RGPD

Règlement Général sur la Protection des Données

ENTRÉE
EN VIGUEUR
24 MAI 2016

APPLICABLE
À COMPTER DU
25 MAI 2018

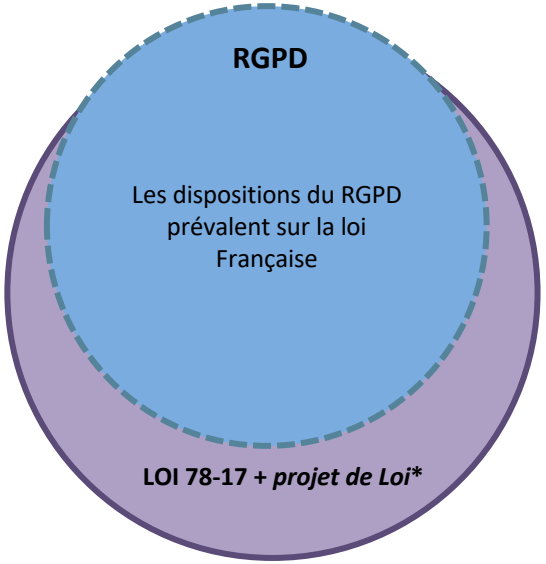
SOMMAIRE

1. CORPUS DE RÈGLES APPLICABLES & AUTORITÉ COMPÉTENTE

OBJECTIFS

Harmoniser & Renforcer la protection des Données Personnelles

Mettre en place un cadre juridique unique pour l'UE



*** Conditions peuvent être plus restrictives**

L'application du RGPD et de la loi nationale

Autorité compétente en France : Commission nationale de l'informatique et liberté dite « CNIL »

- Autorité administrative
- Mission : information; contrôle et conseil

Le RGPD rend inapplicable les dispositions légales et réglementaires nationales incompatibles avec ses dispositions.
Il a une position supérieur dans la hiérarchie des normes mais n'a pas la possibilité d'abroger la loi française.

Le Règlement est d'application directe au sein de chaque état membre (art 94), il comporte de nombreux renvois au droit national desdits Etats membres , qui vont avoir vocation à venir compléter le cadre normatif posé par le RGPD.

Le RGPD a abrogé la directive 1995/ 46/ CE relative à la protection des données à l'égard des traitement à caractère personnel et à la libre circulation de ces données.

Pour éviter les discussions autour de la notion d'incompatibilité : une réforme de la loi Informatique et Liberté est nécessaire pour ne pas rendre inapplicable un certain nombre de dispositions du RGPD


ETES – VOUS
CONCERNÉ PAR LE
RGPD ?

CRITÈRE N°1 :
Déterminer le type de donnée

Le RPGD étend et clarifie le champ d'application territorial de la législation européenne en matière de protection des données personnelles.

=> y'a t-il mise en œuvre d'un ou des **traitements** de **données à caractère personnel ?**

- **Traitement** « toute opération ou tout ensemble **d'opérations effectuées ou non à l'aide de procédés automatisés** et appliqués à des données ou des ensembles de données à caractère personnel ».

- **Donnée personnelle** « toute information qui se rapporte à une **personne physique**, qu'elle soit identifiée, **voire simplement identifiable** (même indirectement, par exemple, par un numéro identifiant ou un recoupement d'informations permettant de nommer une personne)

NB : Vocation à s'appliquer aux traitements de données à caractère personnel, qu'il soient automatisés (même en partie) ou non (à condition que les données traitées soient contenues ou appelées à figurer dans un fichier).

Ne sont pas concernés :

- Traitements à but exclusivement privé ;
- Certains traitements opérés par les Etats membres et/ou autorités compétentes à des fins de préventions ;
- Exécutions de sanctions pénales.

DÉFINITIONS

Qu'est ce qu'une donnée personnelle?

Identité	Coordonnées	Numéro identifiant – Badge
Données de localisation	Adresse IP	Habitudes de consommation
Informations relatives à la vie professionnelle	Adresse mail	

Art. 2-1) 4-2)

DÉFINITIONS

Qu'est-ce qu'un traitement de données à caractère personnel automatisés et non automatisés ?

Collecte	Enregistrement	Organisation	Structuration (Cf. Big Data)
Conservation	Adaptation	Modification	Extraction
Consultation	Utilisation	Communication	Diffusion
Mise à disposition	Rapprochement	Interconnexion	Limitation
Effacement	Destruction	Saisie	Utilisation de DP pour un test

CRITÈRE N°2 :

Identifier qui doit respecter le règlement

Qui a le pouvoir décisionnel sur finalités et moyens du traitements ?

Personne concernée

- Le RGPD prévoit des obligations à la charge des organismes Responsables de traitements et également aux entités qui traitent les données pour le compte d'un tiers (**peu importe la nationalité de la personne concernée**)

Responsable de traitement

- La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Sous-traitant

- La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (y compris à titre gratuit)

CRITÈRE N°3 :
Géographique

Traitement des données effectué dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous traitant sur le territoire de l'UE

Traitement des données appartenant à des personnes concernées ayant leur résidence sur le territoire UE, par un responsable ou un sous-traitant qui n'est pas établi dans l'UE, lorsque les activités de traitement sont liées

- à l'offre de biens ou de services à ces personnes concernées dans l'UE
- ou au suivi du comportement de ces personnes

Traitement des données par un responsable du traitement qui n'est pas établi dans l'UE mais dans un lieu où la législation nationale d'un Etat membre s'applique en vertu du droit international public

LES PRINCIPES CLÉS
EN MATIÈRES DE DONNÉES PERSONNELLES (I)

PRINCIPES SUR LES DONNÉES	DÉFINITIONS	EN PRATIQUE	EXEMPLES
Transparence	Traitement des données : loyale, licite et transparent	Il faut respecter les droits des personnes concernées, cela signifie qu'il ne doit pas y avoir de collecte, utilisation, consultation ou traitement des données sans communication complète sur le traitement aux personnes concernées	Formulaire de collecte en des termes clair : le contenu de l'information à délivrer est précisé dans le règlement.
Limitation des finalités	Collecte pour des finalités déterminées , explicites et légitimes	Collecte pour une finalité précise et ne doit pas être réutilisée ultérieurement pour une autre finalité autre que celle initialement prévue	Les données collectées par un établissement de santé pour suivre l'état des patients ne peuvent être utilisées pour des opérations de prospections sans précautions préalables: risque de détournement de(s) finalité(s).
Sécurité et confidentialité	Traitement des données de façon à garantir une sécurité appropriée	Garantir une sécurité au moyen de mesures organisationnelles et techniques appropriées, éviter que les données soient déformées ou endommagées ou qu'un tiers non autorisé y accède.	Organisation : formalisation d'une politique de sécurité des données, d'actions de sensibilisation des membres du personnel… Techniques : Protocole HTTPS Pour les numéros de CB : stoker sous forme hachée avec utilisation clé secrète

LES PRINCIPES CLÉS
EN MATIÈRES DE DONNÉES PERSONNELLES (II)

PRINCIPES / SUR LES DONNÉES	DÉFINITIONS	EN PRATIQUE	Exemple
Minimisation	Données pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées	La donnée personnelle ne doit être traitée que si la finalité du traitement ne peut pas être atteinte pas d'autres moyens.	Pub sur un site pour permettre aux internautes de recevoir gratuitement devis, documentations , peut recueillir l'identité et les coordonnées du demandeur pour répondre à sa demande mais pas les données bancaires même si c'est pour anticiper une relation future.
Exactitude	Données exactes et mise à jour régulièrement (rectification, voir effacement)	Mesures raisonnables doivent être prises pour s'assurer que les données inexactes sont rectifiées ou effacées	Mettre en place un processus permettant d'effectuer une revue régulière des données afin de déterminer si elles sont encore pertinentes ou au contraire devenues obsolètes
Limitation conservation	Conservation pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées	Limitation au strict minimum (éléments identification des salariés ne doivent pas être conservés au-delà de 5 ans après le départ du salarié, les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de 3 mois…)	une véritable politique de conservation , d'archivages et de purge des données doit être formalisée.

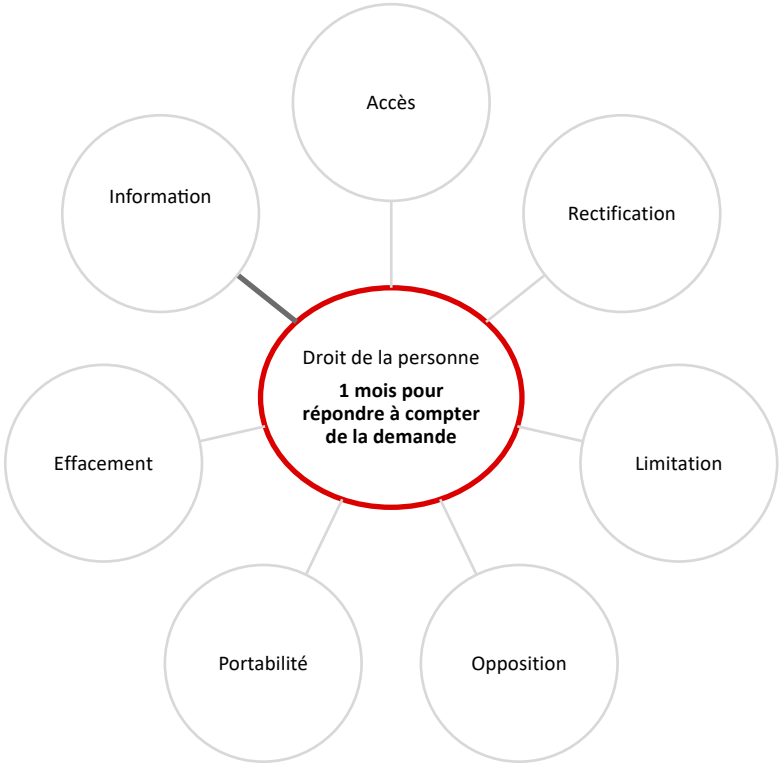
LES PRINCIPES CLÉS
EN MATIÈRES DE TRAITEMENTS (I)

CONDITIONS ALTERNATIVES	DÉFINITIONS	EN PRATIQUE	EXEMPLES
Consentement de la personne concernée	- acte positif et univoque (ne doit pas laisser place à l'incertitude) - libre : liberté de choix : Spécifique: pour finalité précise - Éclairé : après avoir reçu informations afin de décider en connaissance de cause	- Consentement pour traiter les données à des fins d'envoi de newsletters par email; - Consentement des salariés pour l'utilisation de leur photographie dans le cadre d'un réseau social interne.	- ***Consentement valide*** : Case à cocher / Paramétrage technique particulier Dans tous les cas : le consentement doit être obtenu distinctement d'autres consentements ou autres infos (ex: CGV) - *Consentement non* valide : - Les cas de silence - Cases pré-cochées par défaut - Accord implicite ou purement passif
Exécution d'un contrat	Nécessaire dans le cadre d'un contrat ou de l'intention de conclure le contrat	Attention à l'interprétation restrictive : couvert par un contrat ne signifie pas automatiquement nécessaire à son exécution	- Traitement des données des salariés pour que l'employeur puisse les payer - Traitement adresse postale d'un client pour que les produits achetés en ligne puissent être livrés.
Obligation légale **Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique**	Conformément à une obligation légale à laquelle le RT est soumis ou nécessaire à l'exécution d'une mission d'intérêt public	L'obligation devra provenir d'une législation européenne ou de celle d'un Etat membre dont dépend le responsable de Traitement. Si c'est imposé par un Pays tiers : ne relève pas de ce motif	Traitement des données relatives aux rémunérations de leurs salariés par les employeurs pour pouvoir les communiquer à la sécurité sociale ou à l'administration fiscale.

LES PRINCIPES CLÉS
EN MATIÈRES DE TRAITEMENTS (II)

CONDITIONS ALTERNATIVES	DÉFINITIONS	EN PRATIQUE	EXEMPLES
Intérêt vital	Intérêt vital de la personne concernée ou d'une autre personne physique est en jeu	Cette notion semble se limiter à des questions de vie ou de mot ou menaces qui comportent un risque de blessure ou atteinte à la santé	Traitements de données à des fins humanitaires
Intérêt Légitime	Traitement est nécessaire aux fins des intérêts légitimes poursuivis par le RT ou par un tiers, à moins que ne prévalent les intérêts ou libertés de la personne concernée	Mise en balance entre Intérêt du RT (intérêt économique, sécurité, prévention fraude ..) et ceux de la personne concernée ou tiers (vie, privée, atteinte à sa réputation ..) - Preuve doit être apportée par RT , il doit prévenir la personne des motifs légitimes qu'il poursuit lorsque traitement est fondé sur cette base - La personne peut s'y opposer à tout moment	Traitement de données à des fins de prévention contre la fraude

DROITS DES PERSONNES CONCERNÉES




Déployer les mesures nécessaires
à la mise en conformité

LES MESURES À DÉPLOYER

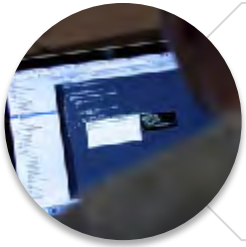
PRINCIPES / SUR LES TRAITEMENTS	DÉFINITION	EN PRATIQUE	EXEMPLE
Accountability (Charge de la preuve RT)	Obligation de mettre en œuvre des mécanismes et procédures internes permettant de démontrer le respect des règles relatives à la protection des données à caractère personnel conformément au règlement, et être en mesure de le démontrer	Organisation au sein de l'entreprise via des mesures concrètes : documentations adaptées, politique de traitement des données écrites et contraignantes , procédure de vérification pour s'assurer de l' effectivité et efficacité des mesures mises en œuvre.	Charte d'utilisation des données à caractère personnel + livret+ guide , rédaction code de conduite, nommer un DPO
Privacy by design (concept nouveau qui participe au respect de l'Accountability)	Nécessité de prendre les mesures appropriées pour concrètement tenir compte de la protection des données dans les projets depuis leur origine et s'assurer de la conformité des produits et services proposés aux dispositions « informatique et libertés » tout au long de leur cycle de vie	Obligation de mettre en œuvre des mécanismes et procédures internes permettant de tenir compte de la protection des données dès la conception – dès le début du projet	1) élaboration d'une méthodologie, procédure intégrée dans les process organisationnels 2) Cahier des charges traduisant les contraintes juridiques à respecter dans tous les nouveaux projets (cf tableau sur les principes) 3) Mécanisme de validation permettant de s'assurer de la conformité I&L 4) Implémentation d'outils appropriés 5) Mise en place d'une organisation adaptée
Privacy by default (concept nouveau qui participe au respect de l'Accountability)	Consiste à prendre des mesures techniques et organisationnelles appropriées pour garantir que par défaut seules les données qui sont nécessaires au regard la finalité spécifique du traitement sont collectées et utilisées.	Les paramètres par défaut doivent faire en sorte que la plus grande protection des données possible soit garantie	ex : application nécessitant géolocalisation – L'utilisateur pourra modifier les paramètres (localisation) à sa guise même s'Il se verra notifier les dangers de ces changements.

Délégué à la Protection des Données

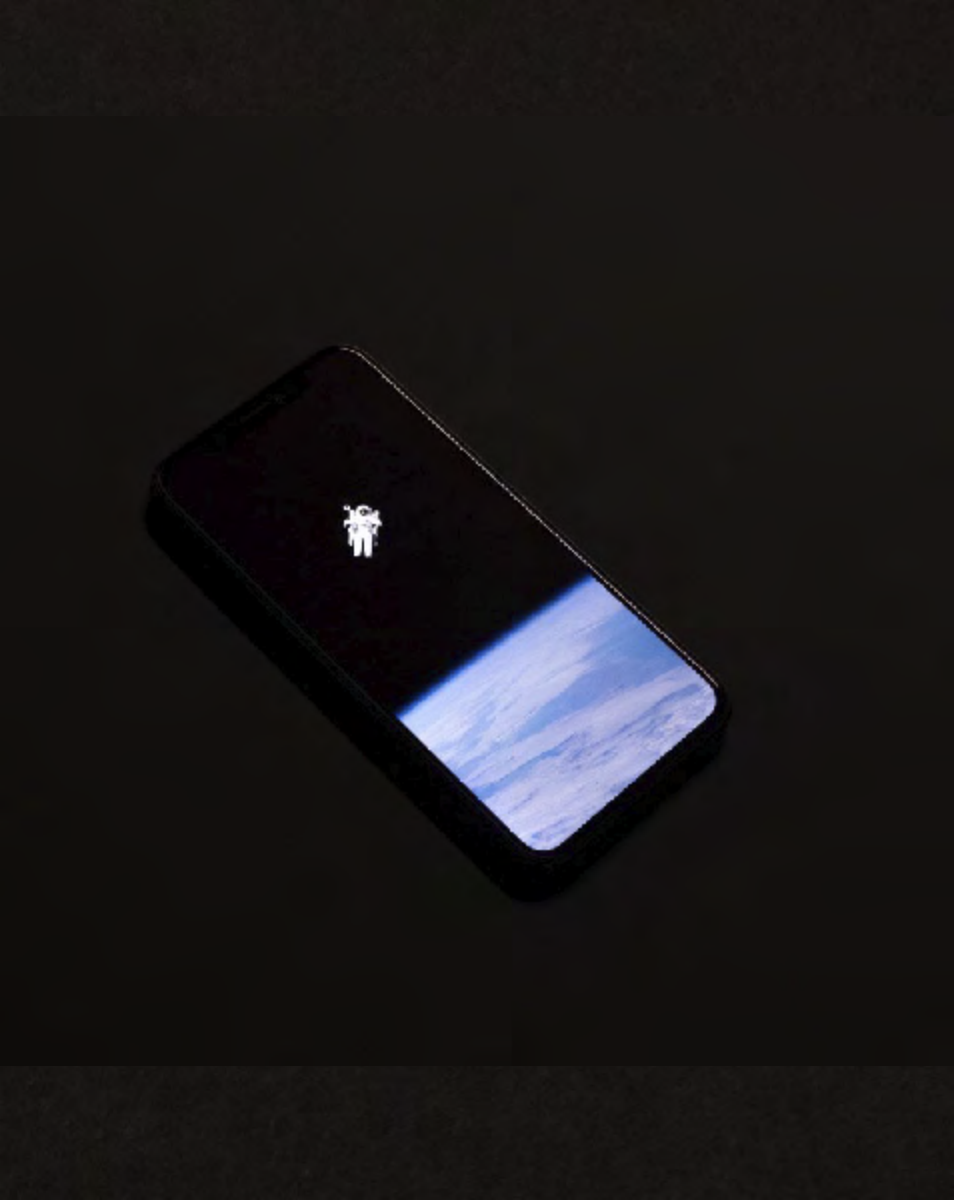
LES CAS D'UNE DÉSIGNATION OBLIGATOIRE

Les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées

Organisme ou autorité publics, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle



Les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données sensibles et de données à caractère personnel relatives à des condamnations pénales et à des infractions.



MISSIONS DU DPO

Informer et conseiller	• sur les obligations du responsable du traitement, du sous-traitant ou des salariés traitant des données à caractère personnel découlant du règlement et des dispositions de l'Union ou de l'Etat membre concerné
Contrôler	• la conformité au règlement et à d'autres dispositions de l'Union ou de l'Etat membre • la conformité aux règles internes en matière de protection des données
Conseiller	• pour la réalisation de l'analyse d'impact
Coopérer	• avec l'autorité de contrôle
Exercer	• la fonction de point de contact pour l'autorité de contrôle

POURQUOI TENIR LES REGISTRES ?

- Pour répondre à la contrainte d'**accountability,** les traitements doivent être répertoriés dans un registre des activités de traitement.
- Mis à jours régulièrement, au fur et à mesure de la mise en œuvre de nouveaux traitements ou modifications des existants.
- Doit être mis à disposition de l'autorité de contrôle en cas de demande

LES PIÈGES À ÉVITER !

- Règlement : la tenue des registres n'est pas obligatoire pour les entités comptant moins de 250 salariés
- Tentation pour TPE/ PME de s'en tenir à cette exception pour échapper à cette obligation
- Attention aux exceptions : il doit y avoir un registre (indépendamment du nombre de salarié) si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il porte sur données dites « particulières » ou relatives à des infractions ou condamnations pénales ou encore s'il n'est pas occasionnel
- Tout traitement mis en œuvre qui présente une certaine pérennité doit faire l'objet d'une insertion dans un registre des activités de traitement, que l'entité compte plus ou moins de 250 salariés..

LES INFORMATIONS DU REGISTRE

RESPONSABLE DU TRAITEMENT	SOUS – TRAITANT
Identité et coordonnées du responsable de traitement et de son représentant et du délégué à la protection	Identité et coordonnées du sous-traitant et de son représentant, de chaque responsable de traitement et de leur représentant et du délégué à la protection des données
Finalités du traitement	Catégorie de traitement
Catégories de personnes concernées	x
Catégories de données traitées	x
Catégorie de destinataires de données	x
Existence de transfert de données hors UE et référence aux garanties associées	
Description générale des mesures de sécurité techniques et organisationnelles mises en œuvre	
Durée de conservation des données	

Fiche registre Responsable de Traitement

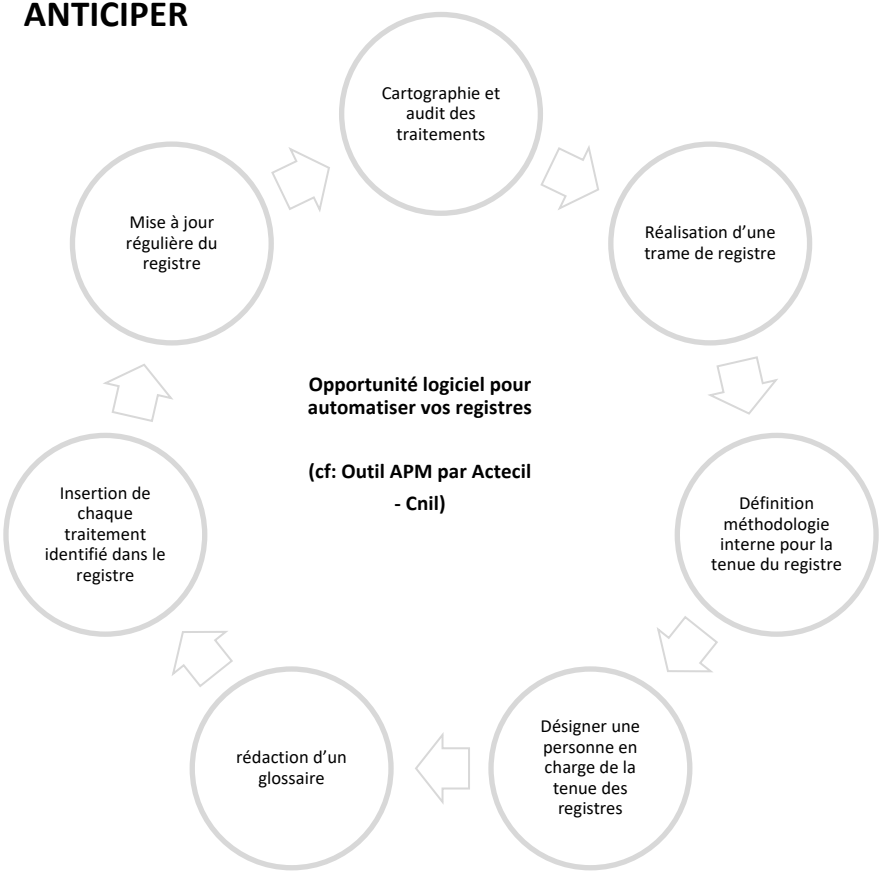
Traitement n°1	**Indiquer le nom du traitement ou la référence interne**
Date de création : **Date de mise à jour :**	Indiquer la date effective de la mise en œuvre. Dans le cas où des démarches préalables auprès de la CNIL ont été nécessaires indiquer la date du récépissé. Indiquer la date de mise à jour lorsqu'il s'agit d'une modification substantielle du traitement initial.
Finalité principale du traitement :	Indiquer ici les objectifs principaux poursuivis par les opérations de traitements de données
Détail des finalités du Traitement **Sous-finalités**	Détailler les composantes essentielles de la finalité générale et les sous-finalités. P*ar exemple, il s'agit d'un logiciel indiquez ses fonctionnalités*
Acteurs **Responsable de traitements** **Délégué à la protection de données** **Représentant UE** **Responsables(s) conjoint(s)**	Indiquer les acteurs impliqués dans la mise en œuvre du traitement ainsi que leurs coordonnées. *Par exemple : nom, adresse, CP, ville, pays, téléphone, adresse mail*
Fonction de la personne ou du service auprès duquel s'exerce le droit d'accès	Qui est chargé du droit d'accès dans le service? Tout personne a droit de demander la communication de données qui la concernent, qui s'occupe de ce type de demande?
Mesure de sécurité	Indiquez les mesures de sécurité techniques et organisationnelles mises en œuvre pour minimiser les risques d'accès non autorisés aux données et d'impact sur la vie privée des personnes concernées. *Par exemple : gestion de habilitations, authentification, journalisation, chiffrement, charte informatique, etc.*
Catégories de personnes concernées par le traitement	A qui appartiennent les données traitées, qui les a communiquées? *Par exemple : clients, collaborateurs, candidats, utilisateurs*
Catégories de données traitées	<u>Catégories de données</u> - Etat civil, identité, données d'identification, images…. - Vie personnelle (habitudes de vie, situation familiale, etc.) - Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.) - Données de connexion (adresse IP, logs, etc.) <u>Durée de conservation</u> Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.

Fiche registre Sous-Traitant

Traitement n°1	Indiquer le nom du traitement ou la référence interne.	
Date de création : **Date de mise à jour :**	Indiquer la date effective de la mise en œuvre du traitement pour le compte du responsable de traitements. Indiquer la date de mise à jour lorsqu'il s'agit d'une modification substantielle du traitement initial.	
Catégories de traitement effectués pour le compte du responsable de traitements	Indiquer ici les catégories de traitements effectués pour le compte de chaque responsable du traitement.	
Détail des finalités du Traitement, **Sous-finalités,** **Fonctionnalités**	Détailler les composantes essentielles de la finalité générale et les sous-finalités. *Par exemple, s'il s'agit d'un logiciel indiquez ses fonctionnalités*	
Acteurs **Sous-traitant** **Responsable de traitements pour le compte duquel est mis en œuvre le traitement** **Délégué à la protection des données** **Représentant UE**	Indiquer les acteurs impliqués dans la mise en œuvre du traitement ainsi que leurs coordonnées. *Par exemple : nom, adresse, CP, ville, pays, téléphone, adresse mail*	
Description générales des mesures de sécurité	Indiquez les mesures de sécurité techniques et organisationnelles mises en œuvre pour minimiser les risques d'accès non autorisés aux données et d'impact sur la vie privée des personnes concernées. *Par exemple : gestion des habilitations, authentification, journalisation, chiffrement, charte informatique, etc.*	
Transferts hors UE	Pays destinataire Identifier les transferts de données hors de l'Union Européenne.	Type de garanties *Par exemple : clauses contractuelles types, niveau adéquat, BCR, etc.*

COMMENT ORGANISER VOS REGISTRES ?

ANTICIPER



Cas du traitement susceptible d’engendrer un risque élevé pour la personne concernée ?

CATÉGORIES PARTICULIÈRES DE DONNÉES

La nouveauté du règlement

En raison de la qualité des données et en particulier lorsqu'il s'agit de catégories particulières de données , des obligations particulières peuvent s'imposer comme par exemple l'étude d'impact ou l'avis de la Cnil. (traitement à grande échelle)

Article 9 : principe interdiction sauf exceptions (art 9 paragraphe 2)
Anciennement : Données sensibles

QUAND FAIRE UNE ANALYSE D'IMPACT ?

Traitements concernés		
Traitements présentant des risques particuliers du fait de leur nature, de leur portée, ou de leurs finalités	Traitements présentant des risques particuliers : - surveillance systématique à grande échelle d'une zone accessible au public, - traitement à grande échelle d'informations sensibles, - évaluation d'aspects personnels fondée sur un traitement automatique et permettant de prendre des décisions à l'égard d'une personne…	Traitements considérés par l'autorité de contrôle comme étant susceptibles de présenter des risques spécifiques pour les droits et libertés des personnes concernées (liste publique)

Exemple de traitement risqué : vidéo protection

L'ANALYSE EN PRATIQUE

Description générale des traitements envisagés et des finalités

Evaluation de la nécessité et de la proportionnalité des opérations de traitement

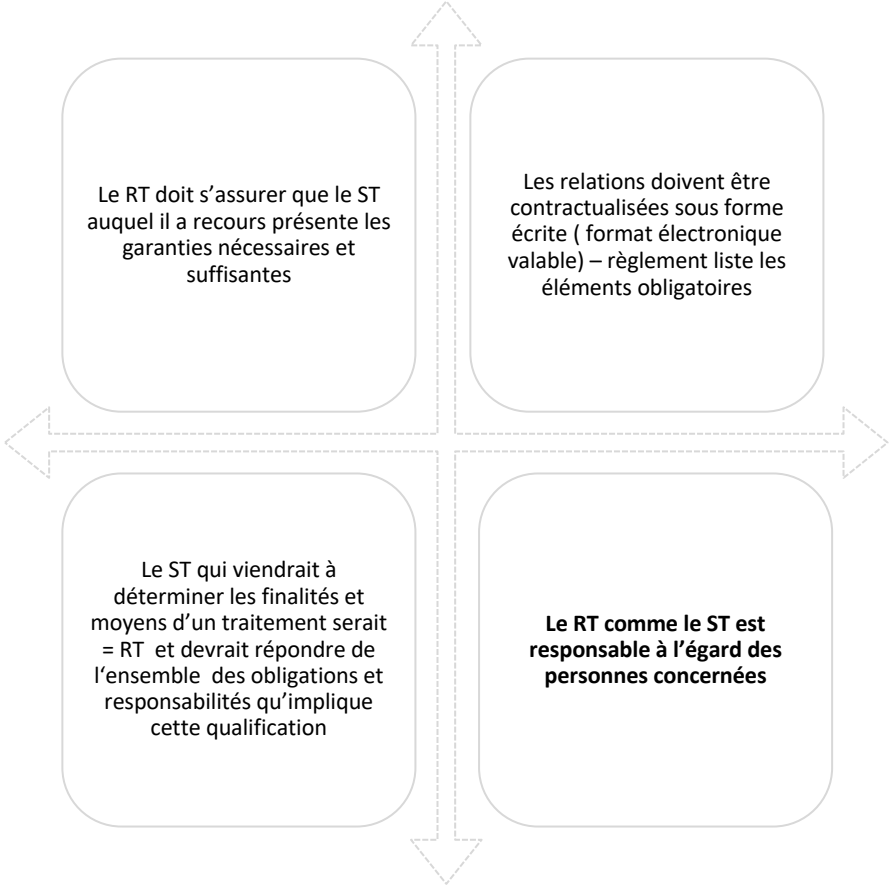
PLUS
consultation préalable de l'autorité de protection des données si le résultat de l'analyse indique que le traitement présente un risque élevé pour la personne concernée

Evaluation des risques pour les droits et libertés des personnes concernées

Mesures envisagées pour faire face aux risques

ORGANISER LES RELATIONS ENTRE LES ACTEURS DU TRAITEMENT

LES RELATIONS : RÉEQUILIBRAGE DES RESPONSABILITÉS PAR LE RGPD



La qualité de RT et ST ne dépend pas de la qualification des parties dans le contrat qui les lie.

Le contrat peut fournir des indices et des informations sur la relation qui existe entre les parties, mais ce qui déterminera réellement le statut de l'entité est l'influence de fait que celle-ci va exercer sur les finalités et les moyens de traitements en questions.

ATTENTION !

Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union relatives à la protection des données

Vérifier la légalité des instructions reçues

Le sous-traitant n'est responsable que :

ou

ou

s'il n'a pas respecté les obligations prévues par le règlement

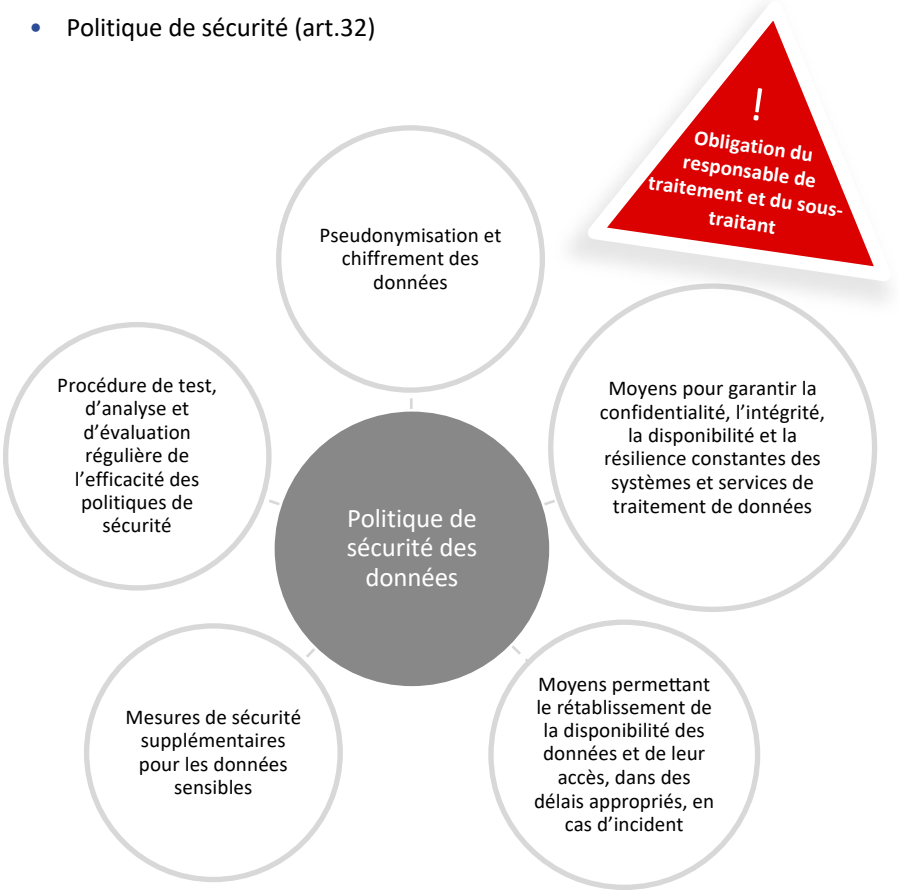
S'il a agi en-dehors des instructions licites du responsable de traitement

S'il a agi contrairement aux instructions du responsable de traitement

L’obligation de sécurité

DÉPLOYER LES MESURES DE SÉCURITÉ ET DE CONFIDENTIALITÉ ADÉQUATES

- Politique de sécurité (art.32)



GESTION DES FAILLES DE SÉCURITÉ EN MATIÈRES DE DONNÉES

Obligation N° 1

Obligation du responsable de traitement

Sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physique »

- dans les 72 Heures à l'autorité de contrôle
- Directement à la personne concernée

Obligation N° 2

Obligation du sous-traitant

« Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel »

- dans les meilleurs délais après en avoir pris connaissance »

COMMENT GERER VOS FAILLES ?

Formaliser procédure de gestion des failles de sécurité décrivant les grandes étapes : identification et correction faille, dépôt de plainte, déclaration sinistre auprès assurance…

Rédiger des modèles –types: notification à l'autorité de contrôle , communication à la personne concernée (cf:site Cnil)

Élaborer un registre documenté des failles de sécurité avec retours d'expérience constructifs

MAITRISER LES TRANSFERTS DE DONNEES HORS UE

Principe: les transferts de données à caractère personnel hors du territoire de l'Union européenne sont interdits à moins que le pays ou le destinataire n'assure un niveau de protection suffisant.

Il est à noter que cette interdiction de transferts ne concerne pas l'Islande, le Liechtenstein et la Norvège, puisque ces pays ont transposé les dispositions de la directive 95/46/CE dans leur législation nationale (ces pays et les 27 Etats membres de l'Union européenne constituent l'Espace économique européen).

Cette interdiction ne concerne pas les transferts vers les pays reconnus comme « adéquats » par la Commission européenne.

A ce jour, *c'est le cas d'Andorre, de l'Argentine, du Canada, des Iles Féroé, de l'Ile de Man, de Guernesey, de Jersey, d'Israël, de l'Uruguay et de la Suisse*.

MAITRISER LES TRANSFERTS DE DONNEES HORS UE

Les transferts hors de ces pays, plusieurs outils ont été développés pour permettre aux acteurs d'apporter un niveau de protection suffisant : les règles internes d'entreprise (ou BCR), les Clauses Contractuelles Types et l'adhésion aux principes du « Privacy Shield » (suivre les recommandations du G29)

- Attention : Contacter la CNIL en cas de transfert de data vers les USA .

La loi prévoit également des exceptions permettant de transférer des données vers des pays tiers sans qu'il n'existe pour autant un niveau de protection suffisant.

L'ensemble de ces mécanismes sont présentés dans le guide de la Cnil afin de répondre aux interrogations du public sur les transferts de données personnelles hors de l'Union européenne.

MAITRISER LES TRANSFERTS DE DONNEES HORS UE

Carte qui* vous *permet de visualiser les différents niveaux de protection des données des pays dans le monde

https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

LES SANCTIONS

- Absence de protection des données dès la conception et protection des données par défaut
- Absence de représentant établi dans l'Union
- Absence de registre des activités de traitement
- Absence de coopération avec l'autorité de contrôle
- Absence de notification à l'autorité de contrôle ou à la personne concernée d'une violation des données
- Absence d'analyse d'impact

10 000 000 €
ou
2 % du CA
annuel mondial

- Non respect des principes de base d'un traitement (licéité, loyauté, légitimité, adéquation et pertinence des données, consentement, données sensibles, etc.)
- Non respect du droit des personnes
- Non respect des règles relatives aux transferts de données à caractère personnel

20 000 000 €
ou
4 % du CA
annuel mondial

ÉLÉMENTS PRIS EN COMPTE

- Nature, gravité et durée de la violation
- Nombre de personnes concernées et niveau de dommage subi
- Violation commise délibérément ou par négligence
- Mesures prises pour atténuer le dommage subi
- Catégorie de données à caractère personnel concernées
- Degré de coopération établi avec l'autorité de contrôle
- Violations commises précédemment
- Degré de responsabilité compte tenu des mesures techniques et organisationnelles mises en œuvre
- Manière dont l'autorité de contrôle a eu connaissance de la violation
- Mesures déjà ordonnées à l'encontre du responsable de traitement ou sous-traitant
- Application de codes de conduite ou de mécanismes de certification
- Autres circonstances aggravantes ou atténuantes

Conseil : amorcer la mise en conformité

RGPD

Focus sur l'hébergement des données

BeSafe
Save & Safe

Hébergement et RGPD

Quels services sont concernés ?

Les principaux services des hébergeurs.

- Messagerie collaborative (MS Office 365, Echange)
- Partage de documents (Dropbox, Wetransfer)
- Hébergement de serveurs privés (machines virtuelles)
- Hébergements d'applications (Saas)
- Sauvegarde externalisée (Baas)
- Sites Internet (E-commerce, réseaux sociaux, etc..)

Le RGPD dans sa version actuelle ne permet pas de répondre clairement

Néanmoins, dans la continuité du RGPD, un nouveau règlement concernent le e-commerce va apparaitre :

Le E-Privacy

E-Privacy

Ce qui va changer pour les exploitants de sites Web

- L'obligation de documenter la conformité avec le RGPD.
- Des consentements et autorisations plus complexes
- Les principes de Privacy by Design et Privacy by Default
- Extension des droits à l'information et au déréférencement (suppression des données)
- Le droit à la transférabilité des données
- Exigences d'information beaucoup plus étendues (par exemple pour la déclaration de protection des données d'un site Internet)

Aujourd'hui	Demain
L'utilisateur doit accepter les cookies pour afficher un site Internet.	Demain, si l'utilisateur refuse un cookie, le contenu du site Internet devra tout de même s'afficher.

➢ Le E-Commerce est la 1ere étape de la réglementation, il faut donc prendre les devants

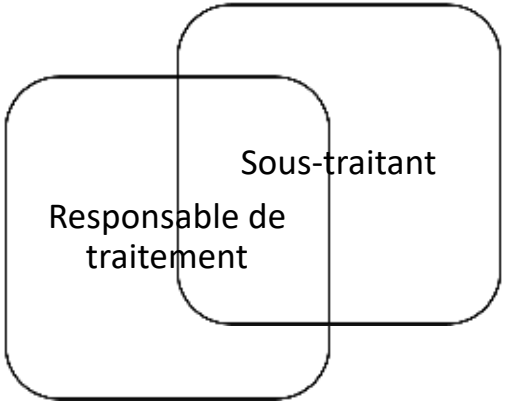
Qui est le sous traitant de qui ?

Dans la réalité, les frontières peuvent se brouiller

Parmi les problématiques actuelles liées à la mise en conformité avec le RGPD figure celle des rapports contractuels avec leurs fournisseurs de solutions et services IT.

- Lorsque les données sont hébergées dans une solution Saas dont les fonctionnalités et caractéristiques techniques sont définies par le fournisseur, celui-ci est-il encore le sous-traitant des données personnelles ?

- Lorsqu'une entreprise héberge physiquement des données personnelles mais n'y a pas logiquement accès, est-elle sous-traitante ?

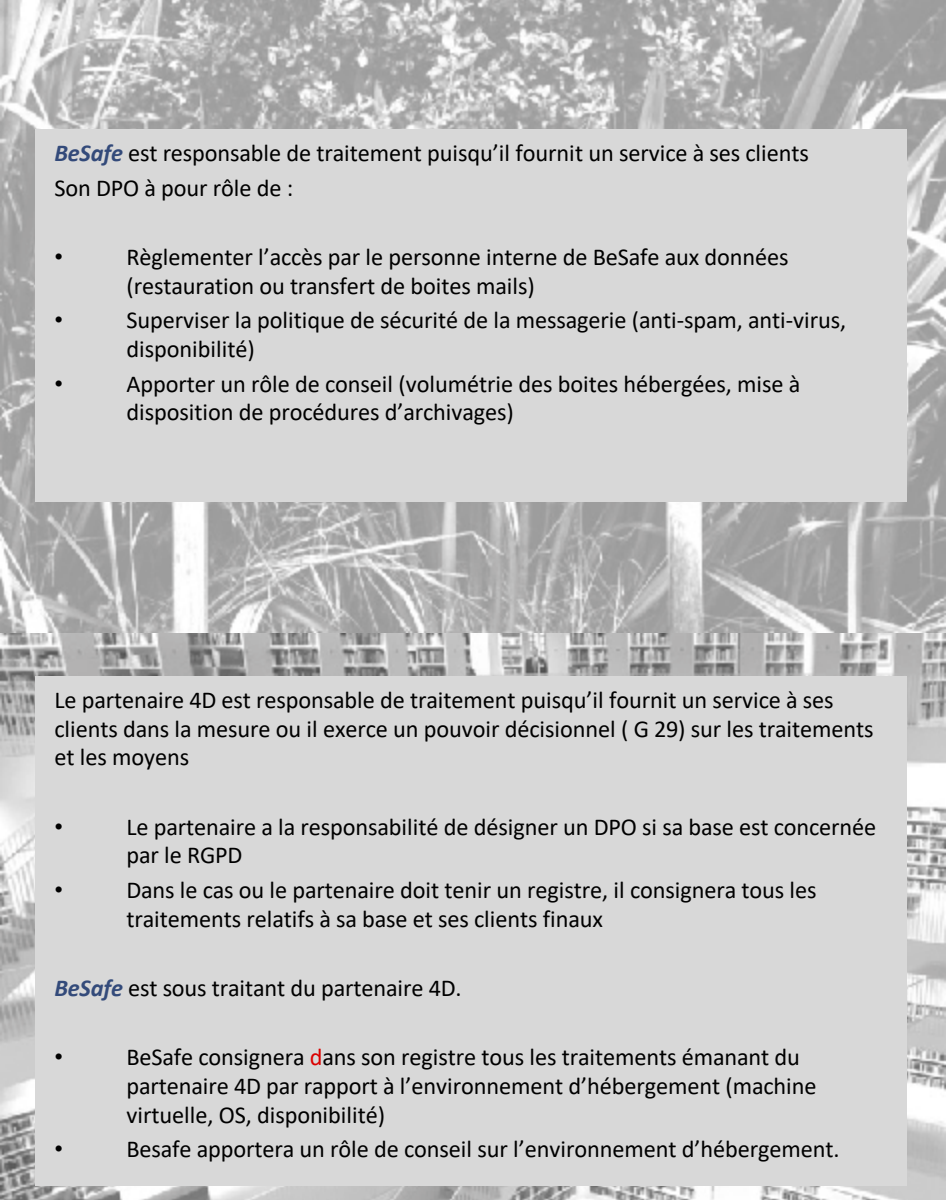


Il n’y pas de réponse avec le RGPD

Mais…

Dans la plupart des cas, l’hébergeur sera considéré comme sous-traitant d’un tiers. En conséquence, il doit :

- Nommer son propre DPO
- Tenir à tenir le registre des traitements internes mais également un registre par client
- Jouer un rôle de conseil vis-à-vis de ses clients hébergés



BeSafe est responsable de traitement puisqu'il fournit un service à ses clients
Son DPO à pour rôle de :

- Règlementer l'accès par le personne interne de BeSafe aux données (restauration ou transfert de boites mails)
- Superviser la politique de sécurité de la messagerie (anti-spam, anti-virus, disponibilité)
- Apporter un rôle de conseil (volumétrie des boites hébergées, mise à disposition de procédures d'archivages)

Le partenaire 4D est responsable de traitement puisqu'il fournit un service à ses clients dans la mesure ou il exerce un pouvoir décisionnel (G 29) sur les traitements et les moyens

- Le partenaire a la responsabilité de désigner un DPO si sa base est concernée par le RGPD
- Dans le cas ou le partenaire doit tenir un registre, il consignera tous les traitements relatifs à sa base et ses clients finaux

BeSafe est sous traitant du partenaire 4D.

- BeSafe consignera dans son registre tous les traitements émanant du partenaire 4D par rapport à l'environnement d'hébergement (machine virtuelle, OS, disponibilité)
- Besafe apportera un rôle de conseil sur l'environnement d'hébergement.

Cas pratiques

Cas N°1 :

Besafe fournit un service de messagerie privée pour l'un de ses clients

- L'hébergement est interne à ***BeSafe*** sans intervention tiers
- Les serveurs de messagerie sont situés en France

Cas N°2 :

Le partenaire 4D confie l'administration de son système informatique à Be Safe qui l'héberge en interne (hors base de données)

- L'hébergement est interne à ***BeSafe*** sans tiers
- Les serveurs hébergés sont situés en France
- Le support BeSafe n'a pas accès au contenu de la base 4D

10 Critères RGPD pour évaluer votre base de données

RGPD et base de données

Le Data Stockage

1 Le volume des données en base

2 Sensibilité des données conservées

3 La présence de données identifiantes

Exemples

Est-ce que je pourrai toujours enregistrer dans une base de données les noms, adresses mail et numéros de mobile de mes interlocuteurs professionnels ?

Oui, et dans les mêmes conditions que celles de la loi actuelle: avec le consentement de la personne concernée.

Pour l'efficacité du recouvrement des créances B to B, je suggère souvent aux chargés de relance de noter des informations du type horaires de travail des interlocuteurs,

On distingue les horaires de travail, qui sont des données personnelles, des horaires de disponibilité, qui sont des données professionnelles. Il vaut donc mieux enregistrer ces dernières

RGPD et base de données

Le Data Collection

4 Le volume des données clients ajouté mensuellement

*6% des acteurs audités sont en conformité avec le RGPD à six mois de son entrée en vigueur**

*84% à 94% des sites ne demandent pas le consentement à la collecte des données personnelles**

* Source : Viuz.com

RGPD et base de données

Le Data Transfert

5 Le transfert de données à des tiers

6 Le transfert de données hors de l'UE

Exemple

Est-ce que le fait que mes bases de données client ou fournisseur soient dans le cloud, ou hébergées hors Union européenne, change quelque chose?

Ne pas savoir où elles se trouvent est déjà un indice de non-conformité. Les données personnelles doivent être protégées de toute intrusion tant au terme de la loi actuelle que du RGPD qui renforce les sanctions.

RGPD et base de données

Le Data Suppression

7 Purges régulières des données non pertinentes

8 Durées de conservation des données personnelles

suppression du compte après X mois d'inactivité, désabonnement après X mois sans ouverture d'email

RGPD et base de données

Le Data Security

Comment adapter votre développement avec le RGPD

RGPD et développement

Droit à l’accès

Si votre application Web est accessible aux utilisateurs, ils doivent pouvoir modifier leur profil.

- **Règle de base - tous les champs de votre table "users" devraient être éditables via l'interface utilisateur**
-
- **Les utilisateurs doivent être en mesure de corriger toutes les données les concernant, y compris les données que vous avez collectées à partir d'autres sources.**

Les cases à cocher consentement

- Pour chaque activité de traitement particulière, il doit y avoir une case à cocher distincte sur le profil de l'utilisateur
- Idéalement, ces cases à cocher devraient provenir directement du registre des activités de traitement
- Notez que les cases à cocher ne doivent pas être présélectionnées, car cela ne compte pas comme "consentement »

RGPD et développement

Droit à l'oubli

- Avoir une méthode «oubliez-moi» qui prend un '*UserId*' et supprime toutes les données personnelles sur cet utilisateur.

- Vos utilisateurs ont des profils sur votre application Web. Vous devez leur donner un moyen de supprimer leurs profils via cette méthode.

Avertir les tiers de l'effacement

- Tous les tiers auxquels les données personnelles ont été transmises. Si transmises à un service cloud (Salesforce, Hubspot, Twitter) appeler une de leurs API qui permet la suppression de données personnelles (manuel pour Google).

Exporter des données

- Avoir une méthode "exporter des données". Lorsque vous cliquez dessus, l'utilisateur doit recevoir toutes les données que vous détenez à leur sujet. Habituellement, ce sont au moins les données que vous supprimez avec la fonctionnalité «oubliez-moi»,

RGPD et développement

Voir toutes mes données

Cette fonction est très similaire à celle pour exporter, sauf que les données doivent être affichées dans le profil de l'utilisateur.

- Vous devez également indiquer à l'utilisateur de quelle manière vous traitez ses données
- Vous pouvez simplement imprimer tous les enregistrements de votre registre de processus de données pour lesquels l'utilisateur a consenti.

Garder les données pour plus de temps que nécessaire

- Si vous avez collecté les données dans un but spécifique, vous devez le supprimer / anonymiser dès que vous n'en avez pas besoin.
- Prévoir une méthode planifiée pour parcourir périodiquement les données et les anonymiser (supprimer les noms et les adresses).

BONUS : COMMENT SE PRÉPARER ?

PLAN D'ACTIONS:

1. **Mobiliser les ressources en interne (nommer un DPO si nécessaire) ;**

2. **Répertorier vos traitements (en qualité de RT, en qualité de ST) ;**

3. **Auditer / améliorer vos outils logiciels :**

   - **Au plan fonctionnel ;**
   - **Au plan des mesures techniques et organisationnelles ;**
   - **Au plan de la R&D ;**

4. **Préparer / revoir la documentation ;**

5. **Préparer / revoir le discours client ;**

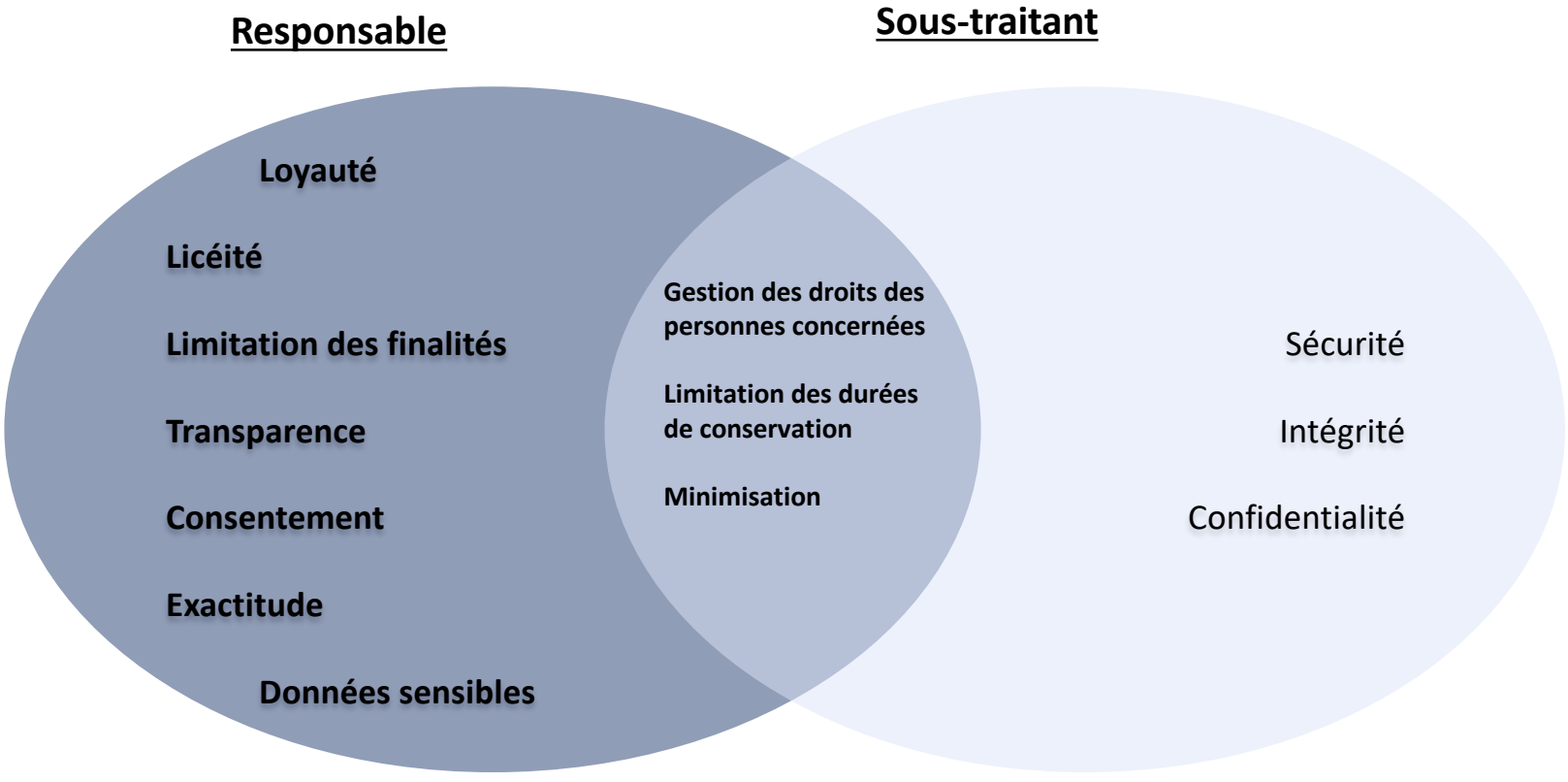
6. **Revoir vos contrats en place avec vos sous-traitants ultérieurs ;**

7. **Revoir vos contrats clients existants (avenant) ;**

8. **Revoir votre modèle de contrat avec les clients potentiels ;**

9. **Se positionner sur les contrats négociés sur la base du modèle de contrat du client.**

La répartitions des obligations:



BONUS : COMMENT PRÉPARER VOS OUTILS ?

Politique de gestion des habilitations et de contrôle d'accès

- **Définition des profils d'habilitation et limitation de l'accès des employés aux seules données strictement nécessaires à l'accomplissement de leurs missions**
- **Suppression des permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités**
- **Mise en place des procédures systématiquement appliquées à l'arrivée, au départ ou au changement d'affectation d'une personne**
- **Révision annuelle des habilitations**

Chiffrement et hachage

Solution de chiffrement adapté
Fonctions de hachage
Pseudonymisation/anonymisation
Outils et mesures visant à vérifier à l'intégrité du code

Politique de sauvegarde des données

- **Périodicité**
- **Serveurs de back-up (localisation, mesures de sécurités en place, etc.)**

Politique de journalisation des événements et de conservation des traces

- Enregistrement des événements pertinents
- Vérification que les journaux ne peuvent pas être modifiés
- Examen périodique des journaux d'événements/détection systématique des anomalies
- Audit des procédures permettant la notification immédiate toute anomalie/incident de sécurité

Politique de sécurisation des postes de travail

- Pare-feu / Antivirus / Mises à jour logicielles hebdomadaires
- Stockage des données en intra (espace de stockage régulièrement sauvegardé)
- Blocage d'applications téléchargées ne provenant pas de source sûre
- Limitation de la connexion de supports mobiles et désactivation de l'autorun

Politique de sécurisation de l'informatique mobile

- Chiffrement des postes nomades
- Chiffrement des supports amovibles
- Mécanismes de sauvegarde et synchronisation
- Mécanismes de protections contre le vol

BONUS : COMMENT ADAPTER VOS OUTILS?

Politique de protection du réseau informatique

- Blocage des services non nécessaires (ex:VoIP)
- Sécurisation des réseaux wi-fi (chiffrement)
- Cloisonnement des réseaux ouverts / invités du réseau interne
- Audit des accès aux interfaces utilisateur
- Limitation des flux réseaux au strict nécessaire, filtrage des flux entrants / sortants sur les équipements (pare-feu, proxy, serveurs, etc.)
- Vérifier qu'aucune interface d'administration n'est accessible directement depuis internet

Sécurisation des serveurs

- Accès à l'interface d'administration : politique d'authentification forte / contrôle d'accès renforcé
- Politique d'administration de bases de données
- Comptes nominatifs pour l'accès aux base
- Comptes spécifiques à chaque application
- Mesures contre les attaques par injection de code SQL, de scripts, etc.
- Cloisonnement des données sensibles
- Environnement d'administration des serveurs via un réseau dédié et isolé
- Outils de détection des vulnérabilités

Politique de protection des locaux

- Règles d'accès (ex: badge, accompagnement des visiteurs), différenciées selon les zones et selon les personnes concernées (employés/ prestataires externes / visiteurs)
- Mesures de contrôle / traçabilité des accès aux locaux
- Moyens de protection physique des matériels informatiques

Plan de reprise et continuité d'activité

- Interlocuteurs clients en cas de sinistre
- Intervenants tiers
- Procédure suivie
- Solution de contournement / Procédure de récupération /Serveur de back-up
- Délais
- Tests périodiques du PCA

Revoir vos contrats clients et vos contrats sous-traitants ultérieurs