new laws require organisations to be more accountable for data protection and this is a real commitment to putting the consumer at the heart of business.” <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/11/ico-survey-shows-most-uk-citizens-don-t-trust-organisations-with-their-data/> [↑](#footnote-ref-14)
15. Présidente de la CNPD, Tine A. Larsen, lors de la Conférence sur le nouveau règlement général sur la protection des données du 11 octobre 2016 - [https://cnpd.public.lu/fr/actualites/national/2016/10/conference-CNPD-SMC-1110/index.html](https://cnpd.public.lu/fr/actualites/national/2016/10/conference-CNPD-SMC-1110/index.html%20) - <https://cnpd.public.lu/pictures/photos/actualites/GDPR/Conf11-10-2016-photo-04.jpeg.> [↑](#footnote-ref-15)
16. <https://www.wired.com/insights/2014/11/the-internet-of-me/> [↑](#footnote-ref-16)