La commission **LEGAL'IN TECH** de Medinsoft présente

LIVRE BLANC
RGPD

Règlement Général sur la Protection des Données

Un guide pour comprendre l'essentiel et mettre en oeuvre le #RGPD au sein de son entreprise

by

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

Avant-propos

Pourtant adopté dès 2016, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ou « RGPD », n'a fait parler de lui que récemment, avec l'approche de son entrée en vigueur le 25 mai 2018.

Si peu comprennent la teneur de cette réglementation, tous ont pour mémoire le montant impressionnant des amendes administratives. Entre peurs et incompréhensions, la plupart des entrepreneurs ne comprennent pas en quoi consiste réellement le RGPD, ni comment l'appliquer au quotidien. Pour exemple, la quantité astronomique de mails reçus le 25 mai, informant les personnes de l'entrée en vigueur du RGPD, alors même que ces envois étaient parfois ... illégaux et très souvent inutiles.

Nous, à la Commission LEGAL'IN TECH, nous favorisons une politique de l'apprentissage plutôt qu'une politique de la peur, et voulons mettre l'expertise de nos contributeurs au service des entreprises. C'est pourquoi plusieurs experts venus du domaine du droit, du numérique, du chiffre et de l'assurance se sont réunis afin de proposer une explication des nouvelles obligations pesant sur les entrepreneurs.
Accompagnés de quelques conseils pratiques, nous espérons que ces fiches pourront vous aider à appréhender une réglementation souvent perçue comme trop complexe.
Bonne lecture !

Océane Phan Tan luu
Présidente commission Legal'In Tech

A PROPOS DE LA COMMISSION LEGAL'IN TECH

La commission Legal'In Tech permet de rassembler des contributeurs et experts dynamiques d'horizons différents afin de bâtir une vision commune et partagée. Nous bâtissons ensemble des outils gratuits facilitant la prise en mains de sujets encore souvent perçus comment complexes.

-> MISSION

- Renforcer les actions pédagogiques et expertises
- Faire du droit un véritable levier business
- Mettre à disposition les meilleurs experts du droit, du chiffre et de l'assurance
- Créer des synergies entre les entreprises

Remerciements

La réalisation de ces fiches réflexe GDPR a été possible grâce au concours de plusieurs personnes à qui la Commission LEGAL'IN TECH voudrait témoigner toute sa reconnaissance.

- Stéphane SOTO, Directeur Général de l'association MEDINSOFT
- Olivier CAZZULO, Président NETSYSTEM DIGITAL
- Vincent RICHET, co-fondateur et Directeur Général de LA COQUE
- Franck RECOING, fondateur de GS PRADO
- Christelle FOURQUET, Expert-Comptable au cabinet ANTHEA ACCESS
- Robin STUCKEY, Avocat associé au cabinet PRIEUR STUCKEY & ASSOCIES
- Danielle PRIEUR, Avocate associé au cabinet PRIEUR STUCKEY & ASSOCIES
- Pierre SIFFRE, Avocat associé au cabinet MARS AVOCATS
- François LATOUR, Avocat
- Francis PAPAZIAN, Président de FINANCES ET CONSEIL MEDITERRANEE

Ont contribué à ce livre blanc

Océane PHAN-TAN-LUU
o.phantanluu@garoe-law.com
www.garoe-law.com

Océane PHAN-TAN-LUU est avocate au Barreau de Marseille où elle est associée fondateur du cabinet GAROE. Membre d'ALPHALEX AVOCAT, qui est présent dans toute l'Europe, elle exerce principalement dans les domaines de la Propriété Intellectuelle et du Numérique.
Présidente de la Commission Legal In Tech, Océane marque son engagement auprès des entreprises innovantes et est le conseil de plusieurs grandes entreprises européennes qu'elle accompagne dans leurs transformations digitales et la protection de leurs actifs de propriété intellectuelle.
Ses connaissances du fonctionnement des institutions et réglementations européennes sont un atout pour aborder et anticiper les mouvements réglementaires à venir dans ces domaines.

Alexandra BARBERIS
alexandrabarberis@avocat-marseille.eu
+33 4 84 35 05 57

Alexandra BARBERIS est avocat, spécialisée en Ingénierie des Sociétés, en Droit de la Propriété Intellectuelle et en Droit des Nouvelles Technologies. Depuis 2009, elle accompagne les chefs d'entreprise dans leur développement en leur permettant d'anticiper et de réduire les risques juridiques, grâce à un service innovant et adapté : le diagnostic juridique.
Véritable boussole, il permet au chef d'entreprise de naviguer dans un monde concurrentiel et ultra normé en évitant les écueils et en déterminant une marche à suivre.
Son engagement aux côtés des chefs d'entreprise se poursuit au sein de la CPME13, où elle exerce les mandats de Secrétaire élue et de Présidente du Club des Mandataires.

Kevin POLIZZI
www.jaguar-network.com

Jaguar Network accompagne les entreprises dans leur transformation numérique en leur fournissant des services souverains de confiance. Le groupe bénéficie d'expertises reconnues dans l'univers des télécommunications, du cloud, de l'IoT et des services managés. Jaguar Network s'appuie sur son réseau de qualité en fibres optiques interconnectant ses propres datacenters situés en France. Ceux-ci répondent aux normes les plus exigeantes en termes d'écoconception, d'exploitation et de sécurité : agrément HADS, certifications Santé, ISO 27001 & PCI-DSS.
L'innovation se positionne au cœur de l'ADN de l'entreprise qui investit massivement dans la R&D de services à valeur ajoutée pour le réseau et le cloud en intégrant des technologies comme le Edge Computing, l'IA, le Big Data et l'IoT.
Forte d'un réseau d'agences régionales, l'entreprise investit continuellement dans les infrastructures à très haute disponibilité et fournit ses services de nouvelle génération à plus de 1 200 clients, entreprises et organisations publiques.

Ont contribué à ce livre blanc

Charlotte BALDASSARI
contact@baldassari-avocats.com
www.baldassari-avocats.com

Avocate au Barreau de Marseille depuis 2006, Charlotte Baldassari a d'abord exercé dans deux cabinets d'avocats d'affaires (FIDAL, Colbert – ex Aelegis) intervenant principalement en Droit de la propriété intellectuelle, Technologies de l'information, Concurrence-distribution.
Au sein du cabinet Baldassari qu'elle a créé en 2013, elle se consacre aujourd'hui à la résolution de problématiques juridiques touchant à la propriété intellectuelle, au numérique et au droit des données personnelles, par le conseil, la défense contentieuse et la mise en place de solutions amiables alternatives au procès (médiation, droit collaboratif, etc.).
Elle est titulaire des certificats de spécialité en Droit de la Propriété Intellectuelle et Droit des Nouvelles Technologies et a participé au programme « Help dans les 28 » financé par le Conseil de l'Europe en partenariat avec le Conseil National des Barreaux sur le thème de la « Vie privée et protection de la vie privée » (40 heures en e-learning) afin d'appréhender dans toute sa complexité le RGDP qui entrera en vigueur en France le 25 mai 2018.
Elle est membre active de la Commission Droit de la Propriété Intellectuelle de l'Ordre du Barreau de Marseille, de la Commission LegalInTech de Medinsoft et de l'AFDIT.

Frédéric VILANOVA
frederic.vilanova@
effectiveyellow.com
www.effectiveyellow.com

Effective Yellow édite des logiciels de gouvernance dédiés aux Directeurs Métiers, DSI, DPO, RSSI. Les Effective Pilots permettent un pilotage multidimensionnel et fédérateur selon une dynamique collaborative moderne (multilingue, full web, tactile). En matière de gouvernance RGPD/GDPR nous distinguons deux phases :
- la phase « Design and Build », regroupant les audits, projets juridiques, techniques, organisationnels et la mise en œuvre des adaptations nécessaires,
- la phase « Run and Maintain » travaillant dans la durée sur le management des opérations (suivi des incidents , des alertes, des demandes...) et les extensions de périmètre.
Notre Effective Pilot RGPD/GDPR permet aux acteurs qui ont des fonctions transverses (Juriste, RSSI, DPO, etc.) de suivre les travaux les impliquant. Notre modèle de référence implémenté assure d'agréger les expertises et garantit la diffusion de l'information aux parties prenantes. Nos expertises pratiques en Direction Maîtrise d'Ouvrage, en Audit et en Consulting Big 5, nous permettent de comprendre vos attentes et de vous accompagner dans votre démarche de gouvernance outillée RGPD/GDPR, en mode standard ou sur-mesure.

Nicolas COURTIER
www.courtier-avocats.com
www.data-accountability.com

Nicolas Courtier est avocat, spécialiste en Droit de la Propriété Intellectuelle et en Droit des Nouvelles Technologies, de l'Informatique et de la Communication.
Depuis le début de sa carrière, il défend et conseille les entreprises, les collectivités et les associations pour tous les aspects du traitement des données.
Il membre de l'Association Française des Correspondants à la Protection des données à Caractère Personnel (AFCDP) et du conseil d'administration de l'Association Française de Droit de l'Informatique et de la Télécommunication (AFDIT). Il est l'auteur de Comprendre le règlement européen sur les données personnelles sans être juriste (Éditions Data Accountability Services, 2018 ; 70 pages). Il propose des formations sur le RGPD et intervient, en partenariat avec un prestataire technique de référence, pour la mise en conformité des organisations au RGPD et pour l'accompagnement des DPO.

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

Ont contribué à ce livre blanc

Marie-France VERFAILLIE
+ 33 7 64 07 37 73
www.bmo-conseil.com

Guide Marketing Stratégique depuis 12 ans, Marie-France VERFAILLIE accompagne les entreprises de la Tech pour leur développement sur les marchés BtoB et BtoC. Elle intervient d'une part pour co-établir une stratégie (business model et marque) qui pérennise le business mais surtout pour co-gérer avec les dirigeants au quotidien la mise en place de tous les leviers de développement de chiffre d'affaires, communication ou d'optimisation des coûts en interne. Sa particularité se positionne dans la volonté de grandir l'autre, et de laisser le pouvoir aux chefs d'entreprise afin qu'ils maintiennent le cap de leur instinct : en pleine connaissance et capacité d'exploiter les atouts. Son cerveau fertile, son énergie et ses capacités de mise en place sont mis à profit des échanges, de la stratégie et du développement de l'entreprise.

Laurence BOZZI
contact@aze-bozzi-avocats.fr

Laurence BOZZI est avocat depuis 1983 à MARSEILLE.
Elle exerce son activité en zone franche, au sein d'une structure qu'elle a contribué à créer, composée de quatre associés, 6 collaborateurs et 5 assistantes, plus particulièrement dédiée au droit de la responsabilité et au droit des assurances.
A ce titre, les enjeux de la GRPD lui sont tout naturellement apparus comme majeurs en termes de mise en danger de la pérennité des entreprises qu'elle conseille du fait des très lourdes sanctions encourues.
Rompue au contentieux de la responsabilité et au risque qu'il présente, elle aura à cœur de l'éviter en vous aidant à mettre en place des mesures propres à garantir la conformité de vos process à la réglementation qui entrera en vigueur le 28 mai 2018.
Sa pratique quotidienne du droit des assurances lui permet également de prendre en compte la protection assurancielle dont vous vous êtes dotés et les besoins qui sont les vôtres dans l'optique d'une couverture de risque maximale.
Elle pourra enfin et bien évidemment vous assister en cas de litiges judiciaire ou administratif, dans le cadre d'une défense experte et pugnace, visant à vous décharger le plus possible du poids nécessairement engendré par de telles poursuites.

Adrien MORANZONI
adrien.moranzoni@gsaprado.fr
www.gsaprado.fr

Chargé de clientèle en risques Cyber et Fraude au sein du groupe d'intermédiation en assurance Générale de Services et d'Assurances et l'agence SWATON, RECOING, BOILLETOT.
Adrien MORANZONI est à même de vous accompagner dans la mise en place d'une police d'assurance vous garantissant contre les atteintes aux données à caractère personnel et répondre ainsi aux risques auxquels vous serez soumis.
Par ailleurs, Doctorant près le Centre de Droit de l'Entreprise de l'Université de Montpellier, Il traite le sujet « Risque Cyber et Garanties d'assurance d'entreprise ». Il met ainsi à la disposition de nos clients et prospects mon expertise afin de les couvrir au mieux contre leur exposition au risque Cyber, un des risques majeurs du XXIème siècle pour les entreprises.
Il se tient à votre disposition pour toutes prises de rendez-vous et aura plaisir à répondre à toutes vos interrogations.

Ont contribué à ce livre blanc

Olinka MALATERRE
olinka.malaterre@temime.fr
+33 4 28 38 11 45

Inscrite au barreau de Marseille, Olinka MALATERRE a rejoint le cabinet TEMIME en 2013 après une première collaboration au cabinet de droit des affaires américain WEIL. Elle obtient un Master en droit des affaires à l'Université Paris I Panthéon- Sorbonne en 2007, qu'elle complète en 2008 en étudiant la majeure stratégie juridique et fiscale dans cette même université ainsi qu'à HEC Paris. Elle est spécialiste du droit pénal général, du droit pénal des affaires et des contentieux civil et commercial. Elle a acquis une compétence toute particulière pour les problématiques pénales liées au Règlement général sur la protection des données tant au stade pré-contentieux qu'au stade contentieux. Elle parle couramment l'anglais.

Jean Pierre GASNIER
jp.gasnier@akheos.fr
+33 6 29 62 72 02

Jean Pierre Gasnier est associé du cabinet Akheos et dirige le département IP/IT. Son expérience lui permet d'offrir une offre à forte valeur ajoutée à ses clients. Il accompagne notamment de nombreuses entreprises dans leur positionnement stratégique au regard des données personnelles. Il effectue de nombreux audits RGPD et enseigne le droit des données personnelles au sein d'une formation destinée aux DPO.

Olivia CHRISTOPHE
www.reachout.fr

ReachOut Communication : Agence de communication spécialisée dans la production de contenus print ou online et des stratégies de communication que ces contenus requièrent, qu'il s'agisse de stratégies numériques ou de stratégies de communication plus traditionnelles. Olivia Christophe, Présidente de ReachOut est, dans le cadre de différentes missions, amenée à rédiger des articles sur le RGPD pour le compte de clients du marché informatique (Marseille / Paris...).
Sa formation marketing permet une présentation claire et synthétique des informations et assurent un recul permettant une meilleure compréhension des enjeux. Sa spécialisation sur le marché informatique dans lequel elle a travaillé 10 ans avant de fonder ReachOut lui permet d'appréhender les enjeux plus rapidement.

Ont contribué à ce livre blanc

Ludovic PERROT
societe@uniy.fr
www.uniy.fr

Le cabinet Uniy est l'Interlocuteur majeur de la transformation d'entreprise en proposant une réflexion innovante sur les pratiques de travail liée au potentiel du digital.
Loin des modèles d'organisation de l'ère industrielle, l'entreprise 3.0 doit moderniser ses pratiques de travail pour s'adapter à l'ère digitale. L'enjeu est de répondre aux nouvelles attentes des clients et des collaborateurs pour rester attractif et compétitif, tout en étant conforme à la réglementation numérique.
Nous avons nommé Réseau Digital d'Entreprise (RDE) ce maillon complémentaire aux ressources humaines et à l'informatique. Notre mission est de concevoir ensemble votre RDE reflet de votre nouvelle organisation.

Jean-Fabrice PIETRI
jfpietri@gecarmed.fr
+33 6 09 86 46 23

Nos clients : les entreprises du territoire ou d'ailleurs, de la TPE à l'ETI locale, régionale ou internationale : nous accompagnons nos clients tout au long de leur développement.
Nos Partenaires Assureurs : les majors connues du grand public (AXA, ALLIANZ, GENERALI) mais aussi les compagnies spécialistes de métiers « hors nomenclature »
Nos domaines d'intervention : protéger l'activité (RC Professionnelle) les biens (Incendie et Pertes d'exploitations) et les hommes (Santé/Prévoyance) qui font l'entreprise.
Mais aussi : nous sommes présents sur les risques émergeants liés à l'écosystème digital : Cyber sécurité, Risques Environnementaux, RGPD etc..
Notre engagement : réactivité, rigueur, exigence vis-à-vis des assureurs, disponibilité pour nos clients.

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

COMPRENDRE L'ESSENTIEL

17 fiches pour se mettre à niveau

FICHE #1

PRESENTATION GENERALE

-> Nécessité d'adopter un nouveau règlement européen

L'Union européenne a adopté le Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) le 27 avril 2016.

Ce nouveau texte s'inscrit dans le cadre d'une réforme complète des dispositions européennes relatives à la protection des données ayant débuté en 2012, il est applicable à compter du 25 mai 2018.

Ce règlement a pour objectif de :

- Rendre aux citoyens le contrôle de leurs données personnelles
- Créer un niveau élevé et uniforme de protection des données à travers l'UE, adapté à l'ère numérique.

-> Contraintes et cadre général

Un règlement européen applicable :

- directement de l'UE ;
- à toutes les entreprises exerçant une activité dans l'UE ;
- dès qu'un résident européen sera directement visé par un traitement de données.

-> Quelques définitions

- **Donnée Personnelle** : Toute information se rapportant à une personne physique identifiée ou identifiable (notamment, par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale)

- **Analyse d'impact (PIA)** : Une Analyse d'impact relative à la protection des données (AIPD/ DPIA/PIA) est obligatoire dans les cas de surveillance systématique soit approfondi (profilage) ou systématique ou le traitement à grande échelle de catégories particulières de donnée (*). C'est une analyse de risque sur la sécurité des données personnelles.

- **Protection des données dès la conception** : Les mesures techniques et organisationnelles pour assure les sécurités des données personnelles sont mises en oeuvre dès la conception du traitement.

- **Data Protection Officier** : Fonction au sein d'une organisation ou externalisée qui a la charge de veiller à la conformité réglementaire en matière de protection des données à caractère personnel

- **Notifier les violations** : Obligation de notifier sous 72h toute violation de données personnelles à la CNIL et si l'impact est important aux personnes concernées.

- **Droit à l'oubli** : Une personne concernée a le droit d'obtenir l'effacement de données à caractère personnel la concernant pour des motifs légitimes.

- **Consentement de la personne concernée** : 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.

- **Portabilité des données** : Possibilité de recevoir les données à caractère personnel dans un format structuré, couramment utilisé et lisible par machine.

(*) catégories particulières de données : raciale, ethnique, politique, religieuse, philosophique, syndicale, orientation sexuelle, génétique, biométrique, liées aux condamnations et infractions

-> Allègement des obligations en matière de formalités préalables

Un règlement européen applicable :

- Suppression des déclarations CNIL
- Consultation de la CNIL pour les traitements les plus sensibles soumis à une analyse d'impact
- Champ des autorisations réduit

-> Sanctions

Bien qu'il soit souvent fait référence aux sanctions administratives, il est important de savoir que ce ne sont pas les seuls risques encourus par les entreprises. En effet le RGPD ouvre la possibilité aux personnes dont les données personnelles sont traitées en violation de leurs droits, de demander l'indemnisation de ce préjudice. Ces procédures peuvent être exercées individuellement ou collectivement.

DOMMAGES ET INTERETS

- Possibilité de procédure individuelle en indemnisation du préjudice, exercée par les utilisateurs du monde
- Sanctions civiles avec octroi de dommages et intérêts
- Sanctions pénales avec des amendes pénales pouvant aller jusqu'à 1 500 000 euros cumulables avec des dommages et intérêts pour les parties civiles

ACTIONS DE GROUPE

- Le RGPD ouvre la voie aux actions de groupe
- Pour les dommages consécutifs à une violation de la loi informatique et libertés et du RGPD
- Recours ouvert à tous, ces actions passent par un intermédiaire, une association dédiée ou un syndicat représentatif des salariés et fonctionnaires
- Joue pour la cessation du manquement et la réparation du préjudice à compter du 25 mai 2018

SANCTIONS ADMINISTRATIVES

- De 10 à 20 millions d'euros selon la catégorie de l'infraction
- De 2 à 4% du Chiffre d'Affaires annuel consolidé

-> Pourquoi ce guide ?

- La Commission LEGAL'IN'TECH a été mise en place pour réfléchir et proposer des solutions rapides, efficaces et pérennes aux entreprises face aux évolutions réglementaires. Cette Commission regroupe divers professionnels, experts comptables, entrepreneurs, assureurs, avocats qui se sont réunis afin de réfléchir aux problématiques d'aujourd'hui et de demain.

- Le RGPD étant un texte qui induit une profonde mutation du monde numérique, c'est donc tout naturellement que la Commission s'est saisie de ce sujet pour répondre aux préoccupations communes des entreprises et présenter dans un document clair et précis les enjeux, les impacts et les réponses à apporter face à cette nouvelle réglementation.

- Nous attirons toutefois l'attention du lecteur sur le fait que les recommandations, clauses et commentaires proposés ci-après sont purement génériques, et il est vivement recommandé de les adapter à chaque entreprise avec l'aide d'un expert qui tiendra compte de l'environnement et du contexte de l'activité.

- Ce guide contient 19 fiches réflexes qui ont pour vocation de rappeler les principaux points d'attention à respecter dans le cadre de la mise en oeuvre de la conformité au RGPD.

FICHE #2

GLOSSAIRE

En vue de partager un vocabulaire commun lié à la sémantique de sécurisation des données personnelles, il est important d'en définir les termes.

- **Anonymisation** : Processus qui permet de faire en sorte qu'une donnée ne permette plus d'individualiser la personne à laquelle elle se rattache, que des données distinctes portant sur un même individu ne permettent pas de corrélation et qu'on ne puisse pas déduire une information sur un individu.

- **Chiffrement** : le chiffrement est une opération qui permet de stocker des données, personnelles ou pas, dans un espace qui n'est plus lisible si l'on ne dispose pas de la clé de déchiffrement pour ouvrir le dispositif.

- **Consentement de la personne concernée** : 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.

- **Cloud / Cloud Computing** : est une technologie qui permet de mettre sur des serveurs localisés à distance des données de stockage ou des logiciels qui sont habituellement stockés sur l'ordinateur d'un utilisateur, voire sur des serveurs installés en réseau local au sein d'une entreprise.

- **Cloud - IaaS (infrastructure as a service)** : est un type d'informatique en mode Cloud qui fournit des ressources informatiques virtualisées via Internet.

- **Cloud - PaaS (platform as a service)** : désigne un service Cloud Computing permettant aux entreprises d'externaliser l'hébergement des outils logiciels et matériels de développement d'applications.

- **Cloud - SaaS (software as a service)** : désigne un service Cloud Computing permettant aux entreprises d'utiliser des logiciels ou des applications installés sur des serveurs hébergés en externe.

- **Data Protection Officier** : Fonction au sein d'une organisation ou externalisée qui a la charge de veiller à la conformité réglementaire en matière de protection des données à caractère personnel

- **Donnée Personnelle** : Toute information se rapportant à une personne physique identifiée ou identifiable (notamment, par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale)

- **Donnée Sensible** : Information qui concerne l'origine raciale ou ethnique, les opinions politiques, les opinions philosophiques ou les opinions religieuses, l'appartenance syndicale, des données biométriques, génétiques, des données comprenant le NIR, les condamnations, la santé ou l'orientation sexuelle. Elles bénéficient d'un régime juridique plus contraignant.

- **Finalité d'un traitement** : désigne le but du traitement. Ce peut être notamment la gestion des recrutements, la gestion des clients, la surveillance des locaux, le ciblage.

- **Incident** : désigne notamment toute anomalie, incompatibilité, dysfonctionnement, bogue, atteinte aux systèmes d'informations de l'entreprise, que ces systèmes soient conservés en interne ou sous traités en externe.

- **Infrastructure** : système d'installations, d'équipements informatiques et de services nécessaires au fonctionnement d'une entreprise.

- **Personne Concernée** : Une personne physique identifiée ou identifiable dont les données personnelles font l'objet d'un traitement.

- **Plan de Sécurité de l'Information** : procédures documentées servant de guide aux entreprises pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement sécuritaire prédéfini de l'information, à la suite d'une perturbation ou d'une lacune identifiée. Ce plan couvre généralement les ressources, les services et les activités requis pour assurer la sécurité des fonctions critiques.

- **Politique** : intentions, orientations et décisions d'une entreprise, mises en oeuvre par la Direction.

- **Privacy by design** : Chaque nouvelle technologie traitant des données personnelles ou permettant d'en traiter doit garantir dès sa conception et lors de chaque utilisation, même si elle n'a pas été prévue à l'origine, le plus haut niveau possible de protection adapté au traitement et au contexte.

- **Privacy by default** : Il s'agit de garantir que « seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. »

- **Processus** : ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie.

- **Procédure** : manière spécifiée d'effectuer une activité ou un processus.

- **Profilage** : Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

- **Programme de Sécurité de l'Information** : Ensemble de projets / d'objectifs soutenus par la Direction et dotés de ressources appropriées pour mettre en oeuvre, améliorer et maintenir le management de la sécurité de l'information.

- **Pseudonymiser** : désigne une technique de protection des données personnelles par laquelle un pseudonyme remplace le nom de l'individu auquel se rattachent les données.

- **Réseau Informatique** : désigne l'ensemble des moyens matériels et logiciels mis en oeuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.

- **Responsable du 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.

- **Sous-traitant (dans le cadre du RGPD)** : La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte et selon les instructions du responsable du traitement. Attention aux faux amis, vos sous-traitants ne sont pas forcément les sous-traitants des données à caractère personnel.

- **Système de Management de la Sécurité de l'Information SMSI** : partie du système de management global qui établit, met en oeuvre, opère, contrôle, révise, maintient et améliore la sécurité de l'information, quel que soit son support (numérique, papier...). Le système de management comprend la structure organisationnelle, les politiques, les planifications, les responsabilités, les procédures, les processus et les ressources.

- **Tiers** : Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les 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, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

FICHE #3

PREREQUIS DE LA SECURITE ET TRAITEMENT DES DONNEES PERSONNELLES

Avant d'entrer dans les arcanes de la sécurisation des données personnelles, il y a quelques opérations et réflexes simples à mettre en pratique, à renforcer, pour donner une base saine aux opérations ultérieures.

Le traitement de vos données personnelles doit s'appuyer sur celles-ci. Si tel n'est pas le cas, la conformité au RGPD pourra être remise en cause.

-> Organiser la gestion de ses données et les accès des utilisateurs

Pour organiser la sécurité de vos informations, l'une des premières démarches est de cartographier les lieux de stockage de vos données personnelles, par exemple : Applications traitant des données personnelles, stockage de fichiers, échanges de fichiers internes et externes, répertoires personnels ou partagés, bases de données.

Il est fondamental de situer les serveurs informatiques sur lesquels sont exploitées ses applications ainsi que les centres de données dans lesquels ces serveurs sont positionnés.

Un inventaire trimestriel est conseillé afin de démontrer la volonté de mise à jour de l'exhaustivité des traitements de l'entreprise. Cet inventaire peut être manuel mais le plus souvent il est automatisé via des applications prévues à cet effet (ex : ocs inventory, ...)

Il est également important de savoir si ces données sont organisées en fonction des métiers qu'elles adressent ou tous métiers confondus. La gestion des identités au sein d'un annuaire d'entreprise vous permettra d'extraire rapidement les accès aux fichiers personnels.

Il vous faut donc :

- Lister les zones de stockage où sont placées vos données métiers
- Identifier les accès à ces données selon le rôle et le niveau d'habilitation au sein de votre organisation
- Vérifier que les droits sont bien structurés afin de limiter les accès aux données personnelles et ainsi éviter les fuites de données.

Afin de parfaire à ce prérequis, il convient de vérifier que vous disposez d'une méthode efficace de gestion des identités numériques et de mots de passe.

-> Recommandations

- Gestion centralisée de la liste des utilisateurs sur un serveur sécurisé et dupliqué,
- S'assurer que chaque membre de l'organisation dispose d'un identifiant dédié et unique, couplé à une politique de mot de passe en ligne avec les préconisations de l'ANSSI (https://www.ssi.gouv.fr/guide/mot-de-passe/)
- La gestion des droits se fait par un profil d'accès en fonction des métiers et de niveaux d'habilitation de chacun.
- Certains profils aux pouvoirs étendus (administration technique d'applications, de base de données, etc.) sont dotés de mots de passe renforcés couplés à une authentification à double facteur (Token, SMS, etc.).
- La procédure d'octroi et de retrait d'un accès pour chacun des salariés de votre organisation doit être pilotée par le service RH et Sécurité de l'entreprise. Attention aux traitements particuliers à réserver aux collaborateurs externes tels que prestataires, intérimaires, stagiaires...

-> Bonnes pratiques et Politique de sécurité informatique

Politique de sécurité des systèmes d'information (PSSI)
Un document de référence doit décrire l'ensemble des mesures techniques et processus organisationnels visant à renforcer la sécurité informatique au sein de l'entreprise. La PSSI doit être partagée avec l'ensemble des collaborateurs de l'organisation et être revue régulièrement. Pour l'élaboration de la PSSI, vous pouvez consulter le guide proposé par l'ANSSI : https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/

Pare Feu (firewall)
D'un point de vue technique, le périmètre informatique doit être segmenté en différentes zones (trust, untrust), l'ensemble doit disposer au moins d'une protection périmétrique de type pare-feu et d'un système de détection d'intrusion afin d'alerter l'organisation en cas de fuite de données. Le pare-feu est un élément essentiel à la mise en oeuvre d'une politique d'accès aux ressources du réseau de votre organisation (vos serveurs de données, vos serveurs d'application...). Sa principale fonction est de contrôler le trafic entre différentes applications et utilisateurs en filtrant les flux de données qui y transitent. Ces zones de confiance variables incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la nécessaire confiance est plus importante).

Protection par utilisation de TLS et de certificat x509
Afin de maximiser la sécurité de vos échanges de données au sein d'un navigateur web, veillez à n'utiliser que les sites internet sécurisé par TLS et avec un certificat x509 venant d'une autorité de confiance reconnue. Les sites équipés d'une telle sécurité ont une adresse URL qui débute par « https ».

Un cadenas est affiché dans la barre de navigation signifiant que vos échanges sont chiffrés entre votre poste de travail et le serveur distant.
À défaut d'un audit général, évaluez la configuration TLS de votre serveur web en utilisant le site : https://www.ssllabs.com/ssltest/

Réseau d'accès distant - VPN
Pour garantir le secret des communications entre un poste de travail distant et les réseaux privés de l'entreprise, il est fortement conseillé de recourir à une connexion distante sécurisée de type VPN. Un tunnel virtuel chiffré est établi entre votre session utilisateur et le serveur de l'entreprise dédié à cet effet. L'ensemble des échanges est ainsi protégé par une clé de chiffrement permettant à vos flux de données de transiter par internet en toute confidentialité.

Audit régulier des infrastructures
Un plan de suivi régulier des infrastructures, des applications et de l'accès aux données doit être organisé sur une base annuelle, en interne par l'équipe dédiée à la sécurité ou en externe par une société de conseil spécialisée.
Un rapport d'audit doit mettre en évidence d'éventuelles failles liées à la non mise à jour des applications ou d'éventuels défauts liés à la conception du modèle de données. Ces éléments permettent d'établir une cartographie des risques à corriger dans un délai à déterminer en fonction du niveau de risque acceptable. Ce document pourra être demandé en support du registre des traitements par l'autorité de contrôle (CNIL).

Sauvegarde des données et continuité des opérations
En support de la politique de sécurité informatique, il est primordial de piloter la sauvegarde et la continuité de service des applications et données directement liées.

Sauvegarde/archivage/restauration
Un plan de sauvegarde doit être mis en oeuvre pour chaque application de l'entreprise, une durée de rétention des données doit être définie par le responsable du traitement en fonction des exigences métiers et de la nature de la donnée (archivage 10 ans pour les données comptables). Des tests de restauration de données doivent être validés sur une base régulière afin d'assurer le bon fonctionnement du processus de sauvegarde. De nombreuses solutions simples à mettre en oeuvre existent en local dans l'entreprise comme dans les infrastructures Cloud.

Plan de reprise d'activité (PRA)
Les applications sont le support prioritaire des traitements de l'entreprise, à ce titre elles nécessitent d'être intégrées dans le plan de reprise d'activité afin de limiter d'éventuels impacts sur l'organisation et le traitement des données personnelles.
Le PRA est déployé sur la base d'une durée maximale d'interruption admissible (Recovery Time Objective, RTO) et d'une durée maximale d'enregistrement des données (Recovery Point Objective, RPO).

FICHE #4

REGISTRE DES TRAITEMENTS

L'un des premiers documents à produire pour être conforme à la réglementation est un registre des traitements.

-> Qu'est-ce qu'un traitement ?

Tout ensemble cohérent de manipulations ou opérations automatisées ou non (collecte, transformation, stockage, transmission, destruction) de données personnelles réalisé par l'organisation ou pour son compte.
L'ensemble des traitements doit être identifié et cartographié.

-> Identification des traitements

Les traitements réalisés au sein d'une organisation sont en lien avec un ou plusieurs processus de l'entreprise. Ces derniers peuvent être en lien avec l'activité de l'organisation (processus métier) ou être des processus support (par exemple les processus des ressources humaines). Pour chaque processus réalisé, il est nécessaire d'identifier les données personnelles.
Les données ainsi identifiées au sein des processus doivent pouvoir être suivies de leur collecte à leur destruction en passant par toutes les utilisations ou stockage.
Les traitements préalablement déclarés à la CNIL devront figurer sur le registre.

Par exemple si vous êtes dans le domaine de la santé et accueillez des patients, vous avez un traitement de gestion administrative des patients et un traitement des données médicales des patients.
A vous d'en faire une cartographie efficace...

-> Responsable du traitement

Tout traitement doit avoir un responsable (une personne garante d'une exécution conforme au regard du RGPD). En général, c'est le représentant légal qui est garant du traitement pour l'entité.
Il peut être intéressant au sein d'une organisation, d'identifier les responsables conjoints : responsable technique, chef d'équipe, acteur référent, porteur du projet, etc. Cette identification permet de responsabiliser tous les acteurs et de vérifier en amont les chaines de responsabilité.
Il peut être intéressant de réfléchir avec un conseil spécialisé à la mise en place de délégations de pouvoir au sein de l'entreprise.

-> Analyse du traitement

Le responsable d'un traitement (ou un représentant) a l'obligation de déterminer les informations suivantes :

- La finalité du traitement qui peut être métier, support, réglementaire ou équivalent. Si des finalités secondaires existent celles-ci devront être répertoriées ;
- La date à laquelle le traitement a commencé à être utilisé.

Pour chacune des étapes du traitement (collecte, transformation, stockage, transfert, destruction), il est donc nécessaire d'identifier :

- Les outils utilisés (applications informatiques, armoires de stockage de documents papiers, fax, serveur de fichier, courriel, etc.) ;
- L'entité qui réalise l'opération en particulier si celle-ci est un tiers qui peut être un sous-traitant au sens du RGPD ;
- Les mesures appliquées pour assurer la sécurité des données, des outils et des opérations ;
- Les catégories de données traitées en particulier si des données sensibles sont manipulées ; en prenant soin pour chaque catégorie de lister les durées de conservation ou délai d'effacement.

Pour les étapes de collecte d'information, il est aussi nécessaire d'identifier les catégories de personnes à qui appartiennent les données collectées, en particulier si ce sont des personnes vulnérables.

Pour les étapes de transfert d'information, il est indispensable de pouvoir déterminer :

- Les destinataires des données,
- Les localisations vers lesquelles les données sont envoyées en particulier si elles sont envoyées en dehors de l'Union Européenne, dans ce dernier cas il est nécessaire d'avoir déterminé les mesures qui garantissent un niveau de sécurité adéquat.

Le règlement prévoit que les données personnelles peuvent circuler librement entre les pays membres de l'UE (ainsi qu'avec la Norvège, le Liechtenstein et l'Islande).

Cependant, il réduit drastiquement les possibilités de transferts de données vers un pays tiers. Pour certains pays, la Commission Européenne a prise des décisions d'adéquation qui permette le transfert dans des conditions quasi identiques, notamment pour des pays comme Andorre, l'Argentine, le Canada, Israël, la Nouvelle-Zélande, la Suisse ou l'Uruguay.

Néanmoins, si vous effectuez des transferts hors UE, nous vous recommandons vivement de vous rapprocher d'un conseil spécialisé afin de vérifier que les restrictions existantes et les procédures à mettre en oeuvre.

-> Inscription sur le registre

L 'analyse du traitement permet ensuite de procéder aux inscriptions sur le registre du traitement qui doit être à disposition en cas de contrôle.

- Ce document assure que les informations suivantes soient enregistrées une référence du traitement (nom, sigle, numéro, etc.),
- La date à laquelle le traitement a commencé à être utilisé,
- Le nom du responsable du traitement,
- Si un délégué à la protection des données existe, celui-ci devra aussi être nommé.
- La finalité,
- Les mesures mises en oeuvre,
- Le type de données traitées, en particulier les données sensibles, avec le délai d'effacement,
- Les catégories de personnes concernées en particulier les personnes vulnérables,
- Les destinataires des données et pour celles transférées en dehors de l'Union Européenne le pays et le type de garanties.

Un modèle de document est disponible sur le site de la CNIL :
https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

-> Informations supplémentaires

Afin de préparer les PIA (analyse d'impact sur les données personnelles), il peut aussi être intéressant de noter dans le registre les informations suivantes :

- Si le traitement concerne une évaluation ou une notation (profilage) ;
- Si le traitement implique une prise de décision automatique avec effet juridique ou similaire immédiat ;
- Si le traitement concerne une surveillance systématique ;
- Si le traitement concerne des données sensibles (déjà identifiées par la cartographie) ;
- La volumétrie de données aussi bien en valeur absolue et en proportion de la population concernée, l'étendue géographique, la durée de traitement ;
- Si le traitement réalisera un croisement de deux autres jeux de données réalisés à des fins différentes ;
- Si le traitement concerne des personnes vulnérables (identifiées dans la cartographie) ;
- Si le traitement est réalisé à l'aide d'une technologie innovante pour laquelle les risques ne sont pas connus ou maîtrisés ;
- Si le traitement peut « empêcher les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat ».

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

FICHE #5

PRIVACY IMPACT ASSESSMENT

-> Etude d'impact sur la vie privée

Lorsqu'un nouveau traitement est mis en oeuvre dans l'entreprise (également applicable en cas de fusion de sociétés, d'acquisition d'une entreprise), le responsable du traitement devra, dans certains cas, anticiper les difficultés en réalisant, en amont, une étude d'impact du traitement sur la vie privée.
L'étude d'impact (« PIA », pour Privacy Impact Assessement) est une analyse méthodique à valeur probante (un audit spécifique), visant à s'assurer qu'un traitement est considéré a priori à risque (traitement de masse, données sensibles, profilage) :

- d'une part, respecte les droits fondamentaux des personnes,
- d'autre part, minimise les risques en termes de sécurité et de violation des obligations légales.

-> Quand l'étude d'impact est-elle nécessaire ?

À chaque fois que je traite des données personnelles, je dois me poser les 4 questions suivantes :

1. Le traitement effectué a-t-il potentiellement un impact sur la vie privée des personnes concernées ? (Mes clients et prospects, mes salariés, patients ...)
2. Les données concernées par ce traitement sont-elles des données personnelles sensibles ?
3. Le traitement des données est-il effectué à grande échelle ?
4. Plusieurs sources sont-elles utilisées pour effectuer le traitement ?

Si je réponds oui à au moins une de ces 4 questions alors une étude d'impact est indispensable.

-> Quelle méthode employer pour conduire un PIA ?

Pour évaluer le niveau de risque lié au traitement, il convient de prendre en considération les principes fondamentaux en matière de protection et de respect de la vie privée :

- Le respect des principes juridiques en matière de protection de la vie privée
- La protection et la traçabilité des données à caractère personnel

Deux facteurs sont à inclure au coeur de chaque étude de PIA afin d'en évaluer correctement le risque :

- La gravité (impact du risque) : elle représente l'ampleur d'un risque et dépend essentiellement du caractère préjudiciable sur les personnes des impacts potentiels.

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

- La vraisemblance : traduit la probabilité de survenance du risque au regard de votre vulnérabilité potentielle.

Celle-ci dépend essentiellement des vulnérabilités de votre système d'information : il s'agit simplement d'évaluer votre surface d'exposition face aux menaces potentielles concernant les traitements impliqués.

Les deux critères de vraisemblance et de gravité sont échelonnés sur quatre niveaux de valeur :

Négligeable	Suppose une sécurité globale répondant aux recommandations de la Commission, donc un niveau de risque proche de zéro.
Limitée	Les recommandations sont globalement appliquées, néanmoins il existe une zone de risque faiblement traitée ouvrant des failles impliquant des fuites de données à caractère personnelles potentielles.
Importante	Les mesures de sécurité sont insuffisamment documentées/validées/testées. Il existe ainsi un risque fort de fuite de données liées à des risques connus.
Maximale	L'implémentation d'une politique de sécurité est inexistante, par conséquent la gestion des traitements ne respecte pas les droits fondamentaux des personnes.

Différents éléments doivent être pris en compte dans la conduite du PIA, notamment, mais non exclusivement :

- Choix et consentement des personnes,
- Légitimité de la finalité du traitement et limitation d'usage des données à caractère personnel,
- Niveau de sensibilité des données personnelles,
- Accès des utilisateurs aux informations et capacité à les maintenir en toute circonstance intègres,
- Responsabilités des acteurs impliqués dans le traitement des données personnelles,
- Sécurisation des données personnelles,
- Mise en responsabilité des sous-traitants, des fournisseurs,
- Procédure de réponse et de restitution en cas de violations/atteintes sur données personnelles,
- Etc.

La cartographie des traitements de données personnelles est indispensable pour pouvoir rédiger les PIA et remplir le registre des traitements. Cette cartographie nécessite de lister dans un fichier excel toutes les données personnelles traitées par votre structure.

Nous vous recommandons de différencier les données personnelles interne (celles que vous collectez au sein de votre structure, auprès de vos collaborateurs et cocontractants) et les données personnelles externes (celles que vous collectez via vos produits, solutions, etc.).

Pour chacune de ces données personnelles vous devez lier a minima les informations suivantes :

- Le ou les traitements qui concerne cette données
- La finalité du ou des traitements
- Le temps de conservation
- La localisation de ces données
- Les modalités de consentement
- Si cette donnée est transférée à un tiers ou récupérée via un tiers
- Si cette données est transférée hors UE

Après l'évaluation des risques, incluant une matrice pour chaque risque de gravité et vraisemblance, un croisement des résultats est effectué pour positionner les différents niveaux risques sur une analyse d'impact. C'est au DPO qu'il incombe la prise de décision finale concernant les actions correctrices en vue de maintenir une conformité optimale au Règlement, des traitements de données effectuées par l'entreprise.

Chaque nouveau traitement induit la réalisation d'une nouvelle étude d'impact, et donc un rapport de PIA ad hoc.
Il est important de réaliser des PIA régulièrement concernant l'ensemble des traitements de l'entreprise.
Sauf cas particulier, il est recommandé de protéger les résultats issus d'un PIA dans un niveau de diffusion restreint.

-> Qui peut conduire un PIA ?

Le PIA peut être réalisé via un collaborateur en interne dédié aux fonctions de sécurité informatique tout comme un responsable de traitement portant ainsi un risque dans son périmètre fonctionnel.

Les interlocuteurs dédiés aux missions de sécurité comme le DPO ou le RSSI doivent être systématiquement informés des risques et niveaux de menace qu'exposent les traitements.

Des auditeurs externes peuvent également conduire un PIA, tels qu'un fournisseur ou sous-traitent, toutefois le responsable du traitement de l'entreprise reste responsable d'apporter systématiquement une réponse adaptée à une menace donnée.

-> Que faire en cas de contrôle ?

Il est indispensable de présenter le ou les rapports de PIA à l'autorité de contrôle afin qu'elle puisse déterminer la conformité du traitement au règlement.

-> Pour aller plus loin

La CNIL propose un logiciel libre et ouvert, sous licence GPLv3 : PIA, qui a pour objectif de faciliter la conduite et la formalisation d'analyses d'impact sur la protection des données telles que prévues par le RGPD.

Vous pouvez aussi avoir recours à des consultants spécialisés en audit, notamment pour les sociétés internationales ou multisite.

Une méthodologie complète est disponible en libre accès sur le site de l'autorité de contrôle compétente : https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf

Une application multi-environnements est disponible en OpenSource : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

FICHE #6

RECUEIL DU CONSENTEMENT

-> Pourquoi recueillir le consentement ?

- Le consentement est défini par le RGPD comme « 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 ».
- En matière de données personnelles, le consentement est donc une démarche active de l'utilisateur, explicite et de préférence écrite, qui doit être libre, spécifique, et informée.
- Cette notion de consentement est un élément clef de la conformité des traitements mis en oeuvre puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement portant sur leurs données.
- Le consentement est nécessaire dans certaines conditions pour légitimer l'utilisation des données personnelles recueillies. C'est le G29, entité qui regroupe les autorités de contrôle des traitements des données personnelles de tous les Etats membres, qui a précisé cette notion et donné des illustrations pratiques.

Attention : Une vigilance accrue doit être portée aux traitements dits sensibles (données concernant les mineurs, données de santé...)

-> Les bonnes pratiques

Le tableau ci-après synthétise les dispositions, bonnes pratiques et précautions en la matière à ce jour, étant précisé qu'il convient de rester attentif aux futures évolutions doctrinales de cette notion.

Notion	Signification	En pratique
« Consentement exprès »	Il s'agit d'une manifestation de volonté de la personne concernée, dont la preuve peut être amenée par tout moyen, mais nécessite une action positive de l'utilisateur.	• Déclaration ou signature écrite, y compris par voie électronique • Déclaration orale • Case à cocher (non pré-cochée par défaut) lors de la consultation d'un site internet • Comportement dont on peut raisonnablement déduire un accord (exception interprétée de manière restrictive), comme le dépôt de sa carte de visite. Attention : l'activation d'une application ou de la fonction Bluetooth ne constitue pas un consentement valable.

COMMISSION LEGAL'IN TECH

THEMATIQUE #RGPD

Notion	Signification	En pratique
« Consentement libre »	Le consentement n'est valable qui si le choix a été effectué librement, c'est-à-dire s'il n'y a pas de risque de tromperie, d'intimidation, de coercition (qu'elle soit sociale, financière, psychologique ou autre) ou de conséquences négatives. La personne concernée doit également pouvoir retirer son consentement sans subir de préjudice réel ou potentiel.	A titre d'illustration, n'est pas considéré comme donné librement un consentement donné : • sous l'influence du Responsable de traitement (par exemple lien de subordination) ; • en état de dépendance vis-à-vis du Responsable de traitement ; • par crainte d'être traité différemment en l'absence de consentement ; Ces situations pouvant être rencontrées dans un contexte professionnel notamment, il est essentiel de faire attention au mode de recueil du consentement, et de prendre en compte la finalité du traitement.
« Consentement Informé / Eclairé »	La personne concernée doit recevoir, de façon claire et compréhensible, des informations exactes et complètes sur tous les éléments pertinents du traitement. Cela suppose également la connaissance des conséquences du refus de consentir au traitement des données en question.	• Qualité des informations : texte en clair, compréhensible pour tous, visible • Accessibilité et visibilité des informations : *nécessité d'une communication des informations à la personne concernée (il ne suffit pas que les informations soient «disponibles» quelque part), *taille et type de caractère lisibles, *affichage d'une boîte de dialogue ou d'une page en surexposition au moment du recueil du consentement... • Revue des choix et confirmation (information régulière des personnes concernées, selon une fréquence à déterminer, portant sur les mentions obligatoires et la possibilité de confirmer ou de retirer son consentement).
« Consentement spécifique »	Chaque traitement et donc chaque recueil du consentement doit être lié à une finalité spécifique : il n'est pas possible de faire un recueil de consentement global.	Obligation de détailler chaque recueil du consentement par rapport aux différents éléments / finalités qui constituent le traitement de données Attention : • Un consentement « général » ne constitue pas un consentement spécifique, et n'est pas valide ; • L'acceptation des conditions générales ne vaut pas acceptation d'un traitement spécifique des données personnelles ; • Les documents prévoyant le consentement automatique pour tous les traitements futurs n'est pas conforme. • Le renvoi à une convention collective n'est pas conforme.

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

Notion	Signification	En pratique
« Consentement univoque »	Pour qu'un consentement soit univoque, la procédure relative à l'obtention et à l'octroi du consentement ne doit laisser aucun doute quant à l'intention de la personne concernée de donner son consentement.	Obligation d'apporter la preuve du consentement : • Mise en place de procédures et de mécanismes techniques et organisationnels • Une absence de réponse ne vaut pas consentement.

-> Le droit d'opposition

Toute personne a le droit de s'opposer, pour des motifs légitimes, au traitement de ses données, sauf si celui-ci répond à une obligation légale (Article 21 du RGPD).

Il est impératif que les personnes puissent s'opposer directement à la réutilisation de leurs coordonnées à des fins de sollicitations, notamment commerciales, lors d'une commande ou de la signature d'un contrat. Ce choix doit pouvoir être formulé par une action directe (case à cocher par exemple) sur le formulaire ou bon de commande.

La simple mention du droit d'opposition dans les conditions générales n'est pas suffisante.

-> Les droits d'accès et de rectification

Au moment de la collecte des données, le Responsable du traitement a l'obligation d'indiquer aux personnes concernées le service auprès duquel elles pourront exercer leur droit d'accès.

Toute personne doit notamment pouvoir (cette liste n'est pas limitative):

- Accéder à l'ensemble des informations recueillies la concernant et notamment demander à connaitre (Article 15 du RGPD) :
  > les destinataires ou catégories de destinataires auxquels ses données à caractère personnel ont été ou seront communiquées et, dans le cas de transfert à des pays en dehors de l'UE, des garanties appropriées
  > les catégories de données à caractère personnel concernées
  > la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée
  > l'existence d'une prise de décision automatisée (scénario marketing ou profilage) et la logique utilisée, ainsi que les conséquences prévues de ce traitement pour la personne concernée

- Faire rectifier les données personnelles la concernant dans les meilleurs délais (Article 16 du RGPD)
- Obtenir l'effacement dans les meilleurs délais des données personnelles la concernant (Article 17 du RGPD) sauf dans la mesure où le traitement est nécessaire :
  > à l'exercice du droit à la liberté d'expression et d'information
  > pour respecter une obligation légale
  > pour des motifs d'intérêt public dans le domaine de la santé publique
  > à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques
  > à la constatation, à l'exercice ou à la défense de droits en justice
- Obtenir la copie des informations et données personnelles traitées par le Responsable du traitement, sous un format structuré, lisible sur tout support électronique et clair. Des frais n'excédant pas le coût de reproduction peuvent être demandés.
- Obtenir la portabilité des données personnelles la concernant (Article 20 du RGPD)

-> Délai de réponse

A compter du 25 mai 2018, le Responsable du traitement aura un mois pour faire droit aux demandes des personnes concernées. A défaut, les personnes concernées pourront adresser une plainte à la CNIL.

-> Recommandations

- Mettre en place une organisation chargée de traiter les demandes informatique et libertés des personnes
- S'assurer des mécanismes de consentement et des procédures permettant de s'assurer du recueil et de la conservation du consentement des personnes concernées
- Surveiller les délais de réponse
- S'assurer que les demandes des personnes concernées par les traitements puissent être techniquement traitées
- Formation des équipes

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

FICHE #7

PRIVACY BY DESIGN BY DEFAULT

-> Contexte et principes de base

L'article 25 du Règlement RGPD impose que le responsable de traitements mette en oeuvre les mesures techniques et organisationnelles appropriées afin de protéger les droits de la personne concernée par le traitement des données personnelles ; les données personnelles doivent ainsi être protégées :

- Dès la conception (« Privacy by design ») ; et
- Par défaut (« Privacy by default »).

-> Que signifie Privacy by design ?

L'article 25 point 1 du Règlement indique que ces mesures doivent être mises en oeuvre au moment du traitement lui-même, mais aussi au moment de la détermination des moyens de traitement, c'est-à-dire lors de la phase, préalable au traitement, de conception et/ou de sélection des outils et de l'organisation d'entreprise qui vont permettre le traitement.

Les 7 principes du Privacy by design sont :

1. **La proactivité et non la réactivité :**
Les mesures prises doivent viser à prévenir et anticiper les risques d'atteinte aux données personnelles plutôt que d'attendre la survenance d'une atteinte pour y remédier. Nécessite la formation du personnel, la mise en oeuvre et l'évaluation des politiques de protection des données. Responsables : Management de haut niveau (Comité de direction, DG, Directeurs, etc.).

2. **Le respect de la vie privée par défaut :**
L'objectif est d'aboutir à un système de protection automatique de la vie privée par les systèmes d'information (SI) et dans l'activité de l'entreprise. Voir point spécifique ci-dessous. Responsables : Les concepteurs, développeurs ou éditeurs de logiciels et les personnes responsables de l'exploitation et/ou des process dans l'entreprise.

3. **Le respect de la vie privée fait partie intégrante de la conception :**
Le respect de la vie privée ne doit pas être intégré comme un module complémentaire au sein des SI, a posteriori. Au contraire, l'analyse des risques sur la vie privée doit se faire dès la conception :
• Les principes de protection doivent faire partie des règles de fonctionnement de base,
• le respect de la vie privée doit être intégré dans le cycle de vie et le processus de conception des logiciels. Responsables : Les concepteurs, développeurs ou éditeurs de logiciels et les personnes responsables de l'exploitation et/ou des process dans l'entreprise.

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

4. Une intégration à somme positive :
Le respect de la vie privée doit être intégré selon une approche « gagnant-gagnant » et non au détriment d'autres intérêts légitimes de l'entreprise. Ce principe nécessite communication, consultation et collaboration (3C) au sein de l'entreprise pour identifier l'ensemble des intérêts divergents et trouver des solutions innovantes pour les concilier. Responsables : Management de haut niveau, concepteurs, développeurs ou éditeurs des logiciels et personnes responsables de l'exploitation et/ou des process dans l'entreprise.

5. Sécurité de bout en bout et protection pendant tout le cycle traitement :
La sécurité est la clef du respect de la vie privée et doit être assurée de la collecte à la destruction des données. Le chiffrement devrait être utilisé par défaut, et de manière habituelle dans les équipements de travail quotidien, pour éviter les risques en cas de perte ou de vols des équipements portables (laptops, tablettes, smartphones et clefs USB notamment), en rendant les données illisibles sans clés. La destruction des données doit être assurée à la fin du cycle de traitement des données. Responsables : Les concepteurs, développeurs ou éditeurs de logiciels et les personnes responsables de l'exploitation et/ou des process dans l'entreprise.

6. Visibilité et transparence :
Il faut s'assurer que, quelle que soit la pratique de l'entreprise et les technologies utilisées, le traitement des données est transparent pour les personnes concernées, conforme aux objectifs pour lesquels elles ont été collectées et vérifiées de manière indépendante. La mise en oeuvre de ce principe implique de communiquer les coordonnées des personnes chargées de la sécurité et du respect de la vie privée, de mettre en place une politique de rédaction des documents publics dans un langage accessible, de rendre accessibles les politiques, procédures et mesures de contrôle des données personnelles, éventuellement de publier des synthèses des études d'impact (PIA) ou des résultats d'audits, rendre disponible une liste des bases de données personnelles de l'entreprise et des outils d'audit. Les personnes concernées doivent pouvoir déterminer si les politiques de protection sont correctement suivies. Responsables : Management de haut niveau, concepteurs, développeurs ou éditeurs des logiciels et architectes systèmes.

7. Centrer sur l'utilisateur :
L'intérêt de la personne concernée par le traitement de ses données doit être la préoccupation principale. Il faut dont offrir une protection forte de la vie privée en fournir les informations appropriées et éventuellement prévoir des options ergonomiques ou conviviales (par exemple : Conservation et effectivité des préférences utilisateur, fournir spontanément un accès aux données les concernant et aux pratiques de l'entreprise sur les données personnelles, etc.). Responsables : Management de haut niveau, concepteurs, développeurs ou éditeurs des logiciels et personnes responsables de l'exploitation et/ou des process dans l'entreprise.

-> Privacy by default

La protection de la vie privée doit être une fonction automatique qui prévoit une collecte de données :

- pour des objectifs les plus restreints et ciblés possibles (en commençant par « pas de collecte »),
- la plus minimisée possible et strictement limitée à ce qui est nécessaire, notamment concernant la quantité, la durée de conservation et l'accessibilité des données,
- pour le seul usage correspondant à l'objectif.

Une séparation doit être mise en place pour empêcher les liens entre les différentes informations sur les personnes, par une politique de sécurité et de confidentialité des données personnelles, des procédures et les technologies utilisées dans l'entreprise.

Une personne physique ne doit pas avoir à intervenir pour que ses données personnelles soient protégées et accessibles uniquement à un nombre limité de personnes physiques.

-> Pour aller plus loin dans l'implémentation

Consulter le guide "Operationalizing Privacy by Design – A Guide to Implementing Strong Privacy Practices, Ann Cavoukian, December 2012" accessible à l'adresse suivante : www.ontla.on.ca/library/repository/mon/26012/320221.pdf

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

FICHE #8

DOCUMENTER SA CONFORMITE

-> Pourquoi ?

En cas de contrôle par la CNIL, ou toute autre autorité de contrôle, il vous sera demander de présenter un recueil de documents destinés à prouver votre démarche initiale de mise en conformité RGPD ainsi que les preuves de maintenance annuelle (suite des changements, des fusions, des acquisitions...).

DOCUMENTATION SUR VOS TRAITEMENTS DE DONNÉES PERSONNELLES	INFORMATION DES PERSONNES	CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS
Pour les responsables de traitements : Le registre des traitements de données. Il faut en préparer trois : 1. Le registre du responsable de traitement 2. Le registre de sous-traitance qui répertorie les données personnelles faisant l'objet d'une sous-traitance. Si vous faites de la sous-traitance pour un tiers, ou si vous traitez des données récupérées avec un sous-traitant. Il est important de séparer les deux cas dans le registre. 3. Le registre de notification de violation des données personnelles qui contient le listing des notifications envoyées auprès des autorités de contrôle de l'UE. **Dans le cas où vous êtes un sous-traitants de traitement des données personnelles :** Le registre de sous-traitance doit contenir les catégories d'activités de traitements des données.	Le registre doit contenir également tout document permettant l'information des personnes concernées (mentions légales, CGV, contrats clients, etc.). D'où l'importance de mettre à jour vos documents commerciaux types. Les modèles de recueil du consentement des personnes concernées. Il vous faut également prévoir une méthode de conservation du consentement donné, tout en vous assurant que ce traitement particulier de conservation du consentement respecte les obligations générales du RGPD.	• Les contrats avec les sous-traitants. Cela peut être des CGV, des contrats, des bons de commandes, etc. • Il est essentiel de contacter l'intégralité de vos prestataires et de leur demander s'ils sont en conformité avec le règlement. En tant que responsable du traitement vous devez vous assurer que les données personnelles que vous traitez le soit en respectant les droits des personnes concernées.

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

DOCUMENTATION SUR VOS TRAITEMENTS DE DONNÉES PERSONNELLES	INFORMATION DES PERSONNES	CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS
Dans tous les cas : • Les différents registres doivent intégrer la typologie de données personnelles traitées et indiquer clairement le ou les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes. • Les analyses d'impact sur la protection des données (PIA) (recommandé cf : outil CNIL fiche 5) Un modèle de registre est disponible sur le site de la Cnil, nous vous recommandons d'adapter ce document à votre activité pour qu'il soit le plus clair et précis possible.		Les procédures internes en cas de violations de données.
L'encadrement des transferts de données hors de l'Union européenne (notamment, les clauses contractuelles types, les Binding Corporate Rules et certifications) Référence : https://www.cnil.fr/fr/definition/bcr-binding-corporate-rules	Les procédures mises en place pour l'exercice des droits : liste des documents.	Les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

FICHE #9

AFFICHE LEGAL DATA PROTECTION

Vous trouverez dans cette fiche, différents modèles d'affichage qui sont à adapter au cas par cas, mais permettent d'informer vos collaborateurs et de laisser à leurs dispositions les informations essentielles en cas d'incidents et de prévenir les risques de contentieux.

Cet affichage légal est un premier pas dans l'assimilation des procédures de protection des données personnelles au sein de votre structure, il est important de coupler cela avec une sensibilisation, voir une formation particulière de vos collaborateurs sur ce sujet.

Il est également essentiel que vous vous assuriez que les stagiaires, alternant, free-lance, etc. soit au courant des mesures mises en place dans l'entreprise.

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

AFFICHAGE #1 : INFORMATION RGPD

-> Contexte et principes de base

- À cause des risques inhérents au traitement des données personnelles, l'UE a mis à niveau et harmonisé la réglementation applicable à la capture et au traitement des données personnelles afin d'assurer la sécurité des utilisateurs sur le sol européen. (Règlement 2016/679)
- L'entreprise met en oeuvre une politique de protection des données personnelles très strictes, tant vis-à-vis des clients que vis-à-vis des salariés.

-> Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est définie comme toute information permettant d'identifier directement ou indirectement une personne, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

-> Points de vigilance

- Si vous observez une faille dans la protection des données personnelles au sein de l'entreprise
- en cas de développements de nouveaux projets, ou encore
- dans le cas où les données seraient volées par des tiers
- etc.

Merci de prendre contact immédiatement avec les personnes en charge au sein de l'entreprise.

Personnes à contacter au sein de l'entreprise

Responsable du traitement :

Nom	Mail	Téléphone

Service juridique

Nom	Mail	Téléphone

Délégué à la protection des données

Nom	Mail	Téléphone

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

MESURES EN CAS DE CONTRÔLE

Que faire ?

Lorsque les agents se présentent :

- Alerter immédiatement la Direction et le département juridique
- Noter l'identité des personnes qui se présentent pour le contrôle
- Faire patienter les agents dans une pièce ne comportant aucun ordinateur ou appareil électronique ; cette pièce doit pouvoir être fermée par une porte.
- Leur proposer un café dans l'attente.

En toute circonstance :
Garder son calme, rester courtois

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

AFFICHAGE #2 : SIGNALEMENT DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

1. Détectez les incidents de sécurité de l'information

Soyez vigilant à tout événement portant atteinte à la confidentialité, intégrité ou disponibilité des activités ou informations de l'entreprise et pouvant avoir un impact important sur les aspects : opérationnel, notoriété, financier, contractuel ou réglementaire.

2. Signalez rapidement l'incident de sécurité, auprès de :

- DPO
- ANSSI
- CNIL ...
- Votre correspondant sécurité
- Ou du RSSI
- Ou la Direction

3. Déclarez l'incident de sécurité

Vous disposez à tout moment de deux moyens pour notifier un incident de sécurité en interne :

Déclaration et traçabilité par mail	

Chaque demande doit contenir des éléments de contexte et de traçabilité (horodatage, ...)

- Qualification de l'impact de l'incident et le domaine de responsabilité :
  - > Impact sur les données personnelles ou de santé
  - > Impact sur l'entreprise sans conséquence pour les services Clients ;
  - > Impact sur service Client dont l'entreprise est responsable des mesures de sécurité ;
  - > Impact sur service Client dont l'entreprise n'est pas responsable des mesures de sécurité ;
  - > Signaler en interne l'incident de sécurité et des circonstances (origines, conséquences)

- Actions correctives en cours, prévues ou réalisées pour réduire/ résoudre l'incident de sécurité

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

FICHE #10

PREVENTION DU CONTENTIEUX

-> Revoir et sécuriser les contrats commerciaux de l'entreprise

Il est essentiel de passer au crible les contrats commerciaux, notamment les conditions générales, afin de les mettre en conformité avec les nouvelles obligations liées au RGPD (c'est aussi l'occasion de vérifier que les contrats ont pris en compte la réforme du droit des contrats qui est intervenue en octobre 2016).

- Des contrats commerciaux juridiquement solides permettent d'éviter une grosse source de contentieux, que ce soit avec vos partenaires, vos clients ou toute autre personne.
- Il est important d'indiquer clairement votre rôle et vos responsabilités. Il semblerait qu'une grande confusion règne sur le terme sous-traitant, ce n'est pas parce que vous êtes un sous-traitant que vous êtes également sous-traitant de traitement de données personnelles. Il faut absolument clarifier cela dans vos contrats, pour ne pas que pèse sur votre structure des responsabilités démesurées.

-> Vérifier et ajuster votre protection juridique

Quelle est la protection juridique couverte par votre assurance ? Contrôlez les plafonds couverts afin de les ajuster, si nécessaire, au regard des nouvelles sanctions encourues en cas de violation des obligations découlant du RGPD (voir Fiche 1).
Contactez au plus vite votre courtier ou votre assureur afin de mettre en place une protection adaptée à vos besoins et à vos moyens. Nouveauté RGPD : Attention aux actions de groupe !

- Il faut impérativement vérifier avec votre assurance que votre couverture prenne bien en charge les dommages et intérêts découlant d'une action de groupe.
- Le dédommagement de groupe de personnes en matière de données personnelles est une nouveauté apportée par le RGPD, au regard du montant des amendes administratives, il est fort possible que le montant des dédommagements soient très élevés.

-> Mettre en place des procédures internes

Pour prévenir le risque de contentieux et s'assurer que les équipes sont préparées, il est important de former les équipes et de mettre en oeuvre des processus adaptés, propres à chaque organisation.
Pour ce faire, il est important de revoir les documents suivants :

- Charte informatique
- Code de bonne conduite
- Les contrats de travail
- L'affichage dans l'entreprise, etc ...

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

-> Provisionner en fonction des risques

Pour certaines entreprises qui traitent des données personnelles dites sensibles, ou dont le coeur de métier est le traitement à grande échelle de données personnelles, il est conseillé de calculer les risques encourus et de provisionner en conséquence.

-> Respirer !

Dans une allocution en date du 18 février 2018, la présidente de la CNIL, Isabelle Falque-Pierrotin, est consciente que toutes les entreprises françaises ne pourront pas mettre en oeuvre le règlement sur la protection des données au 25 mai 2018. Dans une interview accordée aux Échos, elle explique que la CNIL sera néanmoins exigeante concernant les obligations du RGPD qui existaient déjà, comme l'obligation de transparence sur la finalité de la collecte des données. Elle sera en revanche plus souple sur les éléments nouveaux, comme le droit à la portabilité. Par exemple, la CNIL donnera trois ans aux entreprises pour « apprivoiser le nouvel outil des études d'impact ».

Il ne faut donc pas se décourager ! Oui, la mise en conformité peut sembler un processus complexe et long, mais les Autorités de contrôles européennes n'ont pas à l'esprit la sanction administrative à tout prix et sont plutôt dans une optique d'assistance des entreprises à mettre en oeuvre les bonnes pratiques.

La CNIL et les autres autorités de contrôle européennes prendront en compte les efforts fournis avant de sanctionner.

FICHE #11

CONTRÔLE CNIL

-> Qui effectue le contrôle ?

Les agents de la CNIL et/ou les agents d'autres autorités européennes de protection des données.

Ils peuvent être assistés par des experts désignés par l'autorité dont ils dépendent.

La CNIL a le pouvoir d'effectuer des contrôles auprès de l'ensemble des Responsables de traitement. Ces contrôles peuvent se dérouler **sur place, sur audition par convocation ou en ligne, dans le cadre de réclamations, pétitions et plaintes relatives à la mise en oeuvre des traitements de données personnelles**. Le RGPD prévoit que des actions conjointes de plusieurs autorités européennes de protection des données sont possibles.

-> Contexte et principes de base

- Les **contrôles en ligne** sont effectués sans que le Responsable du traitement ne soit prévenu et se limitent à la consultation des données librement accessibles en ligne.
- **Lorsque l'action se déroule sur audition**, la CNIL a l'obligation d'en avertir le Responsable du traitement au moins 8 jours avant la date du contrôle, par lettre remise contre signature ou remise en main propre contre récépissé ou acte d'huissier (D. 2005-1309, art. 66).
- **Dans le cas des contrôles sur place**, c'est la CNIL qui décide de l'opportunité d'informer ou non le Responsable du traitement, au plus tard il en est informé au début du contrôle sur place. (D. 2005-1309, art. 62). Par ailleurs, la CNIL peut demander au Responsable du traitement de préparer tous documents de nature à faciliter le déroulement du contrôle.

-> Peut-on s'opposer au contrôle ?

Le responsable des locaux est informé lors de la visite des agents CNIL qu'il peut exercer son droit d'opposition. Dans ce cas, les motifs de son opposition sont portés au procès-verbal dressé par les agents de la CNIL.

Les opérations de contrôle ne peuvent alors intervenir qu'après autorisation du juge des libertés et de la détention compétente, qui dispose de 48h pour accepter ou refuser la demande (article 44, II de la loi du 6 janvier 1978). **Une fois cette ordonnance rendue, il est impossible de s'opposer au contrôle.**

Si la CNIL suspecte un risque de destruction ou de dissimulation de documents, ou lorsque la gravité des faits le nécessite, le contrôle peut intervenir sans information du Responsable des locaux et sur autorisation préalable du juge des libertés compétent, le Responsable des locaux n'est alors plus en mesure de s'opposer au contrôle.

NOTE : **LE SECRET PROFESSIONNEL**

Il est possible de s'opposer au contrôle sur le fondement du secret professionnel : dans ce cas il faut indiquer les dispositions réglementaires s'y rapportant et préciser la nature des données couvertes par le secret professionnel. Tous ces éléments doivent être inscrits au procès-verbal.
(Exemples non exhaustifs : secret médical, secret bancaire, secret professionnel de l'avocat, du notaire, du banquier ou encore du facteur...)

Toute personne qui s'oppose à la visite, refuse de communiquer les documents demandés ou fournis de fausses informations, peut être poursuivie pour délit d'entrave : un an d'emprisonnement et 15 000 euros d'amende.

-> Déroulement du contrôle sur place

Les contrôles sur place peuvent avoir lieu entre 6 heures et 21 heures, les membres et agents habilités de la CNIL ont accès à tous les locaux et installations servant à la mise en oeuvre du traitement des données personnelles. Deux témoins non soumis à l'autorité de la CNIL peuvent être désignés.

Que faire ?

Lorsque les agents se présentent :

- Alerter immédiatement la Direction et le département juridique
- Noter l'identité des personnes qui se présentent pour le contrôle
- Faire patienter les agents dans une pièce ne comportant aucun ordinateur ou appareil électronique ; cette pièce doit pouvoir être fermée par une porte.
- Leur proposer un café dans l'attente.

Pendant le contrôle :

- Prendre des notes des faits et photocopier tous les documents saisis
- Accompagner les agents dans l'entreprise dans tous leurs déplacements
- Vérifier que le cadre légal est respecté ((information, conditions horaires du contrôle, habilitation des agents de
- contrôle, établissement du procès-verbal, etc.).

En toute circonstance :
Garder son calme, rester courtois

-> Pouvoir d'enquête

Dans le cadre d'une mission de contrôle, les agents habilités sont autorisés à recueillir toutes les informations techniques,
juridiques permettant d'apprécier les conditions du traitement des données personnelles, ils peuvent notamment (Loi de 1978, art. 44 III-al. 1) :

- Obtenir communication et copie de tout document, quel qu'en soit le support, leur permettant d'apprécier les conditions dans lesquelles des traitements automatisés de données à caractère personnel, notamment en termes de sécurité, d'information des personnes, de modalités de collecte des données, sont mis en oeuvre.
  > (Exemple : Contrats (location de fichiers, sous-traitance informatique, etc.), Formulaires, Dossiers papier, Bases de données informatiques, etc.)
- Accéder aux programmes informatiques et aux données et, en demander la transcription pour les besoins du contrôle
- Recueillir tout renseignement technique ou juridique ou toute justification utile à l'accomplissement de leur mission
- Interroger des personnes

Il est recommandé de :

- Donner des réponses brèves, sans avis personnels
- Rester dans son domaine de compétence et ne répondre que lorsque l'on est à mesure de le faire

Les agents ne peuvent saisir :
- les correspondances entre la société et ses avocats

-> Etablissement du procès-verbal

Le procès-verbal est un document qui est établi selon le respect du contradictoire entre les agents de la CNIL et le responsable des locaux, il est donc possible d'émettre des réserves ou des commentaires.

Il relate :

- L'objet de la mission de contrôle
- La nature du contrôle
- Le jour et l'heure des opérations de contrôle
- Le lieu de vérifications ou des contrôles effectués
- Les membres présents lors du contrôle
- Les personnes rencontrées, ainsi que les déclarations spontanées
- Les contrôles effectués
- Les éventuelles difficultés rencontrées
- Le cas échéant, l'opposition au contrôle du responsable des locaux sur le fondement du secret professionnel, les dispositions législatives ou réglementaires sur lesquelles il s'appuie, ainsi que la nature des données qu'il estime couvertes par le secret professionnel.
- L'inventaire des pièces et documents qui ont été saisis

Il est signé par :

- les agents habilités par la CNIL
- le responsable des lieux ou son représentant
- les témoins désignés s'il y en a

-> Et ensuite ?

- Après le contrôle et l'examen des documents recueillis, si la CNIL estime que le dossier ne nécessite pas d'observation particulière, un courrier est adressé par le Président de la CNIL au responsable de traitement.
- Elle peut également prononcer un avertissement, voire mettre en demeure l'entreprise de se mettre en conformité.
- En cas de manquement particulièrement grave, le dossier peut être transmis à la formation contentieuse de la CNIL qui pourra imposer à l'entreprise une amende administrative.
  Note : Le RGPD dispose que cette amende administrative doit prendre en compte la nature, la gravité et la durée de la violation, mais aussi son caractère délibéré. Toute mesure prise pour atténuer le dommage subi par les personnes concernées sera également prise en compte, d'où l'importance de réfléchir à sa mise en conformité et à amorcer les modifications nécessaires.

Attention : en cas de sanction administrative par la CNIL, et conformément à l'article 40 du code de procédure pénale, la CNIL a le devoir d'informer sans délai le Procureur de la République des infractions dont elle a eu connaissance suite au contrôle. Le Parquet pourra décider de l'opportunité ou non d'engager des poursuites à l'encontre du Responsable des traitements.

-> Conseils

1. Anticiper un contrôle et cibler les principaux manquements au RGPD pour les rectifier en priorité.
2. Mettre en place une procédure interne applicable en cas de contrôle de la CNIL, afin que ce dernier se déroule dans les meilleures conditions possibles pour tous
3. Former et informer son personnel à réagir en cas de contrôle.

FICHE #12

DOCUMENTATION RH

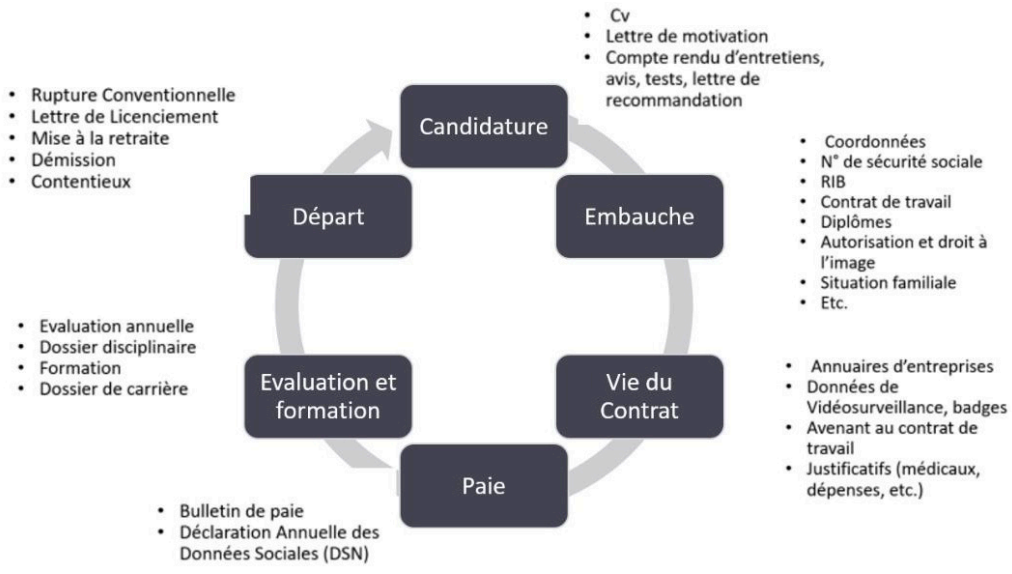
-> Pourquoi les RH sont un des secteurs dans l'entreprise le plus impacté par le RGPD ?

1

- **Concerne un large panel de personnes: Candidats à un poste ou à un stage, employés, apprentis, étudiants en contrat de professionnalisation, etc.**

2

- **Durant tout le cycle de vie du salarié, les RH collectent et traitent des données personnelles, voire sensibles.**



COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

3

- **Les sanctions administratives, civiles et pénales pourront découler du RGPD, mais le salarié pourra également intenter des actions directes à l'encontre de son employeur. (seul ou en groupe)**

-> Comment anticiper et réfléchir à sa conformité RH/RGPD

Faire un état des lieux des procédures internes

CANDIDATURE

- Les contrats vous liant à des organismes de recrutement externe sont-ils conformes aux attendus réglementaires ?
- Comment assurez-vous la suppression des données personnelles des candidats non retenus ?
- Les compte-rendu des entretiens d'embauche sont-ils bien mis à la disposition des candidats en cas de demande ?

EMBAUCHE

- Disposez-vous d'un registre des données à caractère personnel et sensible collectées et des traitements qui y sont apportés ?
- Informez-vous les employés de leurs droits (accès aux données, rectification, suppressions) lors de la collecte des données ? Du but de la collecte des données ? De la personne à contacter en cas de volonté de suppression ou de modification de celle-ci ?

VIE DU CONTRAT

- La sécurité et la confidentialité des données des salariés sont-elles garanties par des moyens physiques et informatiques appropriés ?
- Les habilitations d'accès aux données personnelles sont-ils contrôlés ?
- Avez-vous la possibilité de mettre en œuvre une demande d'accès, de rectification ou de suppression de données personnelles ?

EVALUATION FORMATION

- Vos collaborateurs sont-ils formés et sensibilisés à la protection des données personnelles ? À quelle fréquence ? Gardez-vous les preuves des suivis de formation ?
- Comment gérez-vous les entretiens annuels d'évaluation ? Le salarié évalué est-il informé du traitement, du but et du sort des données personnelles collectées à cet effet ?

PAIE

- Le processus de distribution des fiches de paie respecte-t-il les droits de vos salariés en matière de données personnelles, ces informations restent-elles confidentielles tout du long ?

DÉPART

- Les données des anciens employés sont-elles bien supprimées dans le respect de la durée légale de rétention ?
- Cette suppression est-elle effective pour les données numériques et sous format papier ?

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

-> Identifier les données personnelles traitées

Afin de construire un dispositif de protection des données exhaustif, cohérent et pérenne, la première action sera d'identifier son périmètre d'application en réalisant une cartographie des données collectées et traitées.

Cette analyse nécessite une collaboration entre différents départements, afin d'identifier l'intégralité des données personnelles recueillies tout au long du cycle de vie du salarié et de mettre en oeuvre les chantiers appropriés.

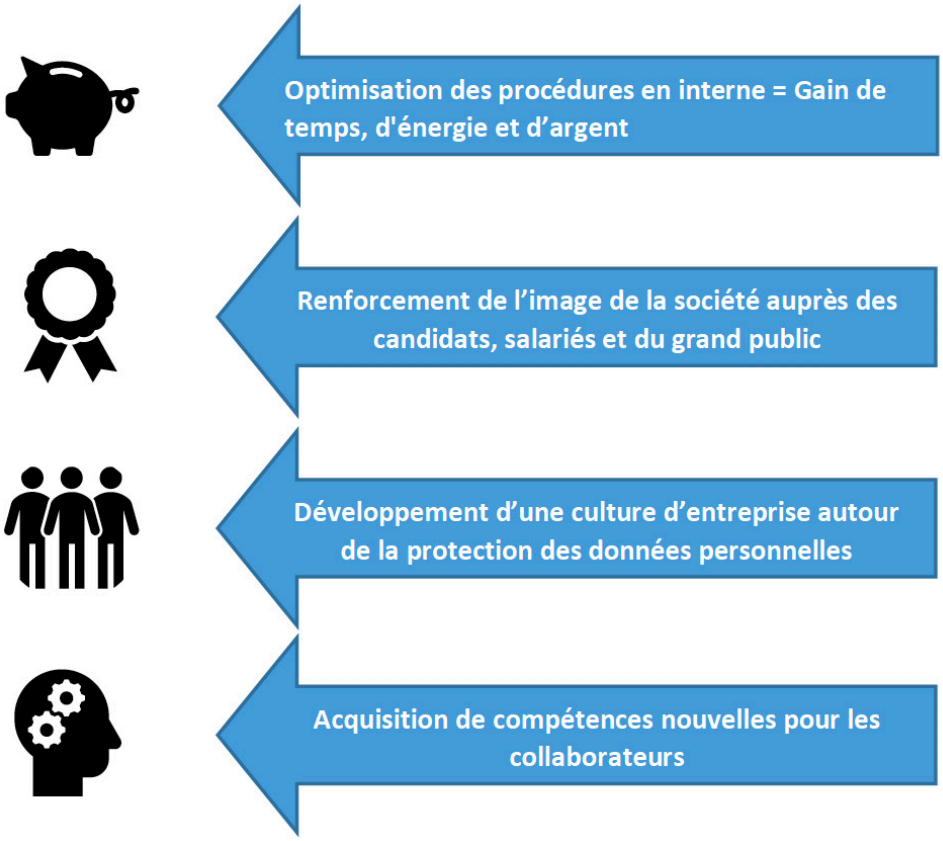
Service RH / Juridique → **Service Informatique** → **Selon la structure le DPO**

Mettre en place un chantier de mise en conformité (générique)

1 - Missionner une personne au sein de l'entreprise (de préférence RH)	Identifier au sein de la société la personne référente pour la mise en conformité des processus RH, cette personne travaillera avec le responsable informatique, et le DPO s'il y en a un, ainsi qu'avec le service juridique.	• Prévoir une formation adaptée avec un conseil juridique spécialisé. • Supervision des chantiers de mise en conformité
2 - Documentation	Procéder à la cartographie des données personnelles collectées, ainsi que les traitements, transferts, durée et méthode de stockage associées pour déterminer le dispositif de protection à mettre en place	• Tenue du Registre des données personnelles et informations associées. • Mise en œuvre d'une politique générale RH à la protection des données personnelles.
3 - Information des candidats et employés	Prévoir une revue globale des documents contractuels liant la société avec ses employés et candidats.	• Avenants au contrat de travail, modification du Règlement Intérieur (consultation des Délégués du Personnel (CSE)), modification des mails et documents suite à une embauche ou une candidature.
4 - Sécurité et gestion des habilitations	Mettre en œuvre les moyens de sécurité physique et logique adaptés, en veillant à définir un dispositif de gestions des accès aux données personnelles.	• Procédures documentées de sécurité des données personnelles. • Tenue d'un registre des habilitations.
5 - Suppression des données	Pour chaque type de données personnelles identifiées, définir les durées de conservation nécessaire, ainsi que les modalités d'archives.	• Procédures documentées de conservation, suppression et archivage.
6 - Formation des collaborateurs	Mise en place d'un plan de formation avec le DPO, ou le Service juridique et RSSI s'il n'y a pas de DPO.	• Plan et support de formation. • Registre de suivi des formations suivies par employé.

-> Le RGPD, une opportunité pour l'entreprise

Adapter les ressources humaines de son entreprise au RGPD a de multiples avantages :



-> En bref

- Toutes les entreprises avec au moins un salarié sur le territoire de l'UE sont concernées ;
- Se mettre en conformité permettra d'éviter un risque indemnitaire supplémentaire devant les juridictions prud'homales en cas de contentieux ;
- Les chantiers à mettre en oeuvre pour les RH peuvent être facilement effectués avant l'entrée en vigueur du Règlement.

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

FICHE #13

PLAN DE MISE EN CONFORMITE

-> Exemple de plan de transformation pour mise en conformité au RGPD

Pour chaque semestre, nous recommandons la constitution d'actions planifiée au travers des fiches de synthèse.
Il est important en amont du projet d'identifier les acteurs clés porteurs de cette démarche (DPO/ RSSI) et de les faire accompagner par le responsable du traitement dans des comités de pilotages mensuels.
Lorsque le traitement des données personnelles impacte les métiers, il est indispensable d'inviter à participer les collaborateurs en charge du développement, exécution ou modification des traitements.

Étape #1 Identifier les zones de responsabilité et de risque

- Découvrir les nouveautés et contraintes du Règlement Européen
- Identifier le responsable du traitement
- Identifier les traitements & flux associés (internes, sous-traitants > cartographie des acteurs impliqués)
- Sommes-nous concernés par les données personnelles ?
- Sensibilisation des directions et formations des équipes
- Lancer une démarche qualité en vue de la mise en conformité RGPD
- Identifier et localiser les chantiers de mise en conformité au sein des services (RACI)
- Identifier la ressource interne et les prestataires (juridiques & techniques)
- Cartographier le SI (applications, serveurs, sous-traitants)
- Identification des données personnelles (et données sensibles) + localisation applicative (géographique)
- Informer les personnes concernées > création d'une fiche réflexe d'information (interne/externe) 72H

Étape #2 Prioriser sur sa cartographie de traitements avec analyse d'impact

- Analyse d'impact (données particulières ou algorithme > maitrise des risques ou doutes sur les risques)
- Analyses d'impact vont surtout concerner les collectivités et les entreprises opérant des traitements de données complexes (données particulières ou caméras par exemple, données de santé).

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

COMMISSION LEGAL'IN TECH

THEMATIQUE #RGPD

- Suite à cartographie des traitements et du système d'information conduire l'analyse d'impact sur les traitements
  - > Minimisation de la collecte --> impact
  - > Évaluation du caractère sensible et du caractère nécessaire de la donnée
- Clauses types à insérer dans les documents contractuels
- Analyse de risques préalable au plan d'action

Étape #3 Privacy by design

=> Voir La fiche 7 pour plus de détail

- Suite à l'analyse d'impact préconisations vis-à- à vis des jeux de données et applications
- Dans le cas d'applications non conformes > relation à l'éditeur & solutions proposées
- Dans le cas de la conformité, demander un certificat à l'éditeur
- En cas de développements internes à l'entreprise > Privacy by design
- Mesurer les écarts vis-à-vis de la cartographie, passer au plan d'action avec des livrables

Étape #4 Mise en place d'une gouvernance de données personnelles

- Réfléchir à une stratégie de gouvernance de données personnelle, déterminer le rôle de chacun et réfléchir à la nomination du DPO en interne ou en tant que prestataire externe.
  Il existe plusieurs stratégies de gouvernance, qui doit s'adapter aux moyens humains et financiers dont dispose la structure, le conseil de personnes spécialisée dans ce domaine est recommandé pour optimiser ce processus.
- Création de la fiche réflexe de désignation du DPO et d'une infographie avec cas concrets «parlants»
- Création de la fiche de poste DPO (voir la Fiche 16)
- Mise en place de l'Affichage légal (voir la Fiche 9)
- Mise en place d'un processus de notification des violations
- Sélection des outils techniques, inventaire, contrôle et suivi des procédures mises en place.

Étape #5 Mesures organisationnelles

- Formation avancée ressources humaine
- Mise en place des délégations de pouvoir
- Préparation et rédaction des registres des traitements (responsable, finalités, personnes concernées et données traitées, destinataires, transfert, durées, mesures de sécurité techniques et organisationnelles)
- Recueil du consentement des salariés et impacts sur les documents RH (contrat de travail, charte informatique, etc.)
- Mise en place de l'information des personnes concernées
- Mise en oeuvre technique, en mettant au point des procédures automatiques pour optimiser les actions.

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

Étape #6 Mesures complémentaires

- Programmer le plan de suivi et de contrôle
- Valoriser le portefeuille de données personnelles
- Optimiser les services de remonter d'information
- Réfléchir à l'opportunité d'une certification

Chantiers récurrents (tous les 6 à 12 mois)

- Pré-audit (Analyse d'écart)
- Mise en conformité
- Mise à jour des PIA et des registres de traitement
- Audit de conformité
- Audit sur les mesures de sécurité pour vérifier leur adéquation au RGPD
- Mettre en oeuvre les actions identifiées lors des audits et des analyses de risque (PIA)

FICHE #14

ASSURANCES

-> ASSURER LE RISQUE ?

Afin d'anticiper un sinistre et ses conséquences directes ou indirectes, il convient d'évaluer précisément les différents niveaux de couvertures des contrats d'assurance souscrits.

A ce jour les différentes compagnies d'assurance ne proposent pas encore un niveau de contrat adaptés aux traitements de l'ensemble des entreprises. Il est donc important d'échanger avec vos interlocuteurs pour bien déterminer les niveaux de protection à mettre en oeuvre face aux risques encourus.

-> Quel contrat souscrire pour se garantir des atteintes aux données à caractère personnel ?

Sont présentés les différents types de couvertures visant à couvrir votre responsabilité en cas d'atteinte aux données à caractère personnel qui sont traitées par votre système d'information[1].

	Types de couvertures	RCMS	RC/RC pro	TRI	Cyber
Responsabilité Civile	RC pour manquement à l'obligation de notification				
	RC liée à la sécurité des systèmes d'information				
	RC pour la publication ou transmission de contenu média sur les sites internet de l'assuré ou sur les médias sociaux (diffamation, atteinte à l'image d'une personne concernée, plagiat ..)				
	Frais d'enquête, d'assistance et de représentation devant des autorités administratives (CNIL)				
	Sanctions pécuniaires assurables prononcées par une autorité administrative				

Légende :

- La garantie est proposée
- La garantie peut exister
- La garantie n'est pas proposée

TRI : Tout Risque Informatique
RCMS : Responsabilité Civile des Mandataires Sociaux
RC : Responsabilité Civile

[1] *Inspiré des débats « Garanties des frais et dommages liées aux risques Cyber », Forum des Compétences, janvier 2018*

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

-> Évaluation du niveau de couverture des contrats

Toutes les compagnies assurances n'ayant pas intégré les enjeux du RGPD, il est important de bien définir son niveau de couverture face aux menaces et à leur vraisemblance.

Ci-dessous les risques couverts par 15 types de contrats d'assurance proposés par différentes compagnies leaders du secteur. Tout Risque Informatique, Responsabilité Civile des Mandataires Sociaux, Responsabilité Civile, Fraude, et Cyber.

Chaque point est à vérifier vis-à-vis de votre contexte et de vos contrats existants, n'hésitez pas à questionner un professionnel de l'assurance et du conseil pour chaque point afin d'en vérifier la couverture et le niveau de dédommagement en cas de sinistre.

Généralement inclus dans les contrats proposés sur le marché
Inclus dans certains contrats sur le marché
Exclu par les contrats proposés sur le marché

-> Etendue de la garantie d'assurance

Cause du sinistre
Erreur humaine
Omission / Négligence
Acte de malveillance informatique
Virus informatique
Défaillance électrique
Défaillance télécommunication
Défaillance du prestataire infogérant
Défaillance du prestataire Plan de Continuation d'Activité
Dysfonctionnement installation infrastructure
Absence des mises à jour des correctifs de sécurité publiés par l'éditeur
Absence d'antivirus
Absence de pare-feu
Fausse déclaration de risque

COMMISSION LEGAL'IN TECH

THEMATIQUE #RGPD

Degré de réalité de la réclamation introduite à votre encontre (preuve à l'appui)

- La réclamation introduite à votre encontre est avérée et fera certainement l'objet d'une condamnation prononcée par une autorité judiciaire, administrative ou fera l'objet d'une sentence arbitrale
- La réclamation introduite à votre encontre est alléguée et ne débouchera pas certainement sur une condamnation prononcée par une autorité judiciaire, administrative ou fera l'objet d'une sentence arbitrale

Personne concernée par l'atteinte aux données personnelles

- Client
- Prospect
- Salarié
- Stagiaire
- Candidat à l'embauche
- Auto-entrepreneur
- Mandataire social

Préjudice garanti suite à l'atteinte à un droit d'une personne concernée

- Atteinte à la vie privée au sens de l'article 9 du Code civil
- Diffamation (atteinte à la réputation d'un tiers)
- Atteinte à la confidentialité des données à caractère personnel
- Atteinte au droit à l'image d'une personne concernée
- Préjudice moral de la personne concernée
- Préjudice corporel (suicide ou tentative de suicide en lien avec la divulgation de données à caractère personnel de la personne concernée)

Frais liés au préjudice pris en charge

- Notification aux personnes concernées de l'incident
- Les dommages-intérêts
- Les indemnités transactionnelles
- Les dépens et frais irrépétibles de procédure (article 700 du Code de procédure civile)

Les dépens les frais irrépétibles de l'instance, les indemnités transactionnelles, ou tout autre montant garanti au titre du présent contrat, que l'assuré est individuellement ou solidairement tenu de payer en raison d'un jugement, d'une sentence arbitrale ou d'une transaction passée avec le consentement écrit préalable de l'assureur
Sinistre du fait de votre sous-traitant
Les dommages-intérêts punitifs, exemplaires ou aggravés et la portion multiple des dommages-intérêts multipliés par l'effet de la loi (multiplied portion of multiplied damages)
Les salaires ou rémunérations de tout assuré
Les sommes dues par l'assuré en vertu d'une obligation contractuelle
Les remises, avoir, rabais, réduction de prix bons, primes ou toute autre mesure incitative contractuelle ou non, les promotions ou avantages offerts aux clients de l'assuré.

-> Termes spécifiques data management

Par principe, la collecte et le traitement de ces données sont interdits au sein des organisations dont les métiers ne l'exigent pas.
Cependant, dans la mesure où la finalité du traitement l'exige, ne sont pas soumis à cette interdiction :

> les traitements pour lesquels la personne concernée a donné son consentement exprès,
> les traitements justifiés par un intérêt public après autorisation de la CNIL ou décret en Conseil d'État.

Ces actions font appel à des éléments stratégiques et techniques « plus affutés », n'hésitez pas à demander conseil.

Les mentions inscrites sur le présent document n'ont pas de valeur contractuelle. Elles sont mentionnées à titre purement informatif et ne peuvent engager la responsabilité de l'auteur du document.

FICHE #15

5 POINTS DE CONTROLE

1. RGPD
Suis-je concerné?

- ❑ Est-ce que ma structure effectue des traitements de données personnelles?
- ❑ Suis-je un responsable de traitement? Un sous-traitant?
- ❑ Un co-responsable?
- ❑ Le Règlement européen m'est t-il applicable?

2.DOCUMENTATION ET ANALYSE D'IMPACT
Les bonnes pratiques

- ❑ Analyse du Traitement : y a t-il des données « sensibles »? Des traitements particuliers? Des traitements soumis à une analyse d'impact?
- ❑ Dois-je mettre en place un registre (obligatoire en général, et recommandé dans tous les cas)?
- ❑ Quelles mesures de sécurité mettre en place?
- ❑ Faut-il désigner un DPO? En interne? Externalisé?
- ❑ Mise en place de mécanisme et procédure interne pour démontrer le respect des règles relative à la protection des données (principe d'accountability).

3. COLLECTE
Les grands principes

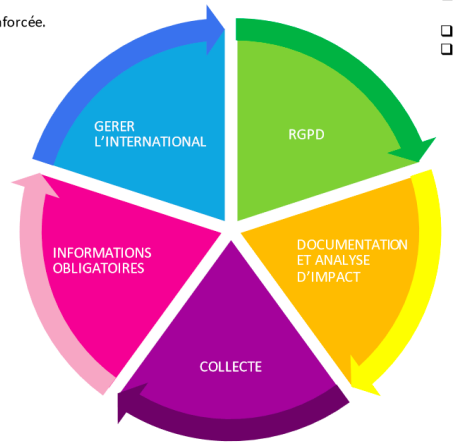
- ❑ Application du principe de minimisation des données
- ❑ Application du principe de limitation des finalités
- ❑ Application des principes de *Privacy by design* et *Privacy by default*
- ❑ Limiter la durée de conservation à ce qui est strictement nécessaire
- ❑ Application du principe selon laquelle la collecte des données et loyale ET licite

4.INFORMATIONS OBLIGATOIRES
Quelles sont les informations à communiquer obligatoirement? Par quel moyen?

- ❑ Identifier le responsable du traitement, la finalité du traitement et le fondement, les droits des personnes concernées, la durée de conservation, etc.
- ❑ Determiner en interne la modalité de communication des informations

5. GERER L'INTERNATIONAL

- ❑ Le droit à une information renforcée des personnes concernées.
- ❑ Mise en place de contrat afin d'encadrer les flux envoyés en dehors de l'UE.
- ❑ Mise en place de procédure interne renforcée.



COMMISSION LEGAL'IN TECH – FICHE #15 5 POINTS DE CONTROLE

COMMISSION
LEGAL'IN TECH

THEMATIQUE
#RGPD

FICHE #16

LE DATA PROTECTION OFFICER

-> Une mesure majeure du RGPD : l'obligation de désigner un DPO

Sans préjudice d'autres cas qui seraient prévus par les États membres, le **responsable de traitements** et le sous-traitant devront **obligatoirement** désigner un DPO lorsque :

- leurs activités de base les conduisent (du fait de la nature, portée et/ou finalité de ces activités) à effectuer un suivi régulier et systématique des personnes à grande échelle ;
- leurs activités de base les amènent à traiter à grande échelle des données sensibles ou qui ont trait à des condamnations et infractions pénales (pour mémoire, sont considérées comme des données sensibles, notamment, les données génétiques, biométriques, ou afférentes à la santé, à la religion, aux opinions politiques ou à l'appartenance syndicale).

« L'activité de base » d'une entreprise est considérée comme l'activité clé lui permettant de réaliser ses objectifs, ou qui est inextricablement liée au traitement.

Si le responsable de traitements remplit les critères de désignation obligatoire, son sous-traitant n'est pas nécessairement tenu lui-même de nommer un DPO, et inversement.

A NOTER : il est possible de désigner un DPO en dehors des cas où le règlement le rend obligatoire. Il aura alors une mission et des obligations identiques.

-> Les conditions d'un traitement à grande échelle

Il est recommandé notamment de prendre en considération les facteurs suivants pour déterminer si le traitement est effectué « à grande échelle » :

- le nombre de personnes concernées ;
- le volume de données et/ou le spectre des catégories de données ;
- la durée ou la permanence de l'activité de traitement ;
- l'étendue géographique de l'activité de traitement.

À titre d'exemples, sont concernés par la nomination d'un DPO les traitements de données (trafic, contenu, localisation) par téléphone, par un fournisseur de services internet ou encore ceux réalisés à titre habituel par une banque ou une société d'assurance.

En revanche, ne constitue pas un traitement à grande échelle, le traitement des données d'un patient par un médecin particulier ou relatif aux condamnations et infractions pénales par un avocat.

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

-> Les missions du DPO

Il lui appartient :

- de rester informé sur les nouvelles obligations,
- de sensibiliser les décideurs et les collaborateurs aux règles découlant du règlement,
- d'assister les décideurs sur les conséquences des traitements,
- d'en réaliser la cartographie,
- de concevoir des actions de sensibilisation
- et de piloter en continu la conformité.

Il intervient dans la préparation de l'analyse d'impact.

Il veille, en toute **indépendance**, au respect du Règlement Européen. Il ne doit pas être placé dans une situation de conflit d'intérêts et est soumis à une obligation de confidentialité.

Véritable chef d'orchestre, il est l'interlocuteur de référence de l'autorité de contrôle et des personnes concernées, avec qui il doit coopérer.

Il est contraint par le Règlement :

- de notifier à l'autorité de contrôle et aux personnes concernées la survenance d'une faille de sécurité qui a pu avoir lieu chez le sous-traitant ou le responsable du traitement, et ce dans un délai de 72 heures
- de vérifier que les recommandations issues de ses analyses d'impact sont suivies d'effet

Il peut être à temps plein dans l'entreprise ou à temps partagé.

A NOTER : les avocats sont autorisés à proposer des offres de DPO à temps partagé.

FICHE #17

AGENDA

-> Construire l'agenda des actions à conduire obligatoirement dans le cadre de RGPD

1. Nommer un Data Protection Officer (DPO), qui s'assurera de la conformité du traitement des données
2. Tenir un registre de traitement des données
3. Identifier le périmètre des données sensibles : le RGPD impose le chiffrement ou la pseudonymisation pour ces données
4. Garantir les droits des personnes : droit à l'oubli, droit à la portabilité des données ...
5. Rédiger une charte de bonnes pratiques pour les salariés, incluant les sanctions encourues en cas de non-respect de la loi.
6. Insérer des clauses dans les contrats de vos sous-traitants garantissant qu'ils respectent les dispositions légales quant aux données qu'ils vous confient.
7. Se préparer à la possibilité d'une fuite de données : mettre en place les procédures d'escalade qui seront activées en cas de violation de données personnelles.

A propos de Medinsoft

Medinsoft est le cluster de la région Sud qui accompagne l'innovation et la croissance des entreprises qui conçoivent et utilisent des outils du numérique.

MISSION :

Depuis plus de 15 ans, Medinsoft est au service de l'écosystème de la région Sud avec 3 missions principales :

DÉVELOPPER I ANIMER I FÉDÉRER

- Développer une image technologique forte sur la région sud pour attirer de grands donneurs d'ordres à s'installer
- Promouvoir l'industrie du numérique en région Sud et au delà pour favoriser l'émergence de projets nouveaux dans ce domaine
- Faire connaître les produits et les compétences des membres du réseau pour augmenter les ventes à l'échelon national et international
- Animer l'écosystème en créant ou en facilitant la création d'événements autour du numérique
- Assurer le développement de synergies complémentaires entre les partenaires pour favoriser la sous-traitance, l'intégration ou la complémentarité des offres des principaux créateurs de logiciels
- Positionner MedInSoft comme un interlocuteur majeur vis à vis des institutionnels politique et économique de la région
- Favoriser l'emploi et le développement social sur le bassin méditerranéen
- Lobbying
- Levées de fonds

Plus que jamais, le logiciel étant au coeur du processus d'innovation quelles que soient les filières, Medinsoft accélère encore et catalyse les énergies.

Rejoindre Medinsoft, c'est l'assurance de se rapprocher d'un cluster d'entrepreneurs dynamique, centré sur l'innovation et doté d'un réseau régional puissant.

No bullshit. Only actions !

Pour nous rejoindre ou pour toute question, une seule adresse !

communication@medinsoft.com

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

Toutes les commissions Medinsoft

- COMMISSION EMPLOI FORMATION
- COMMISSION DIGITAL MKT & SALES
- COMMISSION FINANCEMENT
- COMMISSION LOGICIEL LIBRE
- COMMISSION LEGAL'IN TECH
- COMMISSION INDUSTRIE 4.0
- COMMISSION SMART CITY
- COMMISSION BLOCKCHAIN
- COMMISSION TOURISME
- COMMISSION eSANTE
- COMMISSION eSPORT

Programme ambassadeur

MEDINSOFT PROGRAMME AMBASSADEUR

Depuis début 2019 le programme Ambassadeur vient en support des adhésions afin d'ouvrir au plus grand nombre cette nouvelle dynamique créatrice impulsée par la transformation numérique, pour toutes les entreprises et quels que soient leurs secteur d'activités.

Les Ambassadeurs :

Issus de la Société Civile, les M-Ambassadeurs sont des geeks de cœur ou d'adoption, dirigeants d'entreprises, universitaires, scientifiques, personnalités du monde sportif, culturel, artistique, ou du monde des médias...

Ils résident ou sont originaires de notre territoire métropolitain, en France, comme partout dans le monde. Profondément attachés au territoire, ils souhaitent s'engager pour en faire rayonner l'économie et promouvoir ses atouts réels et son formidable potentiel.

Devenez ambassadeur Medinsoft et profitez de nos contenus (newsletter, invitations à nos événements...) !

Pour cela, envoyez simplement votre mail à communication@medinsoft.com.

MEDINSOFT DIGITAL TRANSFORMATION CLUSTER

Join us !

www.medinsoft.com

MEDINSOFT
DIGITAL TRANSFORMATION CLUSTER

RÉGION SUD PROVENCE ALPES CÔTE D'AZUR
EUROMÉDITERRANÉE Établissement Public d'Aménagement
DÉPARTEMENT BOUCHES DU RHÔNE
AIX EN PROVENCE LA VILLE
AIX MARSEILLE PROVENCE
VILLE DE MARSEILLE www.marseille.fr