
unknowns

—

AUJOURD’HUI

LE RGPD

—

AUJOURD'HUI

1. WTF IS GDPR?!
2. CONTEXTE
3. PÉRIMÈTRE : QUI ? QUAND ? OÙ ?
4. QUOI ? LES DISPOSITIONS
5. COMMENT ? PLAN D'ACTION

WTF IS GDPR?!

Le RGPD ou Règlement Général sur la Protection des Données est le nouveau texte de référence européen pour la protection des données à caractère personnel.

En anglais : GDPR pour General Data Protection Regulation.

À QUOI SERT LE RGPD ?

1. À harmoniser et simplifier la réglementation en matière de protection des données à caractère personnel au niveau européen
2. À renforcer la responsabilité des acteurs en matière de protection des données à caractère personnel
3. À offrir un niveau de protection plus élevé aux données à caractère personnel des citoyens européens

1 Harmoniser et simplifier la réglementation en matière de données à caractère personnel au niveau européen

Avant le RGPD

Une forte disparité de législation entre États, qui nuisait à :

- L'internationalisation des entreprises, qui devaient s'adapter aux spécificités de chaque marché
- À la connaissance et à la compréhension de leurs droits par les utilisateurs, notamment lorsque l'entreprise qui traitait leurs données à caractère personnel était régie par les législations d'un autre pays

Grâce au RGPD

À la différence des directives, les règlements ne nécessitent pas de transposition dans le droit national : le nouveau règlement s'appliquera donc de manière uniforme à l'ensemble des pays membres de l'UE et aura automatiquement force de loi.

Les libertés laissées aux États étant minimes et limitées à des cas exceptionnels.

2 Renforcer la responsabilité des acteurs en matière de protection des données à caractère personnel

Avant le RGPD

Les sanctions en cas de violation des principes de protection des données à caractère personnel étaient rares et souvent trop faibles pour inciter les entreprises à améliorer leurs pratiques.

Ex : Facebook a été condamné en avril 2017 à une sanction de 150 000 € pour de nombreux manquements à la loi Informatique et Libertés de 1978 *(consulter la décision de la CNIL)*

Grâce au RGPD

Toutes les entreprises qui traitent des données à caractère personnel sont potentiellement tenues comme responsables. Elles sont de plus sujettes à des sanctions beaucoup plus lourdes en cas de non respect du règlement pouvant aller jusqu'à 20M€ ou 4% du CA annuel mondial de l'entreprise concernée.

3 Offrir un niveau de protection plus élevé des données à caractère personnel des citoyens européens

Avant le RGPD

Les citoyens européens disposaient déjà de droits en matière de protection de leurs données à caractère personnel.

Grâce au RGPD

Non seulement les droits des citoyens sont renforcés, mais les entreprises vont désormais avoir des obligations beaucoup plus étendues en matière de protection des données à caractère personnel, ainsi que des motivations plus fortes pour se mettre en conformité.

En outre chaque État sera doté d'une institution « chef de file » faisant office de guichet unique pour toute réclamation de la part des citoyens (la CNIL en France).

CONTEXTE

L’application du règlement se fait dans un contexte déjà chargé de nouvelles législations et donc de transformation des systèmes d’information : cet ensemble d’évolutions peut s’avérer assez lourd à prendre en compte en fonction de la typologie de l’entreprise ou de l’entité publique.

CONTEXTE

Au niveau européen :

- Directive NIS (Network and Information Security)
- Directive PSD2 (Payment Services Directive)
- Règlement eIDAS (Electronic Identification and Signature)
- Règlement e-Privacy

Au niveau national :

- République Numérique
- Sapin 2

—

DIRECTIVE NIS

(NETWORK AND INFORMATION SECURITY)

La directive NIS fixe des exigences de sécurité renforcées pour

- les « Opérateurs de services essentiels » (énergie, transports, banques et infrastructures de marchés financiers, santé, fournisseurs d'eau potable et infrastructures numériques)
- les « Fournisseurs de services numériques » (offrant des services numériques sur lesquels de nombreuses entreprises s'appuient : gros sites de service, moteurs de recherche, services Cloud, etc)

Ils doivent mettre en œuvre des mesures techniques et organisationnelles renforcées pour prévenir les incidents et gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités (avec notification obligatoire aux autorités compétentes en cas de risque / défaillance).

Adoptée en juillet 2016, la transposition dans le droit national doit se faire au plus tard le 9 mai 2018.

—

DIRECTIVE PSD2 (PAYMENT SERVICES DIRECTIVE)

La nouvelle directive PSD2 (ou DSP2) est principalement une révision de la PSD1 afin de prendre en compte les évolutions technologiques et les nouveaux usages apparus sur le marché des paiements depuis la 1ère directive et notamment d'encadrer les nouveaux acteurs (agrégateurs d'information et plateformes de paiement en ligne).

Ayant pour objectif final d'avoir un marché centré sur l'utilisateur, ouvert et sécurisé, la directive impose :

- De nouvelles normes de sécurité ;
- Le développement d'APIs (principalement par les banques traditionnelles) pour que les données d'un client soient accessibles (notamment aux nouveaux acteurs).

Adoptée en octobre 2015, la transposition nationale doit être effective pour 2018 (mais les banques réclament un report).

—

RÈGLEMENT eIDAS

(ELECTRONIC IDENTIFICATION AND SIGNATURE)

Règlement relatif à l'identification électronique et aux services de confiance pour les transactions électroniques :

Premier volet spécifique à la signature électronique : le règlement cadre tout le dispositif (identification électronique, services de confiances, etc) permettant que tout document puisse être signé électroniquement et donc avoir valeur juridique.

Volet spécifique au secteur public concernant les systèmes d'identification électronique reconnus par les administrations avec comme objectif de permettre aux citoyens d'utiliser les mêmes services électroniques (identification numérique, signature…) dans l'ensemble des pays membres de l'UE lors de leurs démarches administratives.

La plupart des dispositions sont déjà applicables depuis le 1er juillet 2016. La reconnaissance mutuelle des moyens d'identification électronique sera quand à elle obligatoire à partir de septembre 2018.

RÈGLEMENT E-PRIVACY

Considéré comme le prolongement du RGPD, le règlement « e-Privacy » concerne le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogera la directive de 2002 sur le même thème.

Le règlement devrait également intégrer des modifications concernant le tracking et la gestion des cookies.

Et enfin une entrée en vigueur souhaitée à la même date que le RGPD, c'est-à-dire le 25 mai 2018.

RÉPUBLIQUE NUMÉRIQUE

La loi pour une République Numérique porte, entres autres, sur :

- open data,
- portabilité des données,
- loyauté des plateformes,
- mort numérique,
- secret des correspondances privées,
- coffre-fort numérique,
- recommandé numérique,
- accessibilité numérique…

Entrée en vigueur progressive depuis octobre 2016

SAPIN 2

La loi Sapin 2 comporte des évolutions qui concernent principalement le secteur banques & assurances avec l'ajout de contrôles sur l'assurance-vie et des évolutions du LDD et des Perp…

En vigueur depuis le 11 décembre 2016.

PÉRIMÈTRE D'APPLICATION DU RGPD

Mais QUI est concerné ?

TOUT LE MONDE

Voyons ça de plus près…

PÉRIMÈTRE D'APPLICATION DU RGPD

Les entités qui entrent dans le périmètre d'application du RGPD, sont celles qui répondent au critères suivants :

Critères matériels

LE « QUAND » :
l'entité met en œuvre un ou des traitements de données à caractère personnel

Critères territoriaux

LE « OÙ » : l'entité a un lien géographique avec l'UE

PÉRIMÈTRE D'APPLICATION DU RGPD

Critères matériels

Critères territoriaux

LE « QUAND » :
l'entité met en œuvre un ou des **traitements** de **données à caractère personnel**

PÉRIMÈTRE D'APPLICATION DU RGPD

Critères matériels

1 Qu'est-ce qu'une donnée à caractère personnel ?

Toute information concernant une personne physique, qu'elle soit identifiée ou identifiable, directement ou indirectement

Sont concernées les informations d'identification directe (identité, coordonnées, photo…) **ou indirecte** (identifiant unique, adresse IP, informations relative à la vie professionnelle…).

Cela concerne également toutes les informations que l'on peut rattacher à une personne physique (données de localisation, habitudes de consommation…) que celle-ci soit identifiée ou non.

PÉRIMÈTRE D'APPLICATION DU RGPD

Critères matériels

1 Qu'est-ce qu'une donnée à caractère personnel ?

Une donnée peut perdre son « caractère personnel » si elle a été complètement anonymisée. C'est-à-dire si la personne concernée n'est plus identifiable directement ou indirectement, prenant considération des moyens susceptibles d'être utilisés par le responsable du traitement… ou par toute autre personne.

À noter qu'anonymiser et donc éviter la réidentification de données est plus compliqué qu'il n'y parait : des études* montrent que la combinaison du code postal, de la date de naissance et du sexe permet d'identifier un individu unique dans plus de 60% des cas.

Les données « pseudonymisées » sont en revanche toujours considérées comme des données à caractère personnel. La pseudonymisation est une pratique encouragée par le règlement afin de réduire les risques : certaines obligations du responsable du traitement sont alors allégées.

** Revisiting the Uniqueness of Simple Demographics in the US Population, P. Golle, 2006*

PÉRIMÈTRE D'APPLICATION DU RGPD

Critères matériels

2 De quels « traitements » parle-t-on ?

Tout traitement de données à caractère personnel, qu'il soit automatisé (même en partie) ou non, à condition que les données traitées soient contenues ou appelées à figurer dans un fichier

Quelques exemples de traitements : collecte, enregistrement, organisation, structuration, conservation, adaptation, consultation, utilisation, communication par transmission, diffusion, rapprochement, interconnexion, limitation, effacement, destruction…

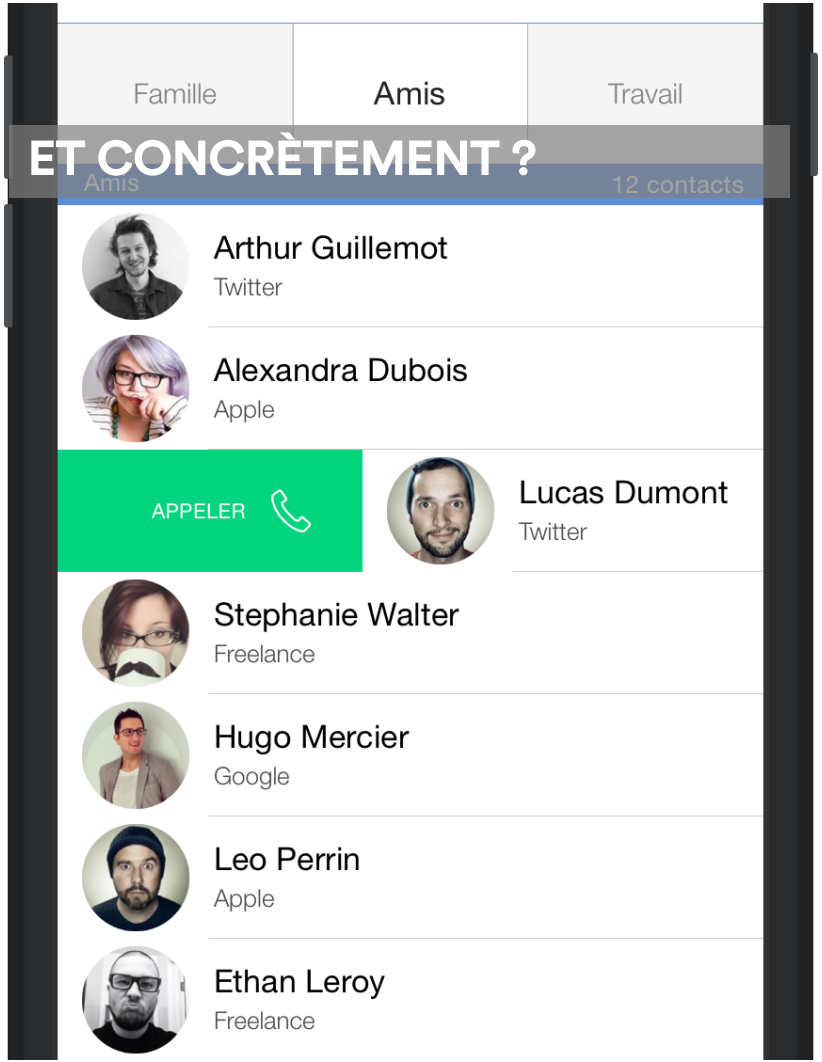
Quelques précisions : un fichier est un ensemble structuré de données accessibles selon des critères déterminés.
Les traitements « manuels » de données, les traitements papiers ou encore les traitements qui peuvent se faire depuis un dispositif autre qu'un ordinateur / smartphone (véhicules, domotique, etc) sont également concernés.

ET CONCRÈTEMENT ?

Les dossiers des employés d'une entreprise, qu'ils soient dématérialisés ou non, sont considérés comme un traitement de données à caractère personnel.

ET CONCRÈTEMENT ?

Récupérer les adresses mails des utilisateurs (peu importe la finalité) est un traitement de données à caractère personnel.



Répertorier des contacts sur un téléphone professionnel est également considéré comme un traitement de données à caractère personnel.

Attention : cela ne s'applique pas aux listes de contacts des téléphones personnels de personnes physique.

PÉRIMÈTRE D'APPLICATION DU RGPD

Critères territoriaux

Critères matériels

Critères territoriaux

LE « OÙ » :
l'entité a un lien géographique avec l'UE

PÉRIMÈTRE D'APPLICATION DU RGPD

Critères territoriaux

1 **Quelles sont les « entités » concernées ?**

Toutes celles qui sont considérées comme « responsables du traitement », ainsi que celles qui agissent comme sous-traitant à un « responsable du traitement »

Qui sont les responsables de traitement ? Toute personne physique ou morale, autorité publique, service ou autre organisme qui seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

PÉRIMÈTRE D'APPLICATION DU RGPD

Critères territoriaux

2 Qu'entend-on par « lien géographique avec l'UE » ?

Concerne tous les responsables de traitement ou sous-traitants qui sont établis au sein de l'UE, que le traitement ait lieu ou non au sein de l'UE.

OU

Tous les responsables de traitement ou sous-traitants qui mettent en œuvre des traitements visant à fournir des biens & services à des personnes au sein de l'UE, ou à suivre leurs comportements au sein de l'UE.

ET CONCRÈTEMENT ?

Un citoyen américain commande un produit à un e-commerçant français. Il fournit ses données personnelles pour se faire livrer aux USA.

/ Le RGPD est applicable au e-commerçant français, car il est établit au sein de l'UE.

Source : August Debouzy (lien)

ET CONCRÈTEMENT ?

Un citoyen européen télécharge une application mobile américaine pour suivre son régime. Pour l'utiliser il doit s'inscrire en renseignant des données personnelles (nom, âge, centres d'intérêts…).

/ Le RGPD est applicable à l'entreprise éditrice de l'application mobile, même si elle n'est pas établie au sein de l'UE, car elle met en œuvre des traitements visant à suivre le comportement d'une personne située au sein de l'UE.

Source : August Debouzy (lien)

ET CONCRÈTEMENT ?

Un citoyen américain en voyage en France commande ses courses pour préparer son retour à partir d'un site américain. Il fournit ses données personnelles pour la livraison à son domicile aux USA.

/ Le RGPD n'est pas applicable : le responsable du traitement n'est pas établit au sein de l'UE, et ne fournit pas des biens à des personnes situées au sein de l'UE.

Source : August Debouzy (lien)

ET CONCRÈTEMENT ?

Un citoyen européen en voyage aux USA souhaite réserver une chambre d'hôtel à partir d'un site de réservation américain. Il fournit ses données personnelles.

/ Le RGPD n'est pas applicable : le service n'est pas fourni au sein de l'UE, et le responsable du traitement n'est pas établit au sein de l'UE.

Source : August Debouzy (lien)

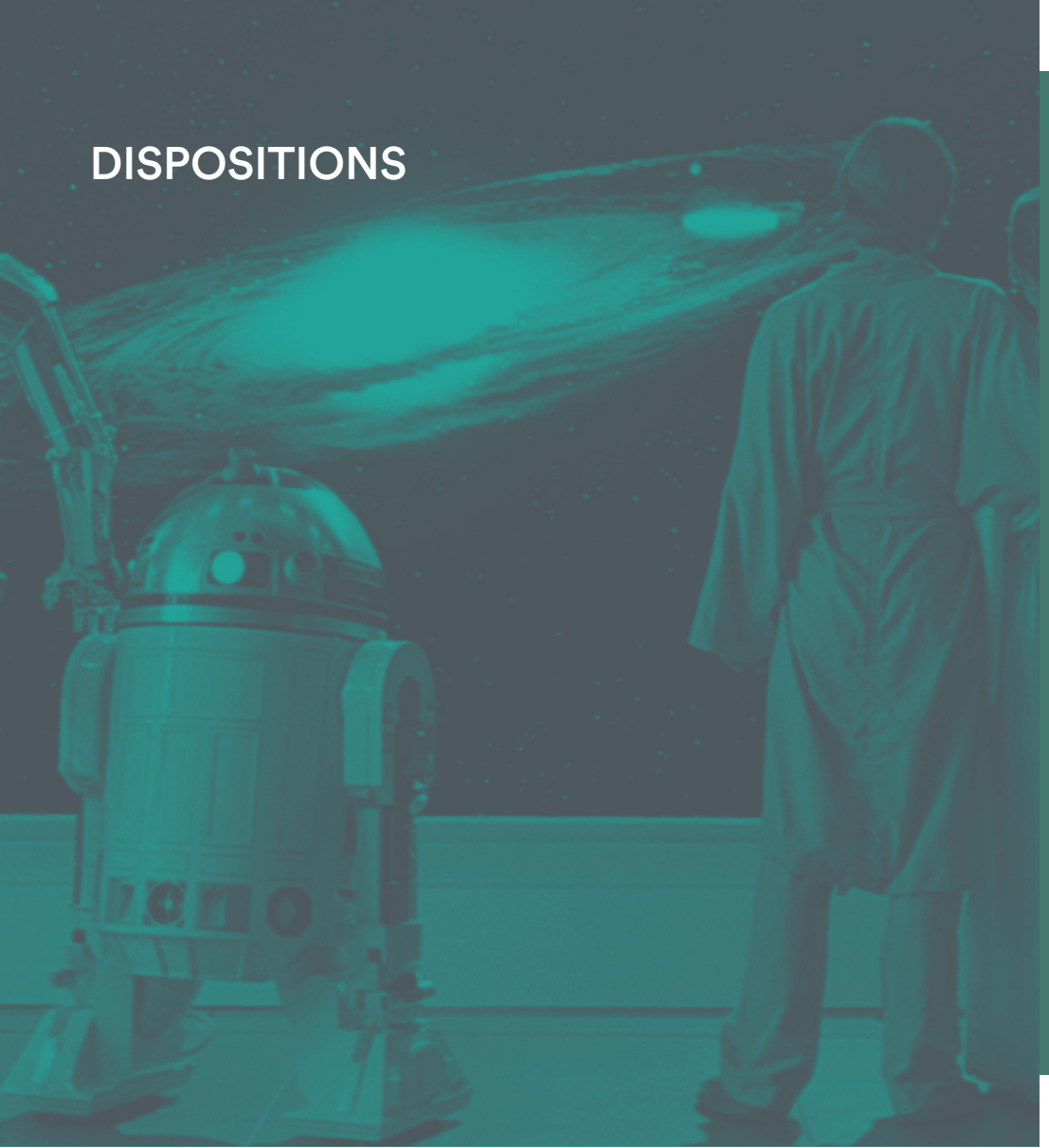
PÉRIMÈTRE D'APPLICATION DU RGPD

Conclusion

Le RGPD s'appliquera à la majorité des entreprises qui sont établies au sein de l'Union Européenne, ainsi qu'à une grande partie des entreprises qui récoltent les données de personnes au sein de l'UE.

Le RGPD s'appliquera également à tout type d'entreprise et pas uniquement aux entreprises du numérique.

DISPOSITIONS



On trouve au sein du RGPD :

1/ un encadrement de l'activité de traitement de données personnelles

2/ des droits étendus pour les utilisateurs au sein de l'UE

3/ des devoirs et obligations étendus pour les responsables de traitement et les sous-traitants

CE QUE LE RGPD DIT, SUIVRE TU DEVRAS

1/ UN ENCADREMENT DE L'ACTIVITÉ DE TRAITEMENT DE DONNÉES PERSONNELLES

2/ des droits étendus pour les utilisateurs au sein de l'UE

3/ des devoirs et obligations étendus pour les responsables de traitement et les sous-traitants

ENCADRER LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Plusieurs principes permettent d'encadrer le traitement de données à caractère personnel :

1. **Le principe de transparence** : les données doivent être traitées de manière loyale, licite et transparente.

Ça veut dire quoi ? Le traitement des données ne doit avoir lieu qu'après communication aux personnes concernées d'une information complète, accessible, facile à comprendre, sur le traitement que celui-ci soit réalisé avec ou sans consentement.
Les informations à fournir couvrent notamment les catégories de données à caractère personnel collectées et les finalités du traitement.

—

ENCADRER LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

2

Le principe de limitation des finalités : les données ne doivent être collectées que pour des finalités déterminées, explicites et légitimes.

Ça veut dire quoi ? Les données collectées ne peuvent être réutilisées ultérieurement pour une finalité autre, incompatible avec la finalité ou les finalités de départ. Par exemple : les données récoltées pour envoyer une newsletter ne peuvent être réutilisées pour de la prospection.

—

ENCADRER LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

3

Le principe de minimisation des données : les données traitées doivent être pertinentes, adéquates et limitées aux vues des finalités pour lesquelles elles sont traitées.

Ça veut dire quoi ? Pas de récolte de données personnelles si la finalité du traitement peut être atteinte sans les utiliser. Par exemple : un site qui envoie des devis gratuits peut recueillir l'identité des demandeurs, mais pas leurs coordonnées bancaires, même pour anticiper un achat futur.

4

Le principe de limitation de la conservation des données : les données ne peuvent être conservées au-delà de la durée nécessaire à la finalité du traitement.

Ça veut dire quoi ? L'entreprise doit mettre en place des processus pour gérer le cycle de vie des données : collecte, mise à jour, rectification, gestion de l'obsolescence, suppression.

—

ENCADRER LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

5 **Le principe d'exactitude des données :** les données traitées doivent être exactes et mises à jour.

6 **Le principe de sécurité, d'intégrité et de confidentialité des données :** les données collectées et traitées doivent être sécurisées par des mesures techniques et organisationnelles appropriées.

Ça veut dire quoi ? Il s'agit de prévenir le traitement non autorisé, illicite, la perte, la destruction, les fuites de données à caractère personnel.

—

ENCADRER LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

7 **Le traitement des données doit-être licite.** Pour être licite, il doit répondre à un des critères suivants :

7.1 La personne concernée a consenti au traitement

7.2 Le traitement est nécessaire à l'exécution d'un contrat

7.3 Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou à l'exécution d'une mission d'intérêt public

7.4 Le traitement est nécessaire à la sauvegarde des intérêts vitaux d'une personne

7.5 Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers

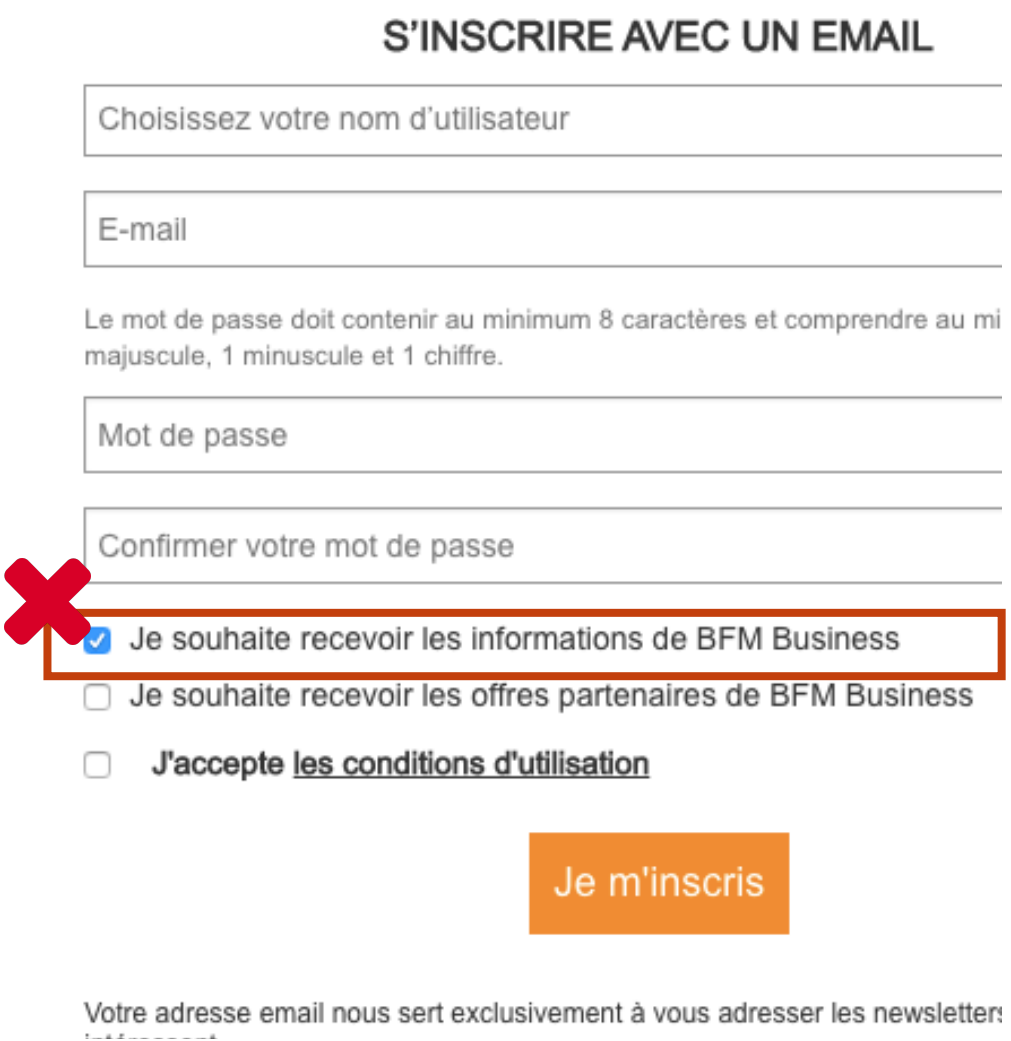
ZOOM SUR LE CONSENTEMENT

7 **Le traitement des données doit-être licite.** Pour être licite, il doit répondre à un des critères suivants :

7.1 La personne concernée a consenti au traitement

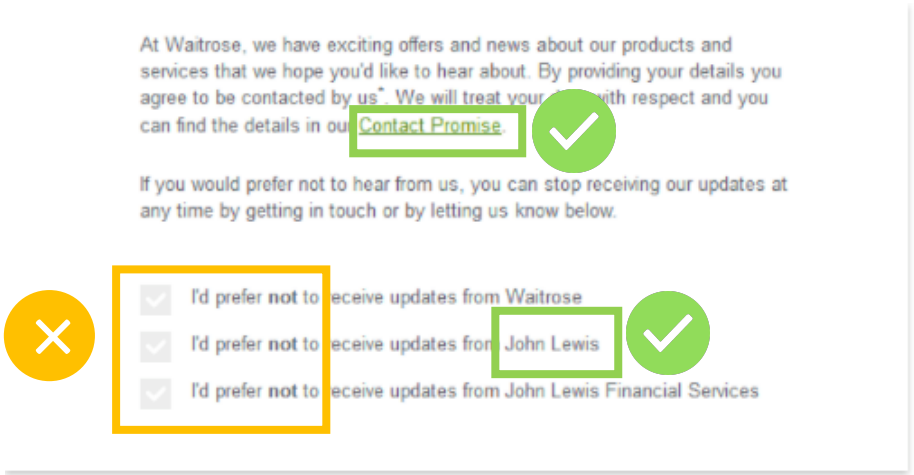
Le consentement est défini comme suit : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Et en pratique ? La question du consentement pose énormément de questions, notamment en termes d'UX. Quelques bonnes pratiques sont décrites dans les slides suivantes



Le principe de consentement instaure la notion « d'un **acte de volonté clair et positif** », en conséquences les méthodes d'opt-in passif (cases précochées) ne sont pas conformes au RGPD.

Sources : Avistem - Le RGPD en focus, e-consultancy.com

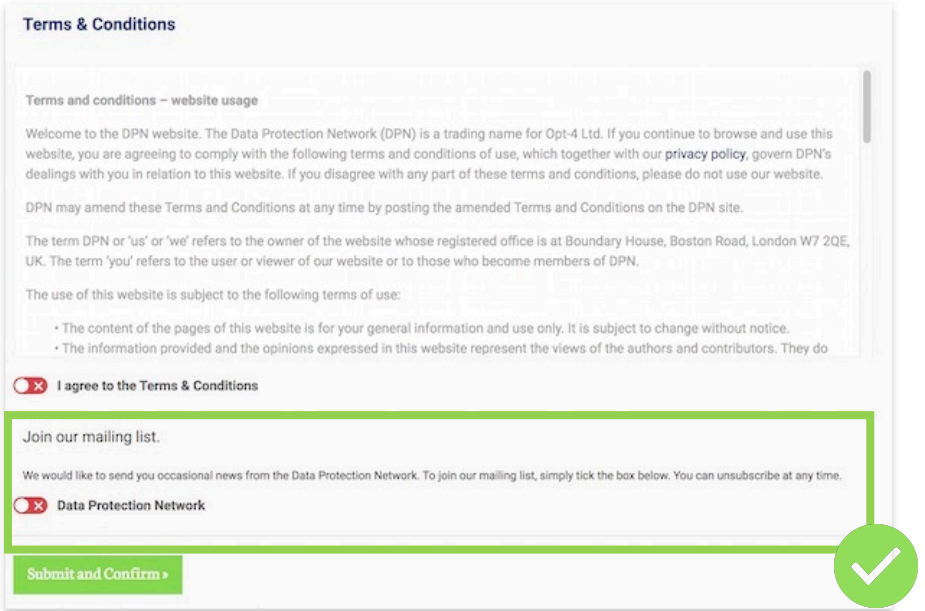


Pour que le consentement soit « **éclairé** » : une information claire, compréhensible, complète sur le traitement doit être transmise à la personne concernée.

Doivent y figurer, entre autres :

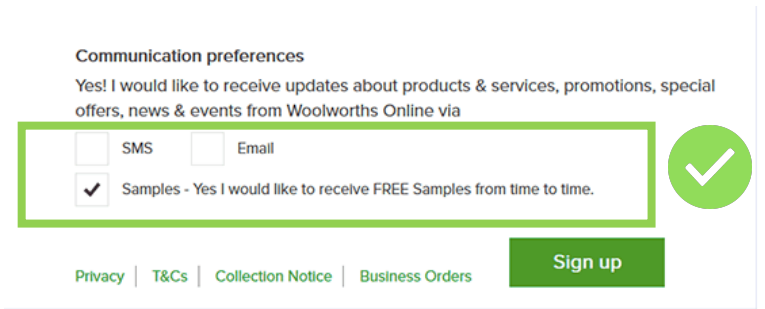
- L'identité et les coordonnées du responsable du traitement
- Les finalités et fondements juridiques du traitement
- Listes des droits des utilisateurs
- Le destinataire des données
- Durée de conservation des données

Sources : Avistem - Le RGPD en focus, e-consultancy.com



Pour que le consentement soit licite, la manifestation de la volonté de la personne doit être « **spécifique** » c'est-à-dire :
quand le consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres informations, **la demande de consentement doit être présentée sous une forme qui la distingue clairement de ces autres questions.**

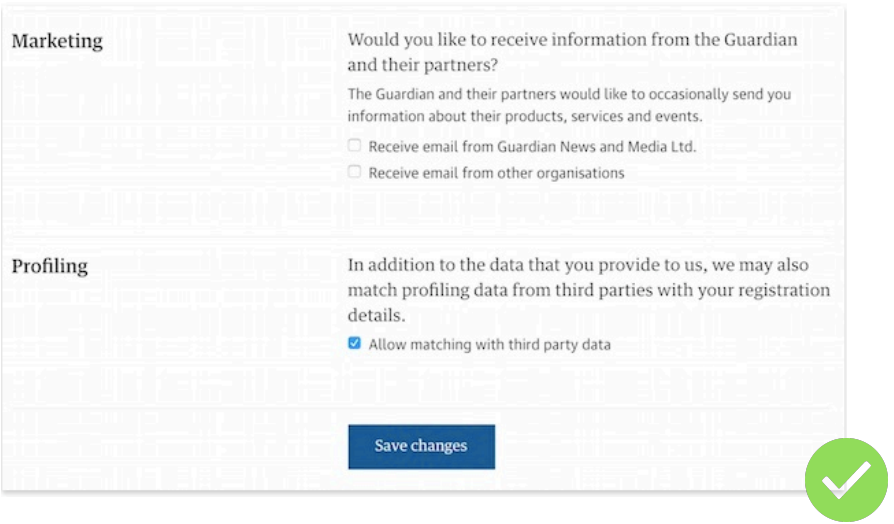
Sources : Avistem - Le RGPD en focus, e-consultancy.com



Le consentement ne peux pas être considéré comme **« libre »** lorsque la personne n'a pas pu donner un consentement distinct pour les différentes opérations de traitement de données présentées.

Bonne pratique : il s'agit de trouver le bon niveau de granularité.

Sources : Avistem - Le RGPD en focus, e-consultancy.com



Le consentement est considéré comme « libre », lorsque la personne a le droit de retirer son consentement à tout moment. Le retrait du consentement doit être aussi simple que son octroi.

Sources : Avistem - Le RGPD en focus, e-consultancy.com

—

ZOOM SUR LE CONTRAT

7 **Le traitement des données doit-être licite.** Pour être licite, il doit répondre à un des critères suivants :

7.2 Le traitement est nécessaire à l'exécution d'un contrat

Et en pratique ? En souscrivant à une offre, payante ou non, en ligne ou non, la personne physique signe un contrat ou valide des conditions générales d'utilisation qui autorise le traitement de données (par exemple, le traitement de l'identité et de l'adresse pour expédier des produits achetés en ligne).
Pour autant, le principe de transparence doit être respecté en détaillant l'objet du traitement dans le contrat et en limitant le traitement aux seules données nécessaires à l'exécution du contrat. Tout autre traitement de données (par exemple, l'abonnement à la newsletter) doit nécessairement faire l'objet d'un consentement spécifique.

—

ZOOM SUR L'OBLIGATION LÉGALE

7 **Le traitement des données doit-être licite.** Pour être licite, il doit répondre à un des critères suivants :

7.3 Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou à l'exécution d'une mission d'intérêt public

Et en pratique ? En tant qu'employeur, une entreprise doit nécessairement traiter les données concernant ses salariés (pour les communiqués à l'administration fiscale par exemple). Comme dans les autres cas, les autres principes doivent être respectés : transparence, droit d'accès / rectification, sécurité… ce qui nécessite donc une mise en conformité des contrats.
En revanche, les traitements de données à caractère personnel des salariés ne relevant pas d'une obligation légale devront faire l'objet d'une demande de consentement.

—

ZOOM SUR LES INTÉRÊTS VITAUX D'UNE PERSONNE

7 **Le traitement des données doit-être licite.** Pour être licite, il doit répondre à un des critères suivants :

7.4 Le traitement est nécessaire à la sauvegarde des intérêts vitaux d'une personne

Par exemple : création d'un dossier médical dans un service d'urgence.

ZOOM SUR L'INTÉRÊT LÉGITIME DU RESPONSABLE DE TRAITEMENT

7 **Le traitement des données doit-être licite.** Pour être licite, il doit répondre à un des critères suivants

7.5 Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers.

Et en pratique ? La notion ouvre une brèche dans le RGPD : les responsables du traitement pourront se passer du consentement des personnes en faisant prévaloir leurs intérêts légitimes, même si dans tous les cas l'utilisateur doit en être informé, de manière transparente.

La notion n'est pas encore claire, et il faudra attendre les conclusions du G29 sur le sujet pour la préciser, mais selon le règlement pourraient être considérées comme légitimes les traitements à des fins de :

- prévention de fraude
- prospection commerciale
- sécurité du réseau

Dans tous les cas, il sera nécessaire d'évaluer et de justifier la pertinence d'un tel traitement.

CE QUE LE RGPD DIT, SUIVRE TU DEVRAS

1/ un encadrement de l'activité de traitement de données personnelles

2/ DES DROITS ÉTENDUS POUR LES UTILISATEURS AU SEIN DE L'UE

3/ des devoirs et obligations étendus pour les responsables de traitement et les sous-traitants

—

DES DROITS ÉTENDUS POUR LES UTILISATEURS

1 **Le droit à l'information :** les personnes doivent être informées du traitement de leurs données à caractère personnel

En pratique : le règlement rend obligatoire un certain nombre d'informations : identité et coordonnées du responsable de traitement, finalités du traitement, liste des droits des personnes, destinataire des données, durée de conservation des données…

2 **Le droit d'accès :** les personnes ont le droit de recevoir gratuitement les données à caractère personnel les concernant, dans un langage structuré, couramment utilisé et lisible par une machine.

3 **Le droit d'obtenir la rectification** des informations inexactes ou incomplètes.

DES DROITS ÉTENDUS POUR LES UTILISATEURS

4 **Le droit d'effacement** (ou droit à l'oubli)

En pratique : la personne concernée peut obtenir l'effacement de ses données dans plusieurs cas de figure : quand elle retire son consentement, quand elle s'oppose à un traitement, quand les données ne sont plus nécessaires aux finalités…

5 **Le droit à la limitation du traitement**

En pratique : le droits à la limitation s'effectue dans des cas limités : quand l'exactitude des données est contestée, quand les données sont sur le point d'être effacées mais que la personne en a besoin pour des raisons juridiques…

—

DES DROITS ÉTENDUS POUR LES UTILISATEURS

6 **Le droit à la portabilité des données :** quand le traitement est fondé sur le consentement ou sur un contrat, ou qu'il est automatisé, la personne a le droit de transmettre ou de demander le transfert de ses données à un autre responsable de traitement. La restitution doit se faire dans un langage couramment utilisé, lisible et structuré.

7 **Le droit d'opposition :** les personnes peuvent demander au responsable de traitement de ne plus traiter leurs données dans certains cas prévus par le règlement.

En pratique : ce droit s'applique notamment quand les données sont traitées à des fins de prospection, ou quand la personne a « des raisons tenant à sa situation particulière ».

—

DES DROITS ÉTENDUS POUR LES UTILISATEURS

8

Le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative.

En pratique : par exemple, lorsque l'accord d'un crédit bancaire se fait uniquement sur la base d'un algorithme, la personne à la droit de se justifier ou de demander une intervention humaine sur son dossier.

CE QUE LE RGPD DIT, SUIVRE TU DEVRAS

1/ un encadrement de l'activité de traitement de données personnelles

2/ des droits étendus pour les utilisateurs au sein de l'UE

3/ DES DEVOIRS ET OBLIGATIONS ÉTENDUS POUR LES RESPONSABLES DE TRAITEMENT ET LES SOUS-TRAITANTS

—

PRINCIPES GÉNÉRAUX

Ces dispositions s'articulent autour de 3 concepts :

- Accountability
- Privacy by design
- Privacy by default

—

DES OBLIGATIONS ÉTENDUES POUR LES RESPONSABLES DE TRAITEMENT ET LES SOUS-TRAITANTS

Non seulement les responsables de traitement doivent respecter les grands principes du règlement en matière de traitement des données personnelles, ainsi que les droits des utilisateurs,

mais le règlement les oblige aussi à s'organiser afin de garantir tous ces principes : c'est le principe d' « accountability »

Selon le principe d'**accountability**, les responsables de traitement doivent être en mesure de prouver, à tout moment, qu'ils ont mis en place les mesures techniques et organisationnelles appropriées pour s'assurer que le traitement des données à caractère personnel sont effectuées conformément au règlement.

—

DES OBLIGATIONS ÉTENDUES POUR LES RESPONSABLES DE TRAITEMENT ET LES SOUS-TRAITANTS

Le règlement oblige même les responsables de traitement à adopter un certain nombre de pratiques, notamment :

1. **Des obligations en matière de documentation :** politique de données à caractère personnel, charte d'utilisation des données, rapports mensuels, audits, registre des activités de traitement, analyses d'impact...

2. **Des obligations organisationnelles :** désignation d'un DPO (data protection officer) dans certains cas, mise en place de formations, de codes de conduite...

—

DES OBLIGATIONS ÉTENDUES POUR LES RESPONSABLES DE TRAITEMENT ET LES SOUS-TRAITANTS

3

Des obligations en terme de développement et d'activité :

- **Privacy by design :** le RGPD oblige les entreprises à prendre les mesures appropriées pour concrètement tenir compte de la protection des données dans les projets depuis leur origine, et de s'assurer de leur conformité tout au long de leur cycle de vie.

  Cela passe bien sûr par le consentement, mais peut aller jusqu'à permettre à l'utilisateur de modifier l'intégralité de ses données, de les récupérer dans un format exploitable, de les supprimer, etc.

—

DES OBLIGATIONS ÉTENDUES POUR LES RESPONSABLES DE TRAITEMENT ET LES SOUS-TRAITANTS

3

Des obligations en terme de développement et d'activité :

- **Privacy by default :** les entreprises traitant les données personnelles doivent garantir, par défaut, le plus haut niveau possible de protection des données.
  Cela couvre aussi les principes de minimisation, de pseudonymisation et de conservation des données dans la durée minimum nécessaire.

CONCLUSION

Le RGPD est une opportunité pour :

- Poser les bases de la protection des données à caractère personnelle des individus
- Inciter les entreprises à développer une culture de la donnée

Mais il suppose de nombreux changements pour les entreprises :
le RGPD va coûter 30 millions d'€ en moyenne aux entreprises du CAC 40

Les entreprises devront être en conformité au RGPD dès le 24 mai 2018,
alors que 60% d'entre elles ne se sentent pas prêtes

Concrètement, comment doivent-elles s'y prendre ?

CONCRÈTEMENT, COMMENT S'Y PRENDRE ?

Une entreprise devant se mettre en conformité avec le règlement peut suivre le plan d'action suivant :

CONCRÈTEMENT, COMMENT S'Y PRENDRE ?

1/ Désigner un pilote

2/ Cartographier les traitements

3/ Identifier et prioriser les actions à mener

4/ Gérer les risques

5/ Poser un cadre de gouvernance et organiser les processus internes

PLAN D'ACTION

1/ DÉSIGNER UN PILOTE

2/ Cartographier les traitements

3/ Identifier et prioriser les actions à mener

4/ Gérer les risques

5/ Poser un cadre de gouvernance
et organiser les processus internes

DÉSIGNER UN PILOTE

Désigner un pilote c'est nommer un **Délégué à la Protection des Données** ou, en anglais, Data Protection Officer (DPO).

Désignation **OBLIGATOIRE** :

- Pour les organismes publics ;
- Pour les entreprises dont l'activité de base amène à **réaliser un suivi régulier et systématique des personnes** à grande échelle, ou à **traiter à grande échelle des données** dites sensibles.

En dehors de ces règles, certains principes généraux (*Privacy by design*, *Privacy by default*, *Accountability*) renforcent rapidement la nécessité de désigner un DPO.

Cette fonction peut être sous-traitée et mutualisée entre plusieurs entreprises.

LES RÔLES DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

- **Informer et conseiller** le responsable de traitement et/ou le sous-traitant
- **Contrôler** le respect du règlement
- **Superviser des audits internes** sur la protection des données personnelles
- **Conseiller** l'organisme sur la réalisation d'études d'impact sur la protection des données et en vérifier l'exécution
- **Inventorier et documenter** les traitements de données
- **Coopérer avec l'autorité de contrôle** (la CNIL) et être le point de contact de celle-ci
- **Être le point de contact** des personnes pour l'exercice de leurs droits

Le Délégué à la Protection des Données peut exercer d'autres missions, pour autant que celles-ci n'entrainent pas de conflit d'intérêts.

Attention, le DPO n'est pas responsable de la conformité au RGPD à la place du responsable de traitement (ou du sous-traitant).

PROFIL DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

La désignation du Délégué à la Protection des Données doit se faire sur la base de ses qualités professionnelles et donc sur ses connaissances spécialisées du droit et des pratiques en matière de protections des données et ses connaissances techniques (compréhension du traitement des données).

Aucun diplôme spécifique n'est exigé, mais le règlement renforce le besoin de formation.
Le poste requiert par ailleurs des qualités organisationelles et en communication, de savoir résister au stress et défendre son indépendance.
Il est également nécessaire de comprendre les autres législations applicables aux activités du responsable du traitement.

ET LE CORRESPONDANT INFORMATIQUES ET LIBERTÉS ?

Du fait de la loi n° 78-17 du 6 janvier 1978, dite Loi informatique et libertés, il était déjà possible pour les entreprise de désigner un Correspondant à la protection des données à caractère personnel, plus connu sous l'appellation de Correspondant Informatique et Libertés (CIL).

Le Délégué à la Protection des Données peut être vu comme une évolution du Correspondant Informatique et Libertés :

- sa désignation devenant obligatoire dans certains cas ;
- il est possible d'externaliser cette ressource ;
- ses missions sont étendues.

En 2016, ils étaient 4729 CIL désignés par 17 725 organismes.

PLAN D'ACTION

1/ Désigner un pilote

2/ CARTOGRAPHIER LES TRAITEMENTS

3/ Identifier et prioriser les actions à mener

4/ Gérer les risques

5/ Poser un cadre de gouvernance
et organiser les processus internes

CARTOGRAPHIER LES TRAITEMENTS

Le règlement impose aux organismes de **tenir une documentation interne complète** sur leurs traitements de données à caractère personnelle. Ainsi doivent être précisés :

- les traitements effectués (collecte, structuration, conservation, modification, consultation, diffusion, etc) ;
- les catégories de données personnelles traitées ; les objectifs poursuivis par les opérations de traitement ;
- les acteurs (internes ou externes).

Pour chaque traitement de données, le responsable du traitement doit être en capacité de répondre aux questions suivantes :

QUI ? **QUOI ?** **POURQUOI ?**

OÙ ? **JUSQU'À QUAND ?** **COMMENT ?**

MAINTENIR UNE DOCUMENTATION COMPLÈTE

Le responsable du traitement devant être capable de prouver, à tout moment et sur simple demande de la CNIL, sa conformité au règlement : il est donc nécessaire de maintenir et d'actualiser régulièrement la documentation relative à la collecte et au traitement des données.

- Registre des traitements
- Analyses d'impact sur la protection des données (PIA)
- Documents relatifs au transfert de données hors-UE
- Mentions d'information sur la collecte et le traitement des données
- Modèles de recueil du consentement
- Preuves du consentement fourni par les personnes concernées
- Procédures mises en place pour l'exercice des droits
- Procédures en cas de violations de données
- Contrats avec les sous-traitants

MAINTENIR UNE DOCUMENTATION COMPLÈTE

En contrepartie, la quasi-totalité des formalités préalables qui existaient avec la CNIL ne sont plus nécessaires.

Il est cependant envisagé de maintenir, au niveau du droit national, certaines formalités pour certaines données sensibles (biométrique, politique, religieuse, etc) ou certains types de traitement (santé publique par exemple).

PLAN D'ACTION

1/ Désigner un pilote

2/ Cartographier les traitements

3/ IDENTIFIER ET PRIORISER LES ACTIONS À MENER

4/ Gérer les risques

5/ Poser un cadre de gouvernance et organiser les processus internes

IDENTIFIER ET PRIORISER LES ACTIONS À MENER

Afin de **se conformer aux obligations** actuelles et à venir, il est nécessaire d'identifier les actions à mener.

Points d'attention :

- Vérifier que seules les données strictement nécessaires à la poursuite des objectifs sont collectées et traitées ;
- Vérifier la base juridique sur laquelle se fonde le traitement (consentement de la personne, intérêt légitime, contrat, obligation légale) ;
- Vérifier que l'utilisateur est correctement informé de la collecte et du traitement des données ;
- Vérifier les modalités d'exercice des droits des personnes (accès, rectification, portabilité, retrait du consentement…) ;
- Vérifier les mesures de sécurité mises en place ;
- Vérifier que les sous-traitants sont en conformité.

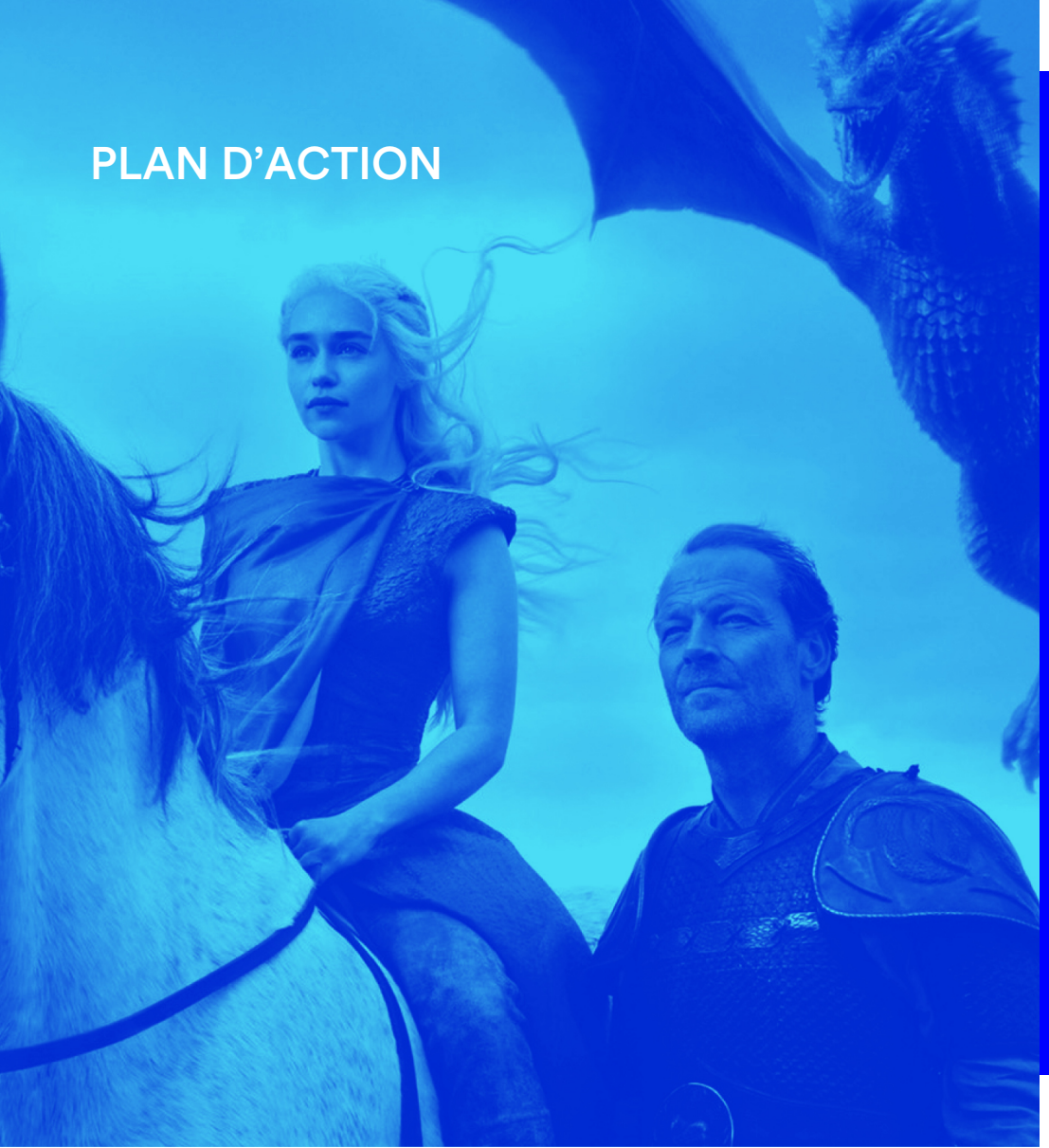
IDENTIFIER ET PRIORISER LES ACTIONS À MENER

Une vigilance particulière doit être portée dans les cas suivants :

- collecte ou traitement de données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale ; des données génétiques, biométriques ou concernant la santé, l'orientation sexuelle ; des données d'infraction ou de condamnation pénale ; des données concernant les mineurs.
- Collecte ou traitement de données ayant pour objet ou effet la surveillance systématique à grande échelle d'une zone accessible au public ; ou à l'évaluation systématique et approfondie d'aspects personnels (profilage).
- Transfert de données hors de l'Union Européenne.

Dans ces cas, il peut être nécessaire de mener des études d'impacts sur la protection des données (PIA), de renforcer l'information, de recueillir des autorisations supplémentaires, etc.

PLAN D'ACTION



1/ Désigner un pilote

2/ Cartographier les traitements

3/ Identifier et prioriser les actions à mener

4/ GÉRER LES RISQUES

5/ Poser un cadre de gouvernance
et organiser les processus internes

GÉRER LES RISQUES

Si, lors des étapes précédentes, des traitements de données personnelles susceptibles d'engendrer des risques sont identifiés, il est nécessaire de mener une étude d'impact sur la protection des données (ou, en anglais, Privacy Impact Assessment).

L'étude d'impact sur la protection des données contient :

- une description du traitement et de ses finalités,
- une évaluation de la nécessité et de la proportionnalité du traitement,
- une appréciation des risques sur les droits et libertés des personnes concernées,
- les mesures envisagées pour traiter ces risques et se conformer au règlement.

Une méthode et des outils sont fournis par la CNIL pour réaliser ces études d'impact : https://www.cnil.fr/fr/PIA-privacy-impact-assessment

GÉRER LES RISQUES

In fine, l'étude d'impact permet :

- d'apprécier les impacts sur la vie privée des personnes concernées,
- de bâtir un traitement de données personnelles ou un produit respectueux de la vie privée,
- de démontrer que les principes fondamentaux du règlement sont respectés.

Les risques sur la protection des données étant toujours appréciés du point de vue des personnes concernées.

PLAN D'ACTION

1/ Désigner un pilote

2/ Cartographier les traitements

3/ Identifier et prioriser les actions à mener

4/ Gérer les risques

5/ POSER UN CADRE DE GOUVERNANCE ET ORGANISER LES PROCESSUS INTERNES

POSER UN CADRE DE GOUVERNANCE ET ORGANISER LES PROCESSUS INTERNES

La mise en conformité au règlement ne se fait pas qu'une seule fois à l'occasion de sa date d'application en mai 2018 (tic-tac, tic-tac…) mais doit être un processus qui s'inscrit dans la durée.

Ce plan d'action doit être pérennisé afin de :

- prendre en compte de la question de la protection des données à caractère personnel pour chaque projet, dès leur conception ;
- maintenir la documentation à jour afin d'être en capacité de prouver sa conformité au règlement ;
- permettre aux personnes d'exercer leurs droits et traiter les réclamations.

D'autres procédures doivent également être définies, notamment en cas de violation des données, changement de prestataire…

SENSIBILISER LES COLLABORATEURS À LA « PRIVACY »

Bien qu'il soit la référence en matière de protection des données personnelles, le DPO n'assure pas seul la mise en conformité : les principes de la nouvelle règlementation doivent donc être diffusés à l'ensemble des collaborateurs.

Les collaborateurs doivent comprendre que tout traitement de données à caractère personnel, même le plus simple comme un fichier Excel de contacts, relève du RGPD et doit donc se faire dans les règles.

- Nouveau processus
- Communication interne
- Formation

Et voilà, vous êtes prêts !

(à vous mettre en conformité)

—

POUR EN SAVOIR PLUS

Nous sommes unknowns. Société de conseil en stratégie & innovation business. Nous identifions, testons et déployons les business de demain grâce à l'ethnographie, le design et la technologie.

Notre mission : faire renouer les grandes entreprises avec leur esprit pionnier et leur permettre d'expérimenter des propositions radicalement innovantes combinant valeur d'usage et valeur business.

/ Venez nous rencontrer

37, avenue Trudaine
75009 Paris, France

/ Contactez-nous

w. www.unknowns.fr
tw. @unknownsfrance
e. moshimoshi@unknowns.fr

/ Sophie Drazic

/ Jérémy Duflot