COMPLIANCE GDPR

SIMPLEMENT

FACILEMENT

CONCRETEMENT

MANUEL DE SOLUTIONS PRATIQUES

Lawint
Cabinet d'avocats

68, rue du Faubourg Saint Honoré – 75008 Paris

Cabinet d'Avocats - SELARL au capital de 5.000€ - RCS Paris 848 321 816
E-mail info@lawint.com www.lawint.com

POURQUOI ETRE CONFORME AU GDPR ?

- Parce que c'est une loi, une obligation ;
- Parce que ne pas le faire, c'est risquer les amendes de la CNIL et le *bad buzz ;*

Mais aussi

- Parce que les grands groupes refusent désormais de travailler avec les sociétés qui ne peuvent pas démontrer qu'elles respectent le GDPR ;
- Parce que les consommateurs comprennent ce que c'est et que leur confiance en sera dépendante dans le futur ;
- Parce que cela permet à la société de réfléchir sur la data, sa place dans la stratégie et la valorisation financière qu'elle représente.

POURQUOI LAWINT PEUT VOUS AIDER ?

- Un des premiers Cabinets d'avocats dans le domaine du droit de la data en France ;
- Plus de 15 ans d'expérience dans le domaine du droit de la data ;
- Une expertise reconnue et éprouvée dans le domaine du droit informatique, propriété intellectuelle et data ainsi que dans le domaine *corporate* (levées de fonds, cession) ;
- Une équipe composée d'avocats – anciens informaticiens qui comprennent la technique et les technologies des bases de données et des structurations de données ;
- Des dizaines d'audits GDPR auprès des plus grands noms comme de PME ;

Et aussi

- Un **OUTIL D'AUDIT EN LIGNE** permettant des audits flash
- Un **PLAN D'ACTIONS PRIORISEES** permettant une gestion de projet optimale
- Une **METHODOLOGIE DE REMEDIATION** efficace, pragmatique et concrète
- Des interventions au **FORFAIT** ou en régie
- La garantie de la **QUALITE** d'Avocat sur un sujet avant tout juridique

ILS NOUS FONT CONFIANCE – TRACK RECORD DATA PROTECTION / GDPR

ETAPE 1 – AUDIT - CARTOGRAPHIES

Que faire ?

- Une liste des applications (sous forme Excel) ;
- Une liste des data si possible ;
- Une liste des déclarations CNIL effectuées (pour ceux qui ont oublié : https://www.cnil.fr/fr/les-formalites-prealables-accomplies-aupres-de-la-cnil-depuis-1979) ;
- Une liste des fournisseurs et partenaires.

Pourquoi le faire ?

Même si le GDPR impose *in fine* une liste de « traitements », celle-ci sera plus aisément réalisée et contrôlée à l'aide des cartographies ci-avant visées.

Comment le faire ?

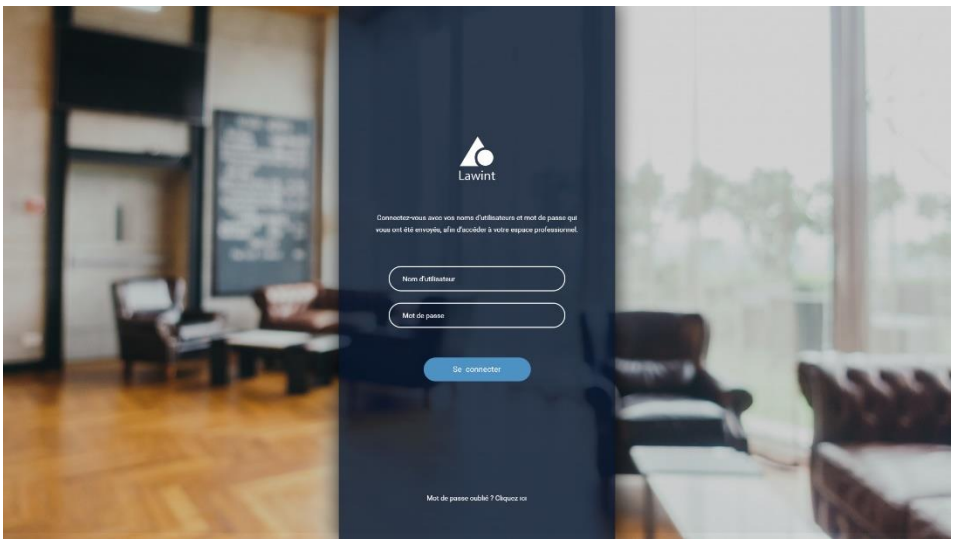
- Désigner une personne / prestataire en charge de l'audit ;
- Impliquer chaque service / direction concernée par un progiciel / application traitant des données personnelles et ce, sous la direction du chef de projet et en partenariat étroit avec la DSI ou équivalent ;
- Interviewer et collecter les documents qui permettent de réaliser les cartographies et listes.

Comment Lawint peut aider ?

Lawint propose des forfaits d'audit GDPR.

Lawint a mené des dizaines d'audits GDPR auprès de grands groupes comme de PME.

Lawint a développé une application en ligne simple, facile d'utilisation, permettant d'optimiser le temps de collecte des informations et documents.



ETAPE 1 – AUDIT - DEFINITION DES TRAITEMENTS

Que faire ?

- La liste de « traitements » de la société.

Le GDPR traite et couvre les « traitements » qui n'ont rien à voir avec les applications.

Un traitement est un ensemble d'opérations visant à traiter, pour une finalité principale, des données personnelles. Par exemple, le traitement du paiement des salaires ou le traitement du démarchage commercial des prospects.

Pourquoi le faire ?

Toute la loi est structurée autour de cette définition. Tous les documents et obligations sont axés autour de la détermination des traitements. C'est l'axe de réflexion GDPR.

Comment le faire ?

Une fois que les cartographies sont établies, il faut se demander quelles sont les principales finalités poursuivies par la société en termes de data. En d'autres termes, la société doit se demander pourquoi elle collecte tel type de données. Quelle est la finalité ?

Généralement, les finalités d'une société comprennent :
- Les finalités RH (recrutement, embauche, paye, surveillance, badges, etc…) ;
- Les finalités transversales (Finances, marketing, communication, etc…) ;
- Les finalités propres à chaque société (les finalités « business ») ;
- Les aspects IT (sécurité, hébergement des données, etc…).

Sous l'empire de la loi pré-GDPR, la CNIL avait émis des normes simplifiées qui correspondent chacune à un traitement. Par exemple, il existe une norme pour les badges qui correspond donc à un traitement.

Comment Lawint peut aider ?

Lawint propose des forfaits d'audit GDPR.

Lawint se base sur une méthodologie éprouvée qui permet de définir les traitements transversaux (RH, finance, etc…) et les traitements « business » propres à chaque entreprise, conformément au GDPR mais surtout à la pratique de la CNIL.

L'outil en ligne, développé par Lawint, permet de collecter les informations et documents permettant d'optimiser le temps de détermination des traitements.

ETAPE 1 – AUDIT - GAP ANALYSIS

Que faire ?

- Un état des lieux synthétique et précis des écarts entre l'existant et les obligations GDPR et juridiques.

Cet état des lieux doit être fait individuellement pour chaque traitement déterminé et de manière transversale pour la couche IT (sécurité / infrastructure / couche applicative / data).

Pourquoi le faire ?

Pour être en conformité et déterminer les priorités et les coûts des actions de mise en conformité. L'audit et le *gap analysis* peuvent faire apparaitre des non-conformités sur d'autres sujets (par exemple, droit du travail ou aspects commerciaux ou encore problèmes de propriété intellectuelle).

Comment le faire ?

Une étude de l'environnement juridique est absolument nécessaire. C'est la loi en général (et non pas le GDPR) qui va déterminer les types de données qu'on a le droit d'utiliser, les traitements qu'on a le droit de faire, les personnes à qui on a le droit d'envoyer.

Par exemple, c'est la réglementation applicable aux médecins qui va répondre à toutes ces questions pour ce qui concerne la mise en conformité GDPR d'un médecin.

De plus, la couche IT (qui n'est pas un traitement, mais qui doit être prise en compte de manière transversale) doit être validée au regard de la réglementation (et non la pratique).

Comment Lawint peut aider ?

En tant que Cabinet d'avocats experts depuis plus de 15 ans, Lawint formalise un rapport et est capable de déterminer, pour chaque traitement, l'environnement juridique et répondre aux questions fondamentales en termes de GDPR, à savoir :

- quelle est la base légale de la collecte de données ;
- quelles données ont le droit d'être collectées et/ou celles qui sont totalement interdites de collecte ;
- quels traitements sont autorisés et/ou ceux interdits ;
- quels sont les tiers autorisés à avoir accès aux données ;
- quelles sont les éventuelles contraintes spécifiques de sécurité ;
- quelles sont les durées de conservation à respecter.

I. SYNTHESE ... 3
II. LE CADRE DE L'AUDIT ... 7
III.1 PRESENTATION DES INTERVENANTS ... 7
III.2 OBJECTIFS POURSUIVIS ... 7
III.3 PERIMETRE DE L'ETUDE ... 7
III.4 PRINCIPAUX INTERLOCUTEURS ... 7
III.5 DEROULE DE L'AUDIT ... 7
III.6 LA METHODOLOGIE DE REDACTION DU RAPPORT ... 7
III.7 LEXIQUE ... 8
III. LES PRINCIPES GENERAUX DU GDPR ... 10
III.1 LES NOTIONS-CLE ... 10
III.2 TERRITORIALITE DU GDPR ... 11
III.3 LES DROITS DES PERSONNES CONCERNEES ... 11
III.4 LES PRINCIPALES OBLIGATIONS DES RESPONSABLES DE TRAITEMENT ... 17
III.5 RESPONSABILITE ... 29
IV. INFRASTRUCTURE & SECURITE INFORMATIQUE ... 33
IV.1 CARTOGRAPHIES ... 33
IV.2 SECURITE ... 34
IV.3 DOCUMENTATION JURIDIQUE ... 48
V. PRINCIPAUX TRAITEMENTS AUDITES ... 54
V.0 DETERMINATION DES TRAITEMENTS DU CLIENT ... 54
V.1 TRAITEMENTS COURTAGE ASSURANCE - BANQUE ... 55
V.2 TRAITEMENTS « RESSOURCES HUMAINES » ... 86
VI. PRECONISATIONS ... 95
VI.1 MISE EN CONFORMITE ET GOUVERNANCE ... 95
VI.2 MISE EN CONFORMITE ET DOCUMENTATION JURIDIQUE ... 95
VI.3 MISE EN CONFORMITE ET PROCEDURES ... 99
VI.4 MISE EN CONFORMITE ET INFORMATIQUE ... 99
VII. LIMITATIONS ... 101
ANNEXE I – LISTE DES DOCUMENTS FOURNIS / PERIMETRE DE L'AUDIT ... 102
ANNEXE 2 – PREMIERE VERSION DU REGISTRE DES TRAITEMENTS ... 103
ANNEXE 3 – MODELE DE REGISTRE DE SOUS-TRAITANT ... 104

L'analyse de la couche IT est effectuée par rapport à un ensemble de réglementations (et non pas des pratiques ou autres), notamment de sécurité informatique qui comprend des dispositions d'ordre juridique.

ETAPE 1 – AUDIT - PLAN D'ACTIONS

Que faire ?

- Un plan d'actions priorisé

Une fois que le *gap analysis* est réalisé pour chaque traitement et la couche transversale relative à l'IT, celui-ci fait apparaitre des points de non-conformité impliquant des actions.

N°	Thème	Sujet	Point d'attention	Remédiation	P°
1	Sécurité	Mot de passe	Pas de politique de changement de mot de passe	Mise en place d'une politique de changement de mot de passe	3
2	Sécurité	Gestion des habilitations	Pas de gestion des habilitations	Mise en place d'une politique des habilitations	4
3	Sécurité	Gestion des habilitations	Pas de classification des données	Mise en place d'une politique de classification des données	2
4	Sécurité	Gestion des habilitations	Pas de charte informatique	Mise en place d'une charte informatique	2
5	Sécurité	Postes de travail	Pas de politique de sécurisation des postes de travail	Mise en place politique de sécurisation des postes de travail	4
6	Sécurité	Tiers	Contrat avec le prestataire à valider	Valider le contrat avec le prestataire et le compléter le cas échéant des mentions GDPR	2
7	Sécurité	Tiers	Contrat avec le prestataire à valider	Valider le contrat avec le prestataire et le compléter le cas échéant des missions complémentaires de sécurité	2
8	Sécurité	Informatique mobile	Pas de politique de sécurisation de l'informatique mobile	Mise en place politique de sécurisation de l'informatique mobile	4

Pourquoi le faire ?

La mise en conformité peut impliquer un travail important dans certaines situations. Compte tenu du fait que la CNIL est consciente du temps que peut prendre la mise en conformité totale, celle-ci prend en compte en priorité la conformité sur les points critiques (sécurité, droits des personnes, etc…) et l'avancement sur les autres points. Il est donc conseillé de prioriser les actions.

Comment le faire ?

Chaque non-conformité doit donner lieu à une ou plusieurs action(s). Il existe 3 types d'actions :
- la mise en conformité « IT » qui va supposer des développements, de l'achat de logiciels et/ou des modifications logicielles ;
- la mise en conformité « juridique » qui va imposer la modification des textes d'information, la collecte et la preuve du consentement le cas échéant, le changement des contrats avec les sous-traitants ou partenaires en cas de traitement de données personnelles, la modification des documents RH en interne (Règlement Intérieur, etc…) et les autres documents traitant de données personnelles ;
- la mise en conformité « process » qui va obliger la rédaction et le maintien de documents (cahiers de procédure) et de procédures en interne portant, par exemple, sur la formation des salariés, la notification des failles de sécurité à la CNIL et/ou à un partenaire ou encore les procédures en cas d'exercice des droits de la part des personnes concernées.

Comment Lawint peut aider ?

Lawint peut assister sur la mise en conformité « juridique » et la mise en conformité « process ». En effet, à force d'être sollicité pour rédiger les procédures « GDPR », Lawint a désormais développé un savoir-faire en termes de rédaction de procédures. Ces cahiers sont simples, pragmatiques, faciles à utiliser.

Lawint propose la rédaction d'un Manuel GDPR qui permet à l'entreprise d'avoir tous les modèles et toutes les procédures à mettre en place.

ETAPE 2 – REMEDIATION - REGISTRE DES TRAITEMENTS / REGISTRE DU SOUS-TRAITANT

Que faire ?

Si la société a plus de 250 salariés ou si la société effectue des traitements sur des données sensibles, le GDPR impose deux types de registres :

- lorsqu'on est responsable de traitement (i.e. celui qui détermine les finalités des traitements, qui choisit ce qu'il veut faire des données), on doit avoir un registre des traitements ;
- lorsqu'on est « sous-traitant » (i.e. celui qui exécute une prestation de service en suivant les instructions du responsable de traitement pour ce qui concerne les données personnelles), on doit avoir un registre spécifique.

On peut être responsable de traitement et « sous-traitant » à la fois. Ainsi, un prestataire qui a des salariés est responsable de traitements pour les traitements RH et « sous-traitant » pour ce qui est des services rendus aux clients. Dans ce cas (assez fréquent), il faut avoir deux registres.

Pourquoi le faire ?

Le GDPR l'impose pour les sociétés de plus de 250 salariés. Toutefois, de manière générale, il est conseillé d'avoir ces registres en toutes hypothèses. La CNIL demandera ces registres. S'ils sont tenus alors que non-obligatoires, la société démontrera une grande preuve de conscience GDPR.

De plus, ces registres structurent littéralement la démarche data dans l'entreprise.

Comment le faire ?

La CNIL a publié une version draft du registre des traitements d'un responsable de traitement : https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx. Ce tableau comprend toutes les informations collectées dans le cadre des étapes 3 et 4 (d'où leur intérêt supplémentaire). Chaque onglet vise un traitement.

Le registre des sous-traitants doit comprendre :

- l'identité du sous-traitant et de chaque responsable de traitement,
- les catégories de traitements effectués pour chaque responsable de traitement,
- les éventuels transferts hors de l'Union,
- une description générale des mesures de sécurité.

Comment Lawint peut aider ?

Dans le cadre de forfaits d'audit / gap analysis, Lawint rédige le registre des traitements.

Lawint a créé un registre des traitements plus complet que celui de la CNIL qui comprend les informations requises par plusieurs autorités au sein de l'Union. De plus, Lawint a créé un registre de sous-traitant conforme au GDPR mais surtout, pragmatique et utilisable facilement par des sociétés pouvant avoir plusieurs centaines / milliers de clients.

ETAPE 2 – REMEDIATION - MENTIONS GDPR SUR LES DOCUMENTS / SITES INTERNET

Que faire ?

Le GDPR modifie quelque peu les mentions obligatoires des personnes concernées et la manière / les cas de collecte de consentement. La loi République Numérique avait déjà ajouté des mentions obligatoires à insérer.

Pourquoi le faire ?

Le code pénal prévoit des sanctions pénales en cas d'absence de fourniture de mentions obligatoires (ou mentions incomplètes) ou encore, en cas de traitement de données sans consentement alors que celui-ci était obligatoire (par exemple, données de santé).

Comment le faire ?

Les mentions doivent figurer sur tout document à destination des personnes concernées (prospects, clients, salariés, partenaires, etc…). Les mentions d'information comprennent celles visées par le GDPR (identité du responsable de traitement, nature du traitement, durée de conservation, transfert hors de l'Union, droits des personnes, contacts, droit de saisir la CNIL, etc…), mais aussi par d'autres lois (la loi pour une République Numérique impose une mention sur le sort des données après la mort par exemple).

Le consentement est indispensable dans certains cas (traitement sensible, données sensibles, etc…). Il doit être collecté de manière individualisée et spécifique (comme l'opt-in) avec une mention claire sur la finalité du traitement. La preuve de l'identité de la personne et de la collecte du consentement est à la charge du responsable de traitement.

Dans les deux cas, il est également nécessaire de déterminer les documents à modifier et/ou les documents devant désormais intégrer les mentions obligatoires.

Comment Lawint peut aider ?

Les équipes de Lawint rédigent des mentions d'information et des process de collecte de consentement depuis des années.

Lawint vérifie également que les mentions précisées comprennent certes celles imposées par le GDPR, mais également celles imposées par d'autres réglementations (par ex, les réglementations pour les courtiers en assurance).

Lawint dispose également des compétences requises pour assister lors de la mise en place des procédures propres à la preuve de la collecte du consentement (en ce compris, l'identification de la personne et de l'horodatage).

ETAPE 2 – REMEDIATION - MENTIONS GDPR CONTRACTUELLES

Que faire ?

Si les mentions sont obligatoires au moment de la collecte des données, et le cas échéant, du consentement, le GDPR et la loi en général imposent de nombreuses mentions et informations supplémentaires dans un document contractuel ou plus large.

Ces mentions peuvent comprendre plusieurs pages.

Pourquoi le faire ?

Le code pénal prévoit des sanctions pénales en cas d'absence de fourniture de mentions obligatoires (ou mentions incomplètes).

Comment le faire ?

Ce genre de documents permet de mettre toutes les mentions.

Il est important de mettre les mentions notamment propres :
- au GDPR ;
- aux aspects cookies ;
- à l'identification de la société (et numéro de TVA intracommunautaire en cas de vente à distance ou de prestations de service) ;
- au secteur d'activité propre à chaque entreprise.

Ces informations complètent les aspects purement contractuels et autres aspects juridiques (responsabilité, PI, etc…).

Comment Lawint peut aider ?

Les équipes de Lawint rédigent des mentions d'information depuis des années et disposent d'un savoir-faire spécifique en matière de contrats commerciaux notamment dans le secteur IT.

ETAPE 2 – REMEDIATION – GESTION GDPR DES ASPECTS RH

Que faire ?

- gérer l'information GDPR des salariés
- modifier en conséquence le Règlement Intérieur et/ou les contrats de travail
- organisation la délégation de pouvoirs à l'intérieur de l'entreprise
- le cas échéant, veiller à la contractualisation des missions du DPO (avenant au contrat de travail)

Pourquoi le faire ?

L'information GDPR vise toutes les personnes concernées, y compris les salariés. Cette information se formalise dans des documents à portée juridique.

Les obligations, notamment d'ordre pénal, pèsent *ab initio* sur le chef d'entreprise. Dans les entreprises d'une taille certaine, il est logique et traditionnel que le chef d'entreprise délègue la responsabilité du respect de la loi comme, par exemple, la sécurité IT visée dans le GDPR au DSI.

De la même manière, la personne désignée en tant que DPO doit voir son contrat de travail évoluer en conséquence.

Comment le faire ?

Après une analyse du positionnement RH de la société et de l'existant en termes documentaires, il convient de rédiger les documents d'information des salariés, ainsi que de l'éventuel avenant de la personne désignée DPO.

La délégation de pouvoirs doit être rédigée conformément à l'ensemble des jurisprudences qui gouvernent les règles de ces documents, notamment en veillant à ce que le délégataire ait les moyens humains, structurels, juridiques et opérationnels d'exécuter la tâche.

Comment Lawint peut aider ?

Les équipes de Lawint rédigent des mentions d'information depuis des années et disposent d'un savoir-faire spécifique y compris pour ce qui concerne les modifications des Règlements Intérieurs et contrats de travail en termes d'information.

Lawint assiste également le client dans sa définition des missions, de la fiche de poste, mais aussi sur l'analyse du contexte et de l'existant pour la délégation de pouvoirs. Lawint s'occupe évidemment de la rédaction des délégations de pouvoirs.

ETAPE 2 – REMEDIATION – GESTION DES RELATIONS AVEC LES PARTENAIRES

Que faire ?

Les tiers qui ont la qualité de « sous-traitant », de co-responsable de traitement ou de destinataire doivent voir leur contrat comprendre de nombreuses clauses.

Pourquoi le faire ?

L'article 28 du GDPR impose un contrat écrit avec de nombreuses clauses pour les sous-traitants. Le GDPR prévoit aussi des clauses spécifiques pour les contrats entre co-responsables de traitement.

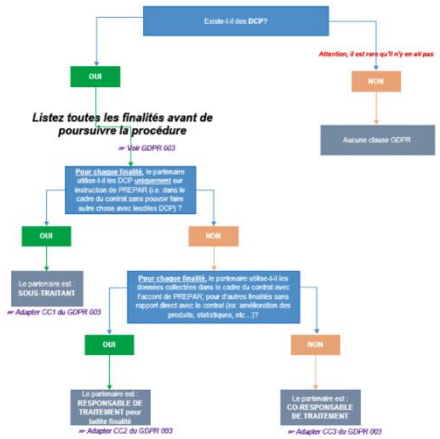
Comment le faire ?

A l'aide de la liste des fournisseurs et partenaires, il convient de déterminer pour chaque tiers la catégorie à laquelle il appartient pour chaque traitement concerné par le contrat :
- le partenaire est « sous-traitant », ou
- le partenaire est « co-responsable de traitement », ou
- le partenaire est responsable d'un traitement propre qui n'est pas sous le contrôle de l'entreprise.

La CNIL propose une clause type pour les sous-traitants (https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses), mais cette clause doit être adaptée à chaque cas de sous-traitant. A ce jour, la CNIL ne propose pas de clause pour les autres cas.

Comment Lawint peut aider ?

Lawint propose une méthodologie permettant de :
- déterminer chaque traitement induit par une relation contractuelle;
- la qualité de chaque intervenant pour chaque traitement ;
- définir le rôle et les obligations de chaque partie au contrat ;
- les clauses contractuelles à insérer dans le contrat.



Pour cela, Lawint propose :
- plusieurs types de questionnaires ;
- l'aide à l'interprétation des réponses ;
- une procédure d'assistance, avec des arbres de décision
- des clauses types contractuelles ;
- des annexes types au contrat.

Lawint propose une assistance, à distance ou sur site, pour traiter le stock de partenaires à qualifier et à contractualiser en conséquence.

Avec plus de 15 ans d'expérience de rédaction et négociation de contrat, Lawint propose évidemment son assistance à ce titre.

ETAPE 2 – REMEDIATION – MANUEL GDPR

Que faire ?

Un document central, qui regroupe toutes les obligations, procédures, clauses et arbres de décision permettant à l'entreprise, mais aussi au DPO d'être conforme au GDPR.

Pourquoi le faire ?

Pour avoir un référentiel unique, comprenant toutes les procédures et tous les documents.

Pour que la gestion documentaire de la conformité soit centralisée et aisée.

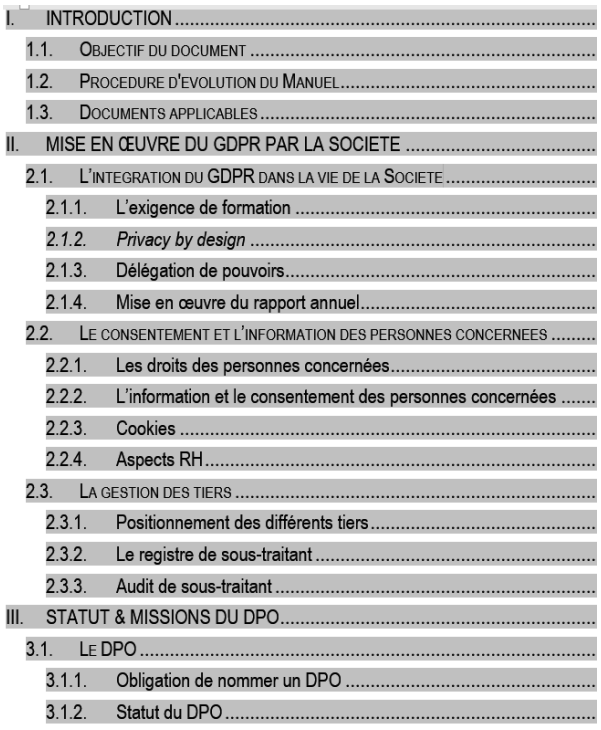
Comment le faire ?

Lawint préconise que le projet :
- intègre tous les métiers et intervenants dans un processus de création et de maintien des documents ;
- tienne compte de toutes les thématiques GDPR adaptées à l'activité de l'entreprise ;
- définisse le rôle de chaque intervenant dans le temps ;
- débouche sur des procédures concrètes et réellement mises en œuvre ;
- induise un corpus documentaire conforme à la pratique de la CNIL.

Comment Lawint peut aider ?

En rédigeant un Manuel spécifique à l'entreprise qui serait composé :
- des obligations de l'entreprise et d'une aide au respect desdites obligations ;
- des obligations du DPO et d'une aide au respect desdites obligations ;
- des procédures nécessaires ;
- des arbres de décision ;
- d'un tableau de durée de conservation des données ;
- des modèles de mentions juridiques à adapter ;
- des modèles de clauses contractuelles à utiliser ;
- des modèles de réponse en cas d'exercice des droits ;
- des modèles de documents RH à finaliser ;
- des modèles de rapport annuel ;
- des modèles de délégations de pouvoirs ;
- des modèles de fiches de poste pour le DPO ;
- des modèles de registre de sous-traitant ;
- des modèles de registre de violation de sécurité ;
- des modèles de réponses à la CNIL.

Ce Manuel doit être adapté à l'activité de chaque entreprise, aux pratiques internes, à la personnalité de la direction, aux souhaits de niveau de conformité, etc…



I. INTRODUCTION
1.1. OBJECTIF DU DOCUMENT
1.2. PROCEDURE D'EVOLUTION DU MANUEL
1.3. DOCUMENTS APPLICABLES
II. MISE EN ŒUVRE DU GDPR PAR LA SOCIETE
2.1. L'INTEGRATION DU GDPR DANS LA VIE DE LA SOCIETE
2.1.1. L'exigence de formation
2.1.2. *Privacy by design*
2.1.3. Délégation de pouvoirs
2.1.4. Mise en œuvre du rapport annuel
2.2. LE CONSENTEMENT ET L'INFORMATION DES PERSONNES CONCERNEES
2.2.1. Les droits des personnes concernées
2.2.2. L'information et le consentement des personnes concernées
2.2.3. Cookies
2.2.4. Aspects RH
2.3. LA GESTION DES TIERS
2.3.1. Positionnement des différents tiers
2.3.2. Le registre de sous-traitant
2.3.3. Audit de sous-traitant
III. STATUT & MISSIONS DU DPO
3.1. LE DPO
3.1.1. Obligation de nommer un DPO
3.1.2. Statut du DPO

ETAPE 2 – REMEDIATION – PROCEDURES COURANTES

Que faire ?

- les documents relatifs aux procédures obligatoires ;
- la mise en place de ces procédures ;
- la formation des personnes concernées sur les procédures ;
- la vérification régulière du respect de ces procédures.

Pourquoi le faire ?

Le GDPR impose de nombreuses procédures qu'il faut documenter. La CNIL demandera ces documents.

Comment le faire ?

Le GDPR impose de nombreuses procédures basées sur des textes juridiques, et notamment :
- la procédure relative à l'exercice des droits,
- la procédure de notification des violations de sécurité,
- la procédure de gestion des « partenaires » (sous-traitants, co-responsables, etc…) ;
- la procédure de gestion des transferts hors de l'Union ;
- la procédure « *privacy by design* » (prise en compte des principes de protection des données personnelles dès la conception ou l'achat de logiciel / prestations de développement) ;
- la procédure de formation du personnel (spécifique au GDPR ou propre à toute l'entreprise) ;
- la procédure de PIA.

Pour ce qui concerne le PIA, Lawint préconise d'utiliser l'outil de PIA offert gracieusement par la CNIL : https://www.cnil.fr/fr/nouveautes-sur-le-pia-guides-outil-piaf-etude-de-cas.

Pour ce qui concerne la formation, Lawint préconise le MOOC de la CNIL qui sera gratuitement accessible jusqu'en septembre 2021 : https://atelier-rgpd.cnil.fr/. Ce MOOC délivre des attestations qu'il est fortement recommandé de conserver. Toutefois, pour des formations plus spécifiques, notamment propres à des secteurs réglementés ou particulier, Lawint propose des formations en présentiel.

Comment Lawint peut aider ?

A force d'être sollicité pour rédiger les procédures « GDPR », Lawint a désormais développé un vrai savoir-faire en termes de rédaction de procédures et en a rédigé pour toutes sortes d'activités, de tailles d'entreprises et de cas spécifiques.

Ces procédures sont simples, courts, pragmatiques, faciles à utiliser par des non-juristes.

Lawint prend en compte l'existant, la taille de l'entreprise et les enjeux de la société afin de structurer ces procédures. La présence d'un DPO permettra à Lawint de les réaliser en partenariat avec cette personne et de procéder, par la même occasion, à un transfert de connaissances.

ETAPE 2 – REMEDIATION - PROCEDURES D'AUDIT

Que faire ?

- des audits annuels de conformité au GDPR (respect des principes, sécurité) de l'entreprise ;
- des audits annuel de « partenaires » critiques ;
- des audits ponctuels avant toute nouvelle entrée en relation avec un partenaire ;

Pourquoi le faire ?

Le GDPR impose une vérification annuelle de plusieurs aspects, notamment propres aux contrats avec les sous-traitants ou la sécurité informatique. De manière plus large, il est fortement conseillé de réaliser des audits réguliers de conformité, notamment de ses propres partenaires qualifiés de stratégiques.

Comment le faire ?

L'audit annuel de conformité au GDPR s'effectue de la même manière que le 1er audit (voir Etape 1). Mais le *gap analysis* s'effectue par rapport au résultat de l'année précédente.

Cet audit doit enclencher ensuite une mise à jour des documents, registres, contrats et autres procédures.

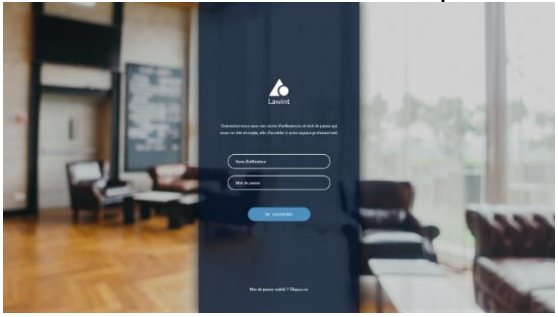
Cet audit permet aussi de rédiger le rapport annuel du DPO qui sera annexé aux documents sociétaux de l'entreprise lors de l'approbation des comptes.

Comment Lawint peut aider ?

- Rédaction des procédures d'audit des partenaires (nouveaux ou critiques):
    - Questionnaire et aide à l'interprétation des réponses ;
    - Qualification de la relation en fonction des traitements ;
    - Négociation des clauses afférente à la relation en fonction de la nature du contrat ;
    - Maintien du registre des « sous-traitants » et du registre du traitement.

  A ce titre, Lawint propose :
    - une procédure d'assistance, avec des arbres de décision
    - des clauses types contractuelles ;
    - des annexes types au contrat.

- Sur une base forfaitaire et avec l'outil dédié, audits de l'entreprise et/ou des partenaires.



ETAPE 2 – REMEDIATION - ENRICHISSEMENT GDPR DES DOCUMENTS DE SECURITE

Que faire ?

Au moins un document central relatif à la sécurité (une « Politique de Sécurité des Systèmes d'Information » par exemple).

Pourquoi le faire ?

Le GDPR, mais d'autres textes également imposent une sécurité informatique à toute entreprise. Cette sécurité doit être mise en place effectivement, mais également de manière documentée. Les documents peuvent être demandés à tout moment par la CNIL et notamment en cas de faille de sécurité.

De plus, l'absence ou la mauvaise sécurité sont pénalement sanctionnées en droit français.

Comment le faire ?

Ce document ou cet ensemble de documents doit comprendre les thématiques suivantes :
- l'authentification des utilisateurs ;
- la gestion des habilitations ;
- la traçabilité des accès et la gestion des incidents ;
- la sécurisation des locaux ;
- la sécurisation des postes de travail ;
- la sécurisation de l'informatique mobile ;
- la sécurisation du réseau informatique interne ;
- la sécurisation des serveurs ;
- la sécurisation des sites web ;
- la sauvegarde et la continuité d'activité ;
- l'archivage de manière sécurisée ;
- la maintenance et la destruction des données ;
- la sécurisation des échanges avec d'autres organismes ;
- l'encadrement des développements informatiques ;
- la politique de chiffrement et signature électronique.

Des documents complémentaires sont les bienvenus, comme un SLA, un PCA ainsi que les cahiers de procédure propres à l'IT.

Comment Lawint peut aider ?

Lawint peut accompagner les clients sur la structuration et l'existence de ces documents. Toutefois, le contenu ne peut être rempli que par le client qui seul connait son infrastructure et ses couches.

ETAPE 2 – REMEDIATION - PROCEDER AUX DEMANDES D'AUTORISATION NECESSAIRES

Que faire ?

Les déclarations à la CNIL ne seront plus nécessaires.

Toutefois, les demandes d'autorisation à la CNIL continuent de perdurer. Les autorisations acquises sous l'ancien régime perdurent, sauf disposition contraire.

Pourquoi le faire ?

Le code pénal prévoit des sanctions pénales en cas de traitements effectués sans autorisation alors que ceux-ci sont obligatoires (par exemple, certains traitements de données de santé).

Comment le faire ?

La CNIL préfère que les demandes d'autorisation soient émises par le site : https://www.cnil.fr/fr/declarer-un-fichier. Les questions sont simples et faciles à comprendre.

Il est préconisé de détailler le plus possible les aspects propres à la sécurité informatique.

Comment Lawint peut aider ?

Lawint a participé à la formalisation de très nombreuses demandes d'autorisation.

Toutefois, l'autre vraie plus-value réside dans le fait de déterminer, en amont avec le client, la nature des traitements et des données, des finalités réellement poursuivies, des tiers autorisés. Ces réunions permettent de définir des finalités et des utilisations de données souvent plus pertinentes et légales.

ETAPE OPTIONNELLE – DESIGNATION D'UN DPO

Que faire ?

Nommer un DPO si :
- les activités de base consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou
- les activités de base consistent en un traitement à grande échelle de données sensibles.

Pourquoi le faire ?

C'est une obligation au titre de la loi qui sera pénalement sanctionnée.

Toutefois, de nombreuses sociétés qui n'ont pas l'obligation de nommer un DPO le font car elles estiment que cela participe à la démonstration de l'importance de la protection des données personnelles et aussi de la confiance des clients.

Comment le faire ?

Le GDPR impose que le DPO ait des compétences avant tout juridiques, mais une compréhension technique. Il faut surtout qu'il soit disponible et qu'il puisse remplir ses tâches :
- informer et conseiller le client et les employés sur les aspects juridiques ;
- contrôler le respect du GDPR par le client ;
- procéder à la sensibilisation et la formation du personnel participant aux opérations de traitement ;
- dispenser des conseils, sur demande, en ce qui concerne les PIA ;
- coopérer avec la CNIL ;
- faire office de point de contact pour la CNIL.

Comment Lawint peut aider ?

Lawint propose en collaboration avec un partenaire IT, une offre d'assistance à DPO, sur une base mensuelle forfaitaire, permettant de répondre aux contraintes de compétence et disponibilité, mais aussi de connaissances pour conseiller et accompagner les clients.

ETAPE OPTIONNELLE – CREATION DE BCR OU PROCEDURE DE TRANSFERT DE DONNEES HORS DE L'UNION

Que faire ?

Les *Binding Corporate Rules* sont un document propre à un groupe d'entreprises ayant des localisations dans et hors de l'Union.

Pourquoi le faire ?

La loi et le GDPR interdisent tout transfert de données personnelles hors de l'Union européenne, sauf dans les cas suivants :

- le transfert a été encadré juridiquement par un contrat spécial avec le récipiendaire des données ;
- le transfert a été fait aux USA vers une entreprise membre du programme *Privacy Shield* (https://www.privacyshield.gov/welcome);
- le transfert a été fait dans le cadre d'un groupe qui a souscrit à des BCR.

Les BCR permettent donc d'avoir la possibilité d'envoyer et recevoir des données personnelles au sein d'un groupe dans le monde entier.

Ce genre de projet permet aussi à la société de prendre conscience de l'importance de la data en son sein, de leur valeur stratégique, mais aussi de leur valeur marchande.

Comment le faire ?

Les BCR sont un contrat signé par toutes les entités d'un groupe. Il faut donc faire un projet de contrat, comprenant de nombreuses clauses et annexes (dont les procédures visées à l'Etape ci-avant).

Ce projet, une fois adopté par le groupe, est présenté à la CNIL qui, en pratique, le discute et en demande souvent quelques modifications. Une fois adoptées formellement par la CNIL, ces BCR entrent en vigueur.

Comment Lawint peut aider ?

La rédaction et surtout l'approbation de BCR par la CNIL sont des étapes qui peuvent prendre plusieurs mois.

Fort de son expérience, Lawint peut assister le client dans son premier projet, tant sur la façon de le présenter aux entités du groupe, que dans ses démarches à l'égard de la CNIL ainsi que dans son déploiement à l'international.

Lawint travaille en français et en anglais.

Lawint
Cabinet d'avocats

Alexandre Diehl
Avocat à la Cour

alexandre.diehl@lawint.com
+33 1 49 11 48 01

68, rue du Faubourg Saint Honoré – 75008 Paris
www.lawint.com