ALEXANDRE DIELH

LAWINT

COMMENT ETRE CONFORME CONCREMENT

DOCUMENTS ET PROCEDURES OBLIGATOIRES

Alexandre Dielh est intervenu lors de la 3ème éditions de Cyber-day.info

COMMENT ETRE CONFORME CONCREMENT ?

DOCUMENTS ET PROCEDURES OBLIGATOIRES

MANUEL DE LUTTE CONTRE LE BLABLA

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

C'EST QUOI LA CONFORMITE ?

Il existe en France des règlements européens, des lois, des décrets, des règlements et des arrêtés qui forment le droit. Depuis toujours, la philosophie Française est d'édicter des règles, des interdits et de laisser aux autorités de prouver une violation de la loi et à la justice de sanctionner en cas de violation.

Mais certaines lois et règlements, récents, imposent aux entreprises de *démontrer* leur conformité à une autorité indépendante qui est à la fois *juge et partie* puisqu'elle peut donner des amendes. Ces lois et règlements constituent la nouvelle sous-catégorie du droit appelée « conformité » ou « *compliance* ».

La conformité recouvre principalement en droit privé :

- pour toutes les entreprises, le GDPR et les dispositions impératives du RSE
- pour les grandes entreprises, la loi Sapin II et loi Vigilance
- pour certaines entreprises, la réglementation cybersécurité OIV ou OSE
- selon les secteurs d'activités, les règlements spécifiques (télécom, banque, santé, énergie, etc…)

POURQUOI ETRE CONFORME ?

- parce que c'est une obligation, souvent sanctionnée par des amendes ou de la prison
- parce que les grands groupes refusent désormais de travailler avec les sociétés qui ne peuvent pas *démontrer* qu'elles sont conformes
- 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

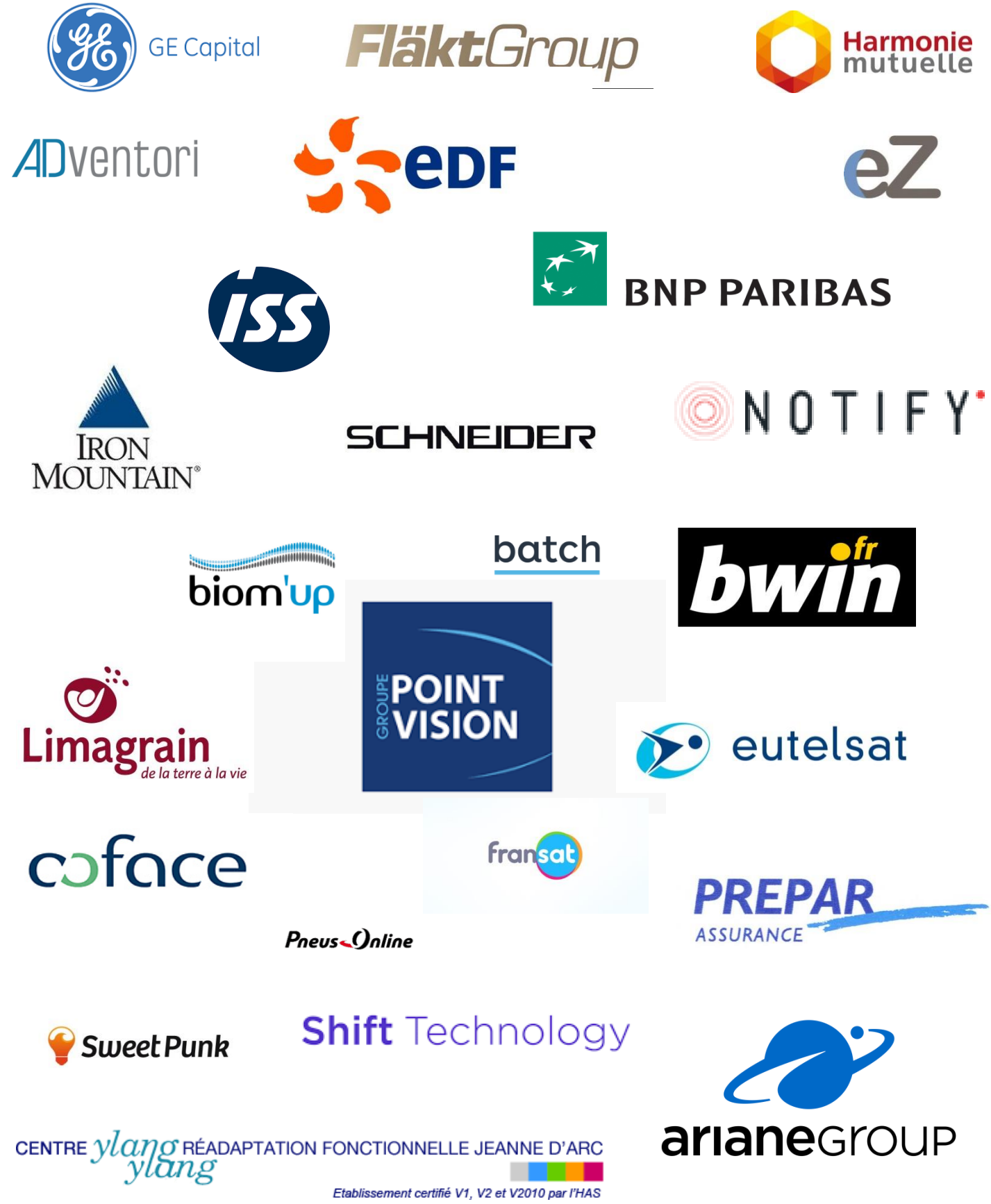
POURQUOI LAWINT PEUT VOUS AIDER ?

- Un Cabinet dédié à la Conformité, Corporate et Contrats
- Un des premiers Cabinets d'avocats dans le domaine du droit de la data en France
- Près de 20 ans d'expérience dans le domaine du droit de la data et de l'informatique
- 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 GDPR OU SAPIN 2 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

ILS NOUS FONT CONFIANCE – *TRACK RECORD* COMPLIANCE



POURQUOI CE GUIDE ?

Voilà près de 20 ans que certains professionnels de Lawint participent à la conformité des entreprises aux lois applicables en France. Et voilà près de 20 ans qu'il est constaté que les entreprises sont perdues dans les documents qu'elles doivent réellement produire en cas de problème, en cas de contrôle, en cas de procès.

Face aux nombreuses prestations inutiles et autres documents sans portée produits par de nombreux prestataires, les entreprises sont aujourd'hui souvent en violation de la loi alors qu'elles sont persuadées, parce qu'elles ont payé le prix fort, d'être en conformité.

Nous avons rédigé ce guide pour répondre concrètement à la question : « de quoi ai-je besoin pour être conforme ? ». Nous pensons qu'il faut se poser la question autrement : « **qu'est ce qu'un contrôleur ou un juge me demanderait ?** ». La réponse est simple : des agissements conformes et des documents qui démontrent la conformité.

La loi est simple : elle est écrite en français, dans un langage compréhensible, et interprétée par des juristes. Pour savoir quels documents sont nécessaires, il suffit de lire et d'interpréter correctement.

Est-ce que le GDPR impose d'avoir un mapping des données ? Non, à aucun moment. Et la CNIL n'a jamais appliqué d'amende si ce document manque. Le faire est intellectuellement enrichissant pour la société, mais ça ne rend absolument pas la société conforme de ce seul fait. En revanche, est-ce que le GDPR impose d'avoir une procédure de garantie de résilience constante du SI ou de rétablissement de la disponibilité des données (PCA/PRA) ? Oui, c'est écrit noir sur blanc à l'article 32 du GDPR.

C'est dans cet esprit que nous avons présenté une liste des principaux documents impératifs que toute société de taille normale, exerçant dans un domaine d'activité non spécifiquement réglementé, doit avoir en son sein. Cette liste n'est pas exhaustive. Nous avons intégré également les documents obligatoires de nature beaucoup plus juridique et opérationnelle, parfois loin de la DSI ou le RSSI.

En cas de contrôle, la CNIL, l'ANSSI ou toute autre autorité peut demander ces documents.

COMMENT LAWINT PEUT VOUS AIDER ?

Forts de compétences juridiques mais aussi techniques, les experts de Lawint ont pu rédiger des centaines de procédures pour les clients dans divers secteurs d'activités, réglementés (banque, assurance, énergie, défense, audiovisuel, etc…) ou non.

Lawint :

- propose et rédige les procédures de nature opérationnelle et/ou juridique ;
- propose une trame et accompagne les entreprises pour les procédures strictement techniques.

DOCUMENT INTERNE JURIDICO-TECHNIQUE – LA PSSI

C'est quoi ?

Le Plan de Sécurité des Système d'Information est un document fondamental, central (d'ailleurs souvent appelé « PCSSI » de ce fait), qui synthétise toutes les philosophies, les politiques et procédures en termes de sécurité de l'entreprise. Dans les plus grandes entreprises, cette PSSI est, de fait, composée de nombreux documents.

Pourquoi le faire ?

De nombreuses lois et règlements, souvent transversaux (par exemple, les lois pour les OIV ou OSE), imposent la rédaction, l'audit et le maintien d'une PSSI. La violation de cette obligation est très souvent d'ordre pénal (amende + prison).

Que met-on dedans ?

Il est traditionnellement admis que les thématiques du Guide d'hygiène informatique de l'ANSSI constituent le socle minimal des points à viser dans une PSSI. Ces thématiques recoupent le Guide de sécurité des données personnelles de la CNIL qui vise principalement la sécurité des données.

Il est donc recommandé de se baser sur le Guide de l'ANSSI pour intégrer les thèmes, dont :

- la formation et sensibilisation
- le mapping des infrastructures, du réseau et des droits
- la gestion des habilitations
- la sécurisation des postes et serveurs
- la sécurisation du réseau
- la sécurisation de l'administration
- le nomadisme
- le tests récurrents, la mise à jour et les audits

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

Si une loi sectorielle impose à l'entreprise d'avoir ce document, les autorités de contrôle le demanderont. Il s'agira souvent d'un document important dans le cadre du contrôle. Si l'entreprise n'a pas l'obligation d'avoir un tel document, elle pourra le présenter spontanément pour rassurer le contrôleur ; celui-ci pourra le demander mais ne pourra pas prononcer de sanction en cas de non-existence du document.

Comment Lawint peut vous aider ?

Lawint peut accompagner une entreprise à identifier les thèmes à intégrer dans la PSSI.

DOCUMENT INTERNE JURIDICO-TECHNIQUE – LE PCA/PRA

C'est quoi ?

Le Plan de Continuité d'Activité (PCA) ou Plan de Reprise d'Activité (PRA) est un processus de management qui identifie les menaces potentielles pour une organisation ainsi que les impacts que ces menaces pourraient avoir sur les opérations liées à l'activité de l'organisation. Il a pour objet de définir la réponse de l'organisation en cas de concrétisation de ces menaces afin de garantir à l'organisation la reprise et la continuité de ses activités.

Pourquoi le faire ?

L'article 32 du RGPD impose au le responsable de traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.

Le non-respect d'une telle obligation est sanctionné par une amende administrative et/ou pénalement par 5 ans d'emprisonnement et 300 000 € d'amende.

Que met-on dedans ?

Le contenu d'un PCA/PRA doit comprendre au moins les points suivants :

- Le contexte, les objectifs et obligations de l'organisation comprenant logiquement la liste des activités essentielles pour l'atteinte des objectifs et la tenue des obligations ainsi que les processus clefs nécessaires au fonctionnement des activités essentielles.
- Les risques retenus comme les plus graves explicités au moyen de scénarios.
- La stratégie de continuité d'activité qui se divise en deux phases, à savoir une phase préventive avant la réalisation du sinistre et une phase proactive lors de la réalisation du sinistre.

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

Il est très fortement probable que ce document soit demandé par la CNIL ou l'ANSSI.

Comment Lawint peut vous aider ?

Lawint vous accompagne dans la rédaction d'un PCA/PRA conforme aux *best practices* existantes et qui tiendra compte des spécificités légales et réglementaires applicables à votre activité.

DOCUMENT INTERNE JURIDICO-TECHNIQUE – LA PROCEDURE DE GESTION DES INCIDENTS DE SECURITE

C'est quoi ?

La survenance d'un incident de sécurité nécessite une réponse rapide et précise qui ne peut être correctement assurée que par le suivi d'une procédure de gestion des incidents de sécurité préalablement déterminée.

Pourquoi le faire ?

La survenance d'un incident de sécurité implique le respect de certaines obligations légales, notamment les obligations de notification aux autorités compétentes. Ne pas procéder à la notification aux autorité compétentes est puni pénalement par 5 ans d'emprisonnement et 300 000 € d'amende.

Que met-on dedans ?

Les mesures nécessaires afin de remédier rapidement aux failles de sécurité et en limiter les conséquences. C'est donc un document qui impliquera le développement séquencé des thèmes suivants :

- Prévenir et détecter les incidents de sécurité (recourir à des anti-virus, maintenir à jour les équipements informatiques, prévoir un système de journalisation des accès, sensibiliser et former les collaborateurs…).
- Déterminer les différents intervenants essentiels à la gestion de l'incident de sécurité.
- Mettre en œuvre un système de *reporting* de la faille de sécurité (interne et externe).
- Déterminer les mesures de gestion de l'incident de sécurité (qualifier l'incident et diriger la phase de réponse).
- Respect des dispositions légales applicables : notification aux autorités compétentes (CNIL, ANSSI, ARS…), aux personnes concernées, au responsable de traitement etc.
- Documenter l'incident de sécurité.

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

Ce document n'est pas expressément visé dans la loi, mais la CNIL et l'ANSSI recommandent très fortement sa rédaction et le demanderont systématiquement.

Comment Lawint peut vous aider ?

Lawint vous propose la rédaction d'une procédure personnalisée de gestion des incidents de sécurité qui répond à l'ensemble des obligations légales (comment notifier, quand notifier, qui notifier etc) et des recommandations applicables (ANSSI, CNIL etc).

DOCUMENT INTERNE JURIDICO-TECHNIQUE – LA PROCEDURE DE SECURISATION DES LOCAUX

C'est quoi ?

C'est une procédure fondée principalement sur les recommandations de la CNIL et de l'ANSSI qui développe l'ensemble des mesures de sécurité physique que doit mettre en place une entreprise.

Pourquoi le faire ?

La sécurité des systèmes d'information, des réseaux et plus généralement des données nécessite la mise en place de mesures de sécurité physique des locaux. Le non-respect d'une telle obligation est sanctionné pénalement et administrativement (amende + prison).

Que faire ?

Adopter en fonction des spécificités de l'entreprises l'ensemble des mesures suivantes :

- Mettre en place les mesures de sécurité élémentaires (formation du personnel aux pratiques élémentaires de sécurité, installer des alarmes anti-intrusion et les vérifier périodiquement, mettre en place des moyens de lutte contre les incendies etc).
- Identifier les lieux sensibles afin de renforcer les mesures de sécurité (aménagement optimal, renforcer la sécurisation des accès par la mise en place de dispositifs biométriques, vidéosurveillance etc).
- Identifier et encadrer selon la sensibilité des lieux les habilitations du personnel.

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

La loi requiert que les mesures de sécurité soient documentées (*accountability*). Ce document peut être demandé par la CNIL ou l'ANSSI.

Comment Lawint peut vous aider ?

Fort de son expérience, Lawint accompagne dans le choix des mesures de sécurité adéquates à la structure : rédaction d'une procédure permettant de mettre en place et documenter les mesures de sécurité et/ou assistance dans la mise en œuvre de certains dispositifs de sécurisation sensibles (ex : dispositifs de sécurité biométrique).

DOCUMENT INTERNE JURIDICO-TECHNIQUE – LA PROCEDURE *PRIVACY BY DESIGN*

C'est quoi ?

C'est une procédure qui impose à la société de tenir compte des principes de la loi dès la conception d'un logiciel, un programme, une solution. Ce document s'adresse principalement aux développeurs, mais aussi à l'ensemble des utilisateurs d'une solution ou encore à la direction des achats quand elle acquière des prestations IT ou des logiciels, y compris en SaaS.

Pourquoi le faire ?

La loi impose le respect des principes de *privacy by design* et de *privacy by defaut*. Le non-respect d'une telle obligation est sanctionné administrativement (amende) et/ou pénalement par 5 ans d'emprisonnement et 300 000 € d'amende.

Que met-on dedans ?

Concrètement cela consiste à adapter dès la conception et par défaut, des mesures organisationnelles et techniques appropriées pour garantir la protection de la vie privée et des libertés fondamentales. C'est donc un document qui visera les principes suivants :

- Paramétrer *by design* les mesures nécessaires à la protection des données
- Faire un choix éclairé de son architecture
- Prendre en compte l'ensemble des *best practices* nécessaires pour le développement du produit
- Tester le produit préalablement à sa mise sur le marché
- Planifier la gestion des incidents, les procédures de mises à jour et réaliser un examen complet de la sécurité du produit avant sa publication
- Maintenir le produit à jour
- Gérer les procédures d'achat

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

Ce document n'est pas expressément visé dans la loi, mais la CNIL et l'ANSSI peuvent le demander. Ce document a vocation à démontrer à la CNIL et/ou l'ANSSI que le principe est bien pris en compte par la société.

Comment Lawint peut vous aider ?

Lawint a rédigé des dizaines de procédures de *privacy by design*, rassemblant l'ensemble des *best practices*. Cette procédure, qui a pour objet de synthétiser les recommandations existantes, permet de spécifier à une entreprise les informations nécessaires pour tenir compte des principes de *privacy by design* et de *privacy by defaut* au niveau de la DSI, mais aussi de la direction des achats quand ils acquièrent des prestations IT ou des logiciels.

DOCUMENT INTERNE JURIDICO-TECHNIQUE – PROCEDURE DE GESTION DES HABILITATIONS

C'est quoi ?

La gestion des habilitations a pour finalité de protéger l'accès aux ressources du système d'information et de permettre de retrouver *a posteriori* qui était habilité à quoi. La procédure de gestion des habilitations permet donc de définir des profils d'habilitation dans les systèmes en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leurs missions.

Pourquoi le faire ?

Le défaut de mise en œuvre des mesures de sécurité adaptées est sanctionné par une amende administrative et/ ou pénalement par 5 ans d'emprisonnement et 300 000 € d'amende.

Que met-on dedans ?

Concrètement la procédure de gestion des habilitations doit comporter les thèmes suivants :

- La logique de définition des profils d'habilitation dans les systèmes en séparant les tâches et les domaines de responsabilité, les habilitations incompatibles entre elles, les habilitations à titre exceptionnel dans certains contextes et sous certaines conditions (durée, contrôles à postériori etc), les éventuelles délégations d'habilitations etc.
- Les conséquences prévues pour les personnes ayant un accès légitime aux donnés en cas de non-respect des mesures de sécurité.
- La gestion dans le temps des permissions d'accès des utilisateurs (en fonction des arrivées, départs, changement d'affectations etc).
- L'organisation d'une revue annuelle des habilitations afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.
- Les mesures permettant de restreindre et de contrôler l'attribution et l'utilisation des accès.

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

La procédure de gestion des habilitations est requise par la CNIL et par l'ANSSI et constitue à ce titre un document indispensable qui pourra être demandé à tout moment en cas de contrôle.

Comment Lawint peut vous aider ?

Forts de notre expérience en protection des données personnelles nous pouvons vous accompagner dans la rédaction de votre politique de gestion des habilitations.

DOCUMENT INTERNE JURIDICO-TECHNIQUE – PROCEDURE DE GESTION DES PIA

C'est quoi ?

C'est une procédure qui constitue les lignes directrices nécessaires à toute entreprise afin de comprendre en quoi consiste un PIA, quels sont les critères de sa mise en œuvre et le moment / manière de réaliser un PIA.

Pourquoi le faire ?

Le principe de responsabilité du responsable de traitement prévoit que celui-ci doit mettre en place un mécanisme d'auto-contrôle lors de la tenue du registre des traitements de données personnelles

La réalisation d'un PIA permet donc de satisfaire aux principes de *privacy by design*, *privacy by default* et au principe d'*accountability* et répond par conséquent à une obligation légale.

Le non-respect d'une telle obligation est sanctionné administrativement par une amende et/ou pénalement par 5 ans d'emprisonnement et 300 000 € d'amende.

Que met-on dedans ?

Pour être complète la procédure PIA doit contenir l'ensemble des points suivants :

- Les cas dans lesquels il est nécessaire / pas nécessaire de réaliser un PIA
- Les personnes intervenant dans la réalisation du PIA
- La manière de réaliser un PIA
- Les cas dans lesquels il faut transmettre son PIA à la CNIL

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

Le PIA est un document essentiel qui sera systématiquement demandé par la CNIL lors de ses contrôles et pourrait éventuellement être demandé par l'ANSSI.

Comment Lawint peut vous aider ?

Fort de son expérience Lawint a rédigé une procédure de PIA contenant l'ensemble des informations nécessaires à la réalisation d'un PIA, et peut également pour accompagner dans la réalisation de votre PIA.

DOCUMENT INTERNE JURIDICO-TECHNIQUE – LA PROCEDURE DE PURGE DES DONNEES

C'est quoi ?

C'est un document, de portée générale, qui détermine les durées de conservation par catégories de données personnelles et finalités, aux fins de purge.

Pourquoi le faire ?

La loi impose que les données personnelles ne soient pas conservées éternellement et qu'il existe, finalité par finalité, des durées de conservation maximales. Cet aspect est régulièrement contrôlé et sanctionné par la CNIL.

Que met-on dedans ?

La procédure est composée de deux éléments centraux :

- un tableau de la durée de conservation par finalité,
- la procédure en elle-même, incluant notamment :
    - la distinction entre les archives intermédiaires et finales,
    - le sort des données,
    - les preuves des purges.

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

Ce document est souvent demandé en contrôle par la CNIL et parfois par l'ANSSI. Avoir déterminé les durées de conservation est une obligation forte, aujourd'hui sanctionnée par la CNIL qui n'hésite plus à appliquer des amendes à ce titre.

Comment Lawint peut vous aider ?

Les durées de conservation sont définies par la loi et leur détermination est un travail de juriste. Lawint, en tant que cabinet d'Avocats, détermine, secteur d'activité par secteur d'activité, réglementation par réglementation, les durées de prescription et de conservation. Chaque secteur est différent, chaque réglementation est différente et il n'existe pas de durée-type.

DOCUMENT INTERNE JURIDIQUE – LA CHARTE INFORMATIQUE

C'est quoi ?

C'est un document, de portée générale et applicable à tous les salariés voire aux personnes externes, imposant des règles et devoirs en termes d'utilisation de l'informatique, du réseau et autres éléments IT.

Pourquoi le faire ?

La loi ne prévoit pas les règles, interdits, limitations et procédures qu'une charte informatique gère. La charte est donc un document complémentaire à la loi, indispensable pour que la société soit protégée de nombreux comportements illicites et puisse appliquer des sanctions le cas échéant.

La charte informatique a une valeur de règlement intérieur et doit être acceptée dans les mêmes formes.

Que met-on dedans ?

Il n'existe pas de charte informatique type, chaque société étant différente, mais il est préconisé d'intégrer au moins les thèmes suivants s'ils ne sont pas traités par ailleurs :

- rappel des droits GDPR,
- sécurisation des postes et serveurs,
- sécurisation des locaux,
- sécurisation du réseau,
- règles d'utilisation des appareils nomades,
- règles d'utilisation de la messagerie,
- règles d'utilisation d'Internet / réseaux sociaux,
- sanctions en cas de non-respect.

Est-ce que la CNIL et/ou l'ANSSI peut le demander en cas de contrôle ?

Sauf rare exception, il n'existe aucune loi imposant à une entreprise d'avoir ce document. En conséquence, il est probable que tout contrôleur demande ce document (qui reste habituel pour une entreprise de plus de 50 salariés), mais aucun contrôleur ne prononcera de sanction en cas de non-existence du document.

Comment Lawint peut vous aider ?

Document parfaitement juridique, Lawint rédige la charte informatique et préconise à l'entreprise les éléments à intégrer. Force de proposition grâce aux dizaines de chartes déjà rédigées, Lawint peut faire profiter ses clients d'un *benchmark* anonymisé pertinent et efficace.

AUTRES DOCUMENTS OBLIGATOIRES MAIS NON TECHNIQUES

C'est quoi ?

Il existe de nombreux autres documents obligatoires, au titre des autres lois de type compliance, qui ne relèvent pas directement des opérationnels techniques (DSI / RSSI, etc…). Ces documents sont souvent sous l'autorité soit du DPO, soit du Juridique, soit de la Direction Générale.

On pourra citer, par exemple :

Domaine	Direction	Intervenants	Nom	Obligation légale
DPO	DPO	DPO	**Procédure d'exercice des droits**	oui
Juridique	Juridique / DPO / Achats	Juridique / DPO / Achats	**Procédure de contractualisation**	oui
Juridique	Juridique / DPO / Achats	Juridique / DPO / Achats	**Procédure d'audit de partenaires**	oui
Juridique	Juridique / DPO / Achats	Juridique / DPO / Achats	**Transferts hors UE**	oui
Corporate	DG	DG / DPO	**Registre des traitements**	presque toujours
Corporate	DG	DG / DPO	**Registre du sous-traitant**	presque toujours
Corporate	DPO	DPO	**Rapport annuel DPO**	oui quand il existe un DPO
Commercial	Communication	Communication / DPO	**Mentions juridiques sur Site / Mail / Publicité**	oui

De plus, les documents habituels d'une entreprise, comme les contrats, doivent comprendre des clauses spécifiques, adaptées à l'entreprise, la relation contractuelle, l'environnement et le contexte spécifique.

Domaine	Direction	Intervenants	Nom	Obligation légale
Commercial	Commercial / Juridique	Commercial / DJ / DPO	**Contrat client**	oui
Commercial	Juridique / DSI	Juridique / DSI / DPO	**Contrat fournisseur**	oui
Commercial	Juridique / DSI	Juridique / DSI / DPO	**Appel d'offres**	oui

Comment Lawint peut vous aider ?

Lawint rédige, propose, modifie, les procédures (exercice des droits, audit de partenaires, etc…) et les documents juridiques. Force de proposition grâce aux centaines de documents déjà rédigés dans le cadre du GDPR, Sapin 2, NIS, *medical devices*, etc…, Lawint sait faire profiter ses clients d'une expérience unique.

AUTRES DOCUMENTS CONSEILLES MAIS NON OBLIGATOIRES

C'est quoi ?

Il existe de très nombreux documents techniques qui ne sont pas obligatoires. En fait, il s'agit de la plupart des documents qu'une entreprise produit ou que les prestataires rédigent.

Ces documents ne sont pas toujours obligatoires mais peuvent l'être parfois selon une loi très spécifique ou une situation particulière.

Toutefois, nous estimons que certains documents, sans être obligatoires, peuvent avoir une utilité juridique et/ou opérationnelle, comme par exemple :

Domaine	Direction	Intervenants	Nom	Obligation légale
Corporate	DG	DG	**Délégation de pouvoirs**	non
Corporate	DG / DPO	DPO	**Procédure en cas de contrôle CNIL**	recommandée
Commercial	DSI / RSSI / Juridique	Commercial / DSI / DPO	**PAS**	fortement recommandé

La délégation de pouvoir sert, par exemple, à ce que le chef d'entreprise n'endosse pas la responsabilité pénale propre à une obligation (par exemple, la sécurité informatique) et transmette cette responsabilité à la personne concernée (par exemple, le RSSI).

Comment Lawint peut vous aider ?

Lawint rédige, propose, modifie, les contrats, les mentions légales applicables aux matériels de communication, les procédures (que faire en cas de contrôle de la CNIL, etc…) et les délégations de pouvoirs. Force de proposition grâce aux centaines de documents déjà rédigés dans le cadre du GDPR, Sapin 2, NIS, *medical devices*, etc…, Lawint peut faire profiter ses clients d'une expérience spécifique.

Pour ce qui concerne le PAS, Lawint propose une trame et accompagne les entreprises pour le finaliser.

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