

Plan de la formation

- 1 Contexte et vue d'ensemble du GDPR
- 2 Principes, définitions et champs d'application
- 3 Projet de mise en conformité
- 4 Principes relatifs aux traitements de données
- 5 Droits des personnes concernées
- 6 Obligations et responsabilités des acteurs du traitement
- 7 Méthodologies et outils du consultant

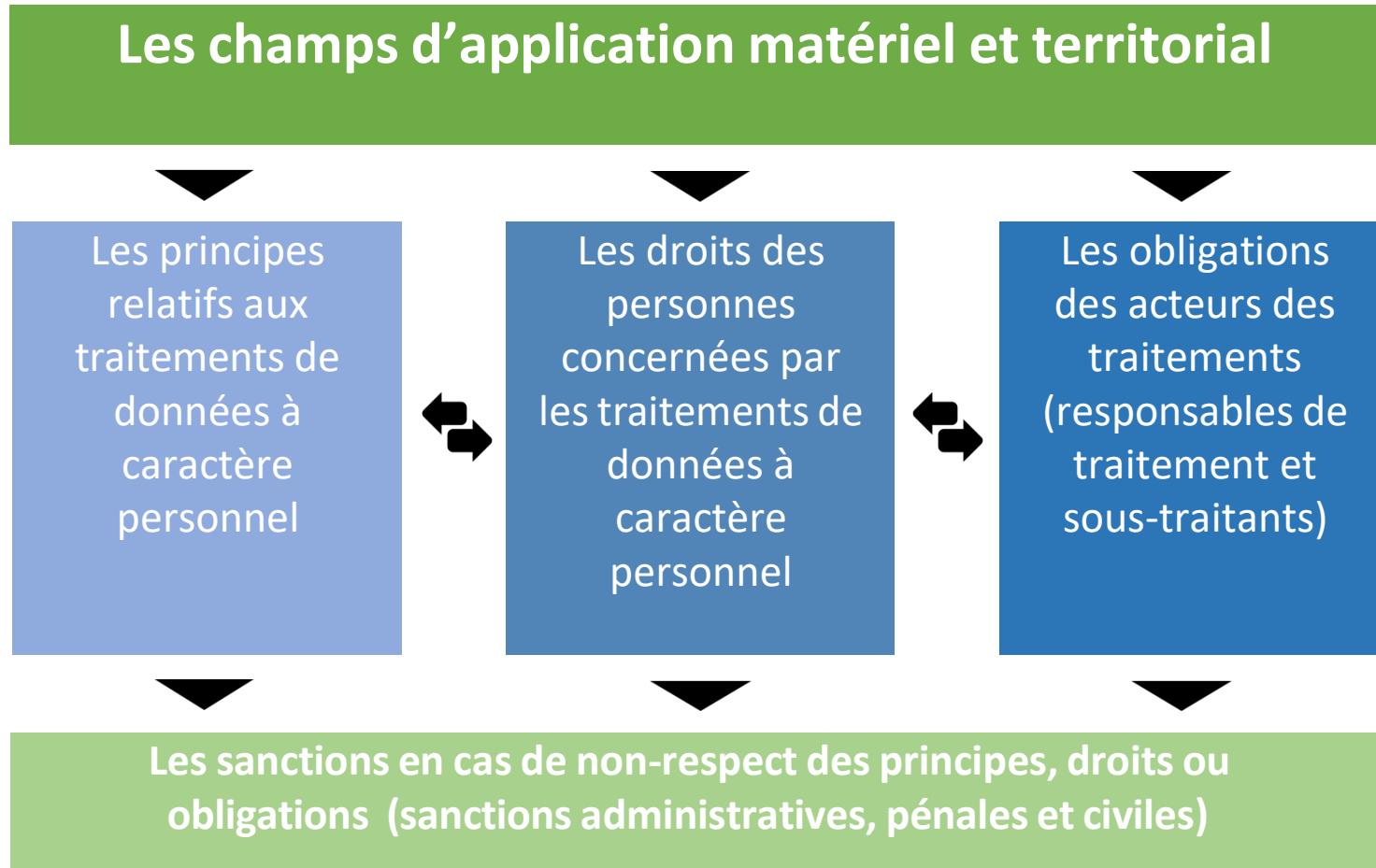
Vie privée et protection des données personnelles

- Le droit de chacun à la protection de sa vie privée a été consacrée par une **loi du 17 juillet 1970** « tendant à renforcer la garantie des droits individuels des citoyens » : « Chacun a droit au respect de sa vie privée. » (art. 9 du Code Civil)
- La France et l'Europe ont développé une réglementation destinée à protéger les données à caractère personnel
 - La **Loi n° 78-17 du 06/01/1978 relative à l'informatique, aux fichiers et aux libertés** modifiée le **06/08/2014**, dite loi « Informatique & libertés »
 - La **Directive européenne n° 95/46 du 24 octobre 1995** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
 - La **Directive européenne n°2002/22 du 12/07/2002**, modifiée le 25/11/2009, et concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques
 - La **Loi n°2016-1321 du 07/10/2016 pour une République numérique**

Réforme du cadre européen de protection

- Le règlement **européen n°2016/679 sur la protection des données personnelles (GDPR)** a été adopté le 27 avril 2016 et publié au Journal Officiel le 4 mai 2016
 - Le règlement constitue une **réforme globale de règles en matière de protection des données personnelles**
 - Le règlement vise à remplacer la directive européenne de 1995 sur la protection des données à caractère personnel (95/46/CE), par **une législation unique**, afin de mettre fin à la fragmentation juridique actuelle entre les Etats membres.
- Ce règlement est applicable à compter du **25 mai 2018** dans tous les pays de l'Union européenne
 - La **Loi n°2016-1321 du 07/10/2016** pour une République numérique vient anticiper certaines dispositions (ex. augmentation des montants d'amende ...)

Vue d'ensemble du règlement GDPR



- Une augmentation des montants des amendes administratives (en fonction de la gravité) jusqu'à **10 M€/2% du CA annuel mondial ou 20 M€/4% du CA annuel mondial**

Ligne directrices du G29

- Les lignes directrices du G29 visent à clarifier et illustrer d'exemples concrets différents aspects du GDPR :
 - Autorité chef de file
 - Délégué à la protection des données
 - Droit à la portabilité
 - Analyse d'impact relative à la protection des données
 - Notification des violations de données personnelles
 - ..

Principe clé de responsabilisation

- Le règlement européen repose sur une logique de conformité, dont les acteurs (responsable de traitement et sous-traitants) sont responsables, sous le contrôle et avec l'accompagnement de l'autorité de protection
 - Cette logique de conformité vient remplacer la logique de « formalités préalables » de la directive 95/46
 - Elle s'accompagne également d'un renforcement des sanctions de l'autorité de contrôle
- Ce principe d'« accountability » consiste à imposer aux acteurs du traitement :
 - de prendre des mesures efficaces et appropriées afin de **se conformer au règlement** européen et
 - **d'apporter la preuve**, sur demande de l'autorité de contrôle, que les mesures appropriées ont été prises.
- Le règlement prévoit, dans cette logique de conformité et de responsabilisation, différentes mesures : délégué à la protection des données, registre des activité de traitement, « protection des données dès la conception et par défaut », analyse d'impact

Plan de la formation

- 1 Contexte et vue d'ensemble du GDPR
- 2 Principes, définitions et champs d'application
- 3 Projet de mise en conformité
- 4 Principes relatifs aux traitements de données
- 5 Droits des personnes concernées
- 6 Obligations et responsabilités des acteurs du traitement
- 7 Méthodologies et outils du consultant

Notion de donnée à caractère personnel

- Une « **donnée à caractère personnel** » correspond à toute information qui permet d'identifier, directement ou indirectement, une personne physique (art. 4)
 - Il peut s'agir notamment d'une 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 »;
 - Exemples : nom et prénom, numéro de téléphone, adresse postale, électronique, numéro de compte ou carte bancaire, numéro de sécurité sociale, identifiant national, données de trafic (adresse IP), données de géolocalisation, données biométriques, photographies, code d'identification RH, identifiant d'accès à une application (logins) ...

Notion de traitement de données

- Un « **traitement de données à caractère personnel** » correspond à toute opération (ou ensemble d'opérations) réalisé(es) sur des données à caractère personnel (art. 4 du GDPR)
 - Une notion très large, recouvrant toute opération ou tout ensemble d'opérations portant sur des données à caractère personnel, quel que soit le procédé utilisé,
 - Exemples : collecte, enregistrement, organisation, conservation, adaptation ou modification, extraction, consultation, utilisation, communication par transmission, diffusion ou mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction

Acteurs du traitement de données

- Un « **responsable de traitement** » est défini comme 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 (art. 4)
- Un « **sous-traitant** » est défini comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (art. 4)
- Un « **destinataire** » est défini comme la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers (art. 4)

Champ d'application matériel

- Le GDPR s'applique à tous les traitements de données à caractère personnel :
 - qui **sont automatisés** (complètement ou partiellement automatisés)
 - qui **ne sont pas automatisés** à condition que les données à caractère personnel concernées soient contenues ou appelées à figurer dans des fichiers.
 - un « fichier » est défini (art. 4) comme « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »
- Le GDPR ne s'applique pas aux traitements (qu'ils soient automatisés ou non)
 - qui sont mis en œuvre pour l'exercice d'activités **exclusivement personnelles**
 - qui sont mis en œuvre par les Etats membres et/ou autorités compétentes dans le cadre d'activités spécifiques (art. 2)

Champ d'application territorial

- Le GDPR s'applique aux traitements de données à caractère personnel :
 - qui sont effectués dans le cadre **des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union** (que le traitement ait lieu ou non dans l'Union Européenne)
 - qui sont effectués par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union Européenne
 - lorsque ces traitements visent à **fournir des biens et des services** aux résidents d'un pays membre de l'UE, ou
 - à suivre le comportement de personnes, dans la mesure où ce comportement a lieu au sein l'UE

Plan de la formation

- 1 Contexte et vue d'ensemble du GDPR
- 2 Principes, définitions et champs d'application
- 3 Projet de mise en conformité
- 4 Principes relatifs aux traitements de données
- 5 Droits des personnes concernées
- 6 Obligations et responsabilités des acteurs du traitement
- 7 Méthodologies et outils du consultant

Projet de mise en conformité



Projet transverse impliquant différents acteurs : juridique, sécurité, métiers ...

Gouvernance de la conformité

Le principe de responsabilisation (« **accountability** ») impose indirectement aux responsables de traitements et/ou sous-traitants la mise en place d'un **système de management de la protection des données à caractère personnel**

1	MAINTENIR UNE ORGANISATION INTERNE LIÉE À LA PROTECTION DES DONNÉES		
2	MAINTENIR UN INVENTAIRE DES TRAITEMENTS	3	VÉRIFIER LA CONFORMITÉ DES TRAITEMENTS
4	MAINTENIR DES DOCUMENTS SUPPORT	5	COMMUNIQUER, SENSIBILISER ET FORMER
6	GÉRER LES RÉCLAMATIONS ET LES CONTENTIEUX	7	GÉRER LES RISQUES DES TIERS
8	GÉRER LES RISQUES DE SÉCURITÉ DE L'INFORMATION	9	GÉRER LES VIOLATIONS DE DONNÉES
10	SUPERVISER ET CONTRÔLER LA CONFORMITÉ		

Conformité des traitements

1. CARTOGRAPHIER LE TRAITEMENT

 Acteurs et responsabilités

 Catégories de personnes concernées par le traitement

 Catégories des données et durées de conservation

 Données sensibles

 Catégories de destinataires

 Transferts de données hors de l'Union Européenne

2. ANALYSER LA CONFORMITÉ DU TRAITEMENT

 Licéité du traitement

 Loyauté de la collecte

 Limitation des finalités

 Minimisation des données

 Exactitude des données

 Transparence et information des personnes concernées

 Sécurité des données

 Garantie juridique pour les transferts hors UE

 Réalisation requise d'un PIA

 Encadrement des relations avec les sous-traitants

 Respect des droits des personnes

3. DÉFINIR ET METTRE EN ŒUVRE LE PLAN D'ACTION DE MISE EN CONFORMITÉ DU TRAITEMENT

Plan de la formation

- 1 Contexte et vue d'ensemble du GDPR
- 2 Principes, définitions et champs d'application
- 3 Projet de mise en conformité
- 4 Principes relatifs aux traitements de données
- 5 Droits des personnes concernées
- 6 Obligations et responsabilités des acteurs du traitement
- 7 Méthodologies et outils du consultant

Régime juridique applicable aux traitements

- 1. Les traitements de données à caractère personnel sont permis sauf si la loi en dispose autrement**
- 2. Lorsque la loi n'interdit pas le traitement, ce traitement n'est licite que s'il respecte un certain nombre de conditions de fond**

Licéité	Loyauté	Limitation des finalités	Minimisation des données	Exactitude
Transparence	Limitation de la conservation	Sécurité	Transfert hors UE	Responsabilité

Interdiction par la loi de certains traitements

- Le GDPR (art. 9.1) **interdit par principe** le traitement de certaines catégories de données :
 - qui font apparaître, directement ou indirectement :
 - les **origines raciales ou ethniques**;
 - les **opinions politiques**,
 - Les **convictions philosophiques ou religieuses**;
 - l'**appartenance syndicale** des personnes,
 - qui sont relatives à **la santé**, la **vie sexuelle** ou **l'orientation sexuelle** de personnes
 - des données **génétiques** ou des données **biométriques** aux fins d'identifier une personne physique de manière unique
- Il est cependant prévu des exceptions (art. 9.1.2 à 4) à ce principe d'interdiction, et sous certaines conditions :
 - Exemple : le consentement de la personnes, la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, la nécessité aux fins de l'exécution des obligations et de l'exercice des droits en matière de droit du travail, de la sécurité sociale et de la protection sociale ...

Principe de licéité (1)

- Un traitement doit avoir le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes (art. 6):
 - 1) Le respect d'une obligation légale incombant au responsable de traitement ;
 - 2) La sauvegarde de la vie de la personne concernée ;
 - 3) L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
 - 4) L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci;
 - 5) La réalisation de l'intérêt légitime poursuivi par le responsable de traitement ou par le destinataire sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentales de la personne concernée.

Principe de licéité (2)

- Lorsque le consentement constitue la base légale du traitement (art. 7)
 - Ce consentement doit être spécifique, c'est-à-dire distingué clairement des autres questions, sous une forme compréhensible et aisément accessible, formulée en des termes clairs et simples.
 - La personne concernée a le droit de retirer son consentement à tout moment, ce dont elle doit être expressément informée.
 - Le responsable de traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données personnelles la concernant.

Exemple : La CNIL sanctionne 2 sites de rencontre en raison du traitement de données sensibles (vie sexuelle, opinions religieuses, origines ethniques) sans consentement exprès des utilisateurs. La seule inscription au site de rencontre (acceptation CGU) ne peut valoir accord exprès des personnes au traitement de telles données qui révèlent des éléments de leur intimité (Délibérations n°2016-405 et n°2016-406 du 15 décembre 2016)

Principe de loyauté

- Tout traitement de données personnelles doit être effectué dans des conditions permettant d'en assurer la transparence vis-à-vis des personnes concernées et ne saurait être mis en œuvre à l'insu des personnes concernées (art. 5.1.a)

Exemple : la collecte d'e-mails par un robot sur internet et à l'insu des intéressés constitue une collecte déloyale (CA Bordeaux, 18 décembre 2013)

Exemple : la collecte de données relatives à la navigation des internautes, à leur insu, sur des sites tiers alors même qu'ils ne disposent pas de compte sur le site (via le bouton « J'aime » par exemple) constitue une collecte déloyale (décision n° 2016-007 du 26 janvier 2016, Facebook)

Exemple : la collecte de données transmises sur des réseaux Wi-Fi non sécurisés de foyers situés sur le passage des Google cars (condamnations en France, Belgique, Italie, Allemagne et Espagne)

Exemple : l'utilisation de scripts ou de robots destinés à aspirer les données afin de savoir si le client d'un site est actif ou non (données accessibles librement et sans protection/volonté de restreindre l'accès) constitue un moyen déloyal de recueillir à l'insu des personnes physiques des adresses électroniques (CA Paris, 15 septembre 2017)

Principe de limitation des finalités

- Des données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé, explicite et légitime (art. 5.1.b). Les objectifs poursuivis par le responsable du traitement doivent donc être préalablement définis, de manière claire, explicite et exhaustive.
- Toute utilisation de données à caractère personnel pour un objectif incompatible avec la finalité première du traitement est un détournement de finalité passible de sanctions administratives ou pénales.

Exemple : l'employeur qui avait informé ses salariés de la géolocalisation de leur véhicule de fonction dans un but statistique ne peut pas se servir des données produites par le système comme preuve d'un comportement fautif, entraînant un licenciement (CA de Lyon, 13 mars 2013)

Exemple : utiliser les adresses électroniques des abonnés d'un théâtre pour leur adresser une communication politique, alors que celles-ci avaient été initialement collectées pour assurer la gestion de leur abonnement ou leur adresser des informations culturelles (délibération CNIL n°2015-040 du 12 février 2015, TNB)

Exemple : La Cour d'appel de Paris annule le licenciement disciplinaire d'un employé en raison d'un détournement de la finalité de l'outil de DLP (prévu pour la sécurité du système d'information) utilisé en l'espèce pour contrôler l'activité des salariés (CA Paris, 12 mai 2016)

Principe de minimisation des données

- Seules doivent être traitées les informations pertinentes, adéquates et non excessives au regard de la finalité du traitement, c'est-à-dire de son objectif (principe de "minimisation des données"). (art. 5.1.c).

Exemple : l'enregistrement dans la base client de commentaires non-pertinents (« Clte Imbécile », « Client raciste », « Clt a une maladie cardiaque ») constitue un manquement à l'obligation de conserver des données adéquates, pertinentes et non-excessives (délibération n° 2016-083 du 26 septembre 2016, Cdiscount)

Exemple : la mise en place d'un système de vidéosurveillance qui réalise une collecte systématique des images des salariés dans ou aux abords immédiats des lieux de repos de l'établissement, des sanitaires ou encore dans des vestiaires ne peut être regardée comme proportionnée à la seule finalité de protection des biens et personnes qu'en présence de justifications précises (délibération n°2014-307 du 17 juillet 2014)

Principe d'exactitude

- Les données doivent être exactes et si nécessaire tenues à jour. (art. 5.1.d)
- Le responsable de traitement doit prendre toutes les mesures raisonnables pour que les données à caractère personnel qui sont inexactes (au regard des finalités de traitement), soient effacées ou rectifiées sans tarder (exactitude);

Exemple : la CNIL a prononcé un avertissement public à l'encontre d'un opérateur de télécommunication pour un manquement à l'obligation de veiller à l'exactitude des données à caractère personnel suite à un dysfonctionnement informatique ayant entraîné la communication par erreur de l'identité d'un même abonné à l'HADOPI à 1531 reprises (délibération CNIL n° 2016-053 du 1er mars 2016, NC Numericable)

Principe de transparence (7)

- Toute personne physique auprès de laquelle sont recueillies des données à caractère personnel la concernant doit en être préalablement informée en des termes clairs, simples et aisément accessibles. (art. 12, 13 et 14)
 - Ces informations peuvent figurer sur le support servant à recueillir les données personnelles (formulaire, page web, etc.) ou sur un autre document porté à la connaissance des personnes concernées (affichage dans un bureau, charte informatique ...).

Principe de transparence (8)

■ Les personnes concernées doivent être informées lors de la collecte (art. 13):

- 1) de l'identité du responsable de traitement ou de son représentant;
- 2) des coordonnées du délégué à la protection des données
- 3) des finalités poursuivies par le traitement et la base juridique justifiant la légitimité du traitement ;
- 4) de la mention explicite des intérêts légitimes poursuivis par le responsable de traitement lorsque ces derniers constituent la base juridique du traitement ;
- 5) des catégories de données à caractère personnel concernées;
- 6) des destinataires ou catégories de destinataires des données ;
- 7) le cas échéant, des transferts de données effectuées vers des pays non membres de l'Union européenne (pays d'établissement des destinataires, nature des données transférées, finalité du transfert, catégories de destinataires, niveau de protection offert par le(s) pays tiers);
- 8) de la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée ;
- 9) de l'existence de droits à leur profit (droit d'opposition, droit d'accès aux données les concernant, droit de rectification ou d'effacement, droit à limitation du traitement et droit à la portabilité);
- 10) de l'existence du droit de retirer son consentement à tout moment ;
- 11) le droit d'introduire une réclamation auprès de l'Autorité de Contrôle ;
- 12) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données;
- 13) de l'existence d'une prise de décision automatisée, y compris un profilage produisant des effets juridiques ou l'affectant de manière significative de façon similaire et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Principe de transparence (9)

- Lorsque les données n'ont pas été collectées directement par le responsable de traitement, le responsable doit également indiquer, en plus des informations mentionnées à l'article 13, la source auprès de laquelle il a obtenu ces données et, le cas échéant, si ces données étaient publiquement accessibles (art. 14)

- Ces informations doivent être communiquées dans une période raisonnable après l'obtention des données et au plus tard à la première des dates suivantes :
 - un mois après l'obtention des données, eu égard aux circonstances particulières dans lesquelles les données sont traitées,
 - lors de la première communication avec la personne concernée ou
 - en cas de communication de ces données à un tiers, avant une telle communication.

Principe de limitation de la conservation

- Une durée de conservation précise doit impérativement être déterminée, en fonction de la finalité de chaque traitement, par le responsable du traitement. (art. 5.1.e)
- Des dispositions législatives ou réglementaires peuvent toutefois contraindre un responsable de traitement à conserver des données au-delà de leur durée de conservation en base active. Dans ce cas, les données peuvent être conservées dans une base d'archive, le temps nécessaire au respect de l'obligation en question, dans le respect des conditions prévues par la législation/réglementation ou l'Autorité de contrôle.

Exemple : la conservation de dossier RH de plusieurs salariés ayant quitté l'entreprise depuis plus de cinq ans, en l'absence d'obligation légale ou réglementaire n'est pas une durée nécessaire à la finalité poursuivie (Délibération n°2014-307 du 17 juillet 2014, Providis Logistique)

Exemple : la société qui n'a pas défini de durée de conservation précise et n'a pas mis en œuvre un mécanisme de purge des données (automatique ou manuel) dans sa base, n'a pas pris les mesures permettant de respecter son obligation de définition d'une durée de conservation des données adaptée à la finalité de la base. (Délibération n°2012-214 du 19 juillet 2012, FNAC direct)

Exemple : la CNIL sanctionne une société qui (après une mise en demeure) fixe une durée de conservation des données relatives aux clients en contradiction avec les exigences et son engagement de conformité à la norme simplifiée n°48 relative à la gestion des clients/prospects (délibération CNIL n° 2016-204 du 07 juillet 2016, Brandalley)

Principe de sécurité

- Le responsable du traitement est astreint à une obligation de sécurité : il doit notamment prendre les mesures nécessaires pour garantir la confidentialité et l'intégrité des données qu'il a collectées et éviter leur divulgation à des tiers non autorisés (art. 5.1.f).

Privacy by design & by default

- Obligation de prendre en compte la protection des données dès la conception des systèmes et des produits : minimisation des données, pseudonymisation, mesures de sécurité ...
- Obligation de mettre en œuvre des mesures pour garantir par défaut la protection des données : restreindre par défaut l'accès, limiter la quantité et les durées de conservation

Privacy Impact Assessment

- Obligation (pour certains traitements sensibles) de réaliser (et revoir régulièrement) une analyse des risques sur la vie privée des personnes : identification des risques et contre-mesures appropriées
- Obligation de consulter l'autorité de contrôle en cas de risques résiduels élevés

Obligation de sécurité

- Obligation de mettre en place les mesures appropriées en prenant en compte l'état de l'art, les coûts des mesures et les risques
- Enumération de quatre catégories de mesures qui pourront être appropriées selon les besoins : chiffrement, pseudonymisation, audits ...
- Possibilité d'appliquer un mécanisme de certification pour démontrer la conformité

Notification des violations

- Obligation de notifier à l'autorité de contrôle toute violation de sécurité sur les données dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance
- Obligation de tenir un registre des violations
- Obligation de notifier les personnes concernées « en cas de risque élevé pour leurs droits et libertés » dans les meilleurs délais

Principe de sécurité - Exemples

07/08/2014 Orange

- Accès aux données nominatives (env. 1,3 millions) par un tiers non-autorisé
- Absence d'audit de sécurité sur la version de l'application technique spécifiquement développée
- Communication au prestataire des mises à jour des fichiers (de données) de manière non sécurisée
- Aucune clause de sécurité et de confidentialité des données imposée au prestataire secondaire

20/09/2016 Cdiscount

- Conservation en clair de 4179 numéros de cartes bancaires (2104 cartes bancaires avec cryptogramme) dans des champs commentaires sans mesures de sécurité particulières d'obfuscation ou tokenisation permettant de garantir la sécurité des données et d'empêcher que des tiers non autorisés y aient accès (ex. prestataires externes)

27/07/2017 Hertz

- Accès à partir d'une adresse URL, aux données personnelles renseignées par 35 357 personnes inscrites sur un site (identité, coordonnées, numéro de permis de conduire) en raison d'une erreur commise par le prestataire lors d'une opération de changement de serveur (suppression accidentelle d'une ligne de code avait entraîné le réaffichage des formulaires remplis par les adhérents au programme de réduction)
- Absence de cahier des charges pour le développement de site (par son prestataire) et absence de protocole complet de test afin de garantir l'absence de toute vulnérabilité avant la mise en production

Encadrement des transferts hors UE (

- Les **transferts** de données vers un pays situés **en-dehors de l'Union européenne** (ou de l'Espace économique européen) ou une organisation internationale ne peuvent avoir lieu qu'avec l'une des garanties juridiques prévues par le règlement (art. 44 à 46)
 - Décision d'adéquation de la Commission Européenne (pays adéquats) et Privacy Shield
 - Clauses Contractuelles Types
 - Binding Corporate Rules
 - Code de conduite ou Certification approuvée
 - Dérogations prévues à l'article 49
- La notion de transfert regroupe de manière large la communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (ex : accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex. d'un disque dur d'ordinateur à un serveur)

Encadrement des transferts hors UE (

Pays destinataire avec une législation reconnue par une **décision de la Commission européenne** comme offrant une protection suffisante



- la Commission européenne peut constater par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat
 - Liste des pays adéquats (liste évolutive) : Andorre, Argentine, Canada, Guernesey, Ile de Man, Iles Féroé, Israël, Jersey, Nouvelle-Zélande, Suisse, Uruguay

La Commission a adopté le 12/07/2016 le « **Privacy Shield** », un nouveau cadre juridique pour le transfert des données personnelles vers les USA (entrée en vigueur le 01/08/2016)

- Les entreprises américaines destinataires des données doivent être inscrites sur le registre tenu par l'administration américaine et respecter les obligations et les garanties prévues

Encadrement des transferts hors UE (

signature entre les deux parties de **Clauses**

Contractuelles Types adoptées ou approuvées par la Commission européenne

règles d'entreprise contraignantes (**Binding Corporate Rules**) correspondant à un code de conduite interne qui définit la politique d'un groupe (multinational) en matière de transferts de données personnelles hors de l'UE (art. 47)



- des clauses types de protection des données adoptées par la Commission européenne

- des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission européenne



- les BCR doivent être contraignantes et respectées par toutes les entités du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs salariés

- les BCR font l'objet d'une revue (puis autorisation) par les Autorités de contrôle de l'UE

- les procédures associées aux BCR

- régime de responsabilité pesant sur le siège européen
- procédure de formation du personnel
- procédure d'audit
- procédure interne de gestion de plainte
- réseau de responsables à la protection des données

Encadrement des transferts hors UE (

un **code de conduite** approuvé (art. 40) ou un **mécanisme de certification** approuvé (art. 42), assorti de l'engagement contraignant/exécutoire d'appliquer les garanties appropriées



- Possibilité pour un responsable de traitement ou un sous-traitant d'appliquer un « **code de conduite** » ou un mécanisme de « **certification** » pour faciliter la mise en œuvre et disposer d'éléments attestant du respect des obligations
 - Des codes de conduites élaborés par des associations ou représentants de catégorie d'acteurs en fonction de la spécificité des différents secteurs de traitement de données et des besoins spécifiques (art. 40 et 41)
 - Des mécanismes de certification en matière de protection des données aux fins de démontrer que les opérations de traitement effectuées respectent le règlement (art. 42 et 43)
 - Une certification ne diminue pas la responsabilité du responsable du traitement ou du sous-traitant

Encadrement des transferts hors UE (

Exceptions prévues à
l'article 49 du GDPR



- Soit la personne a **consenti expressément** au transfert de ses données personnelles
- Soit le transfert **s'avère nécessaire** à l'une des conditions suivantes :
 - la **sauvegarde de la vie** de cette personne, la sauvegarde de **l'intérêt public**, la **défense d'un droit** en justice, la **consultation d'un registre public**
 - **l'exécution d'un contrat** entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci
 - la **conclusion ou l'exécution d'un contrat** conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers

Plan de la formation

- 1 Contexte et vue d'ensemble du GDPR
- 2 Principes, définitions et champs d'application
- 3 Projet de mise en conformité
- 4 Principes relatifs aux traitements de données
- 5 Droits des personnes concernées
- 6 Obligations et responsabilités des acteurs du traitement
- 7 Méthodologies et outils du consultant

Les droits des personnes concernées

- Les personnes concernées par le traitement des données à caractère personnel disposent des droits suivants :
 - Droit d'accès aux données et aux informations concernant le traitement
 - Droit d'opposition au traitement
 - Droit de rectification des données
 - Droit à l'effacement (« droit à l'oubli »)
 - Droit à la limitation du traitement
 - Droit à la portabilité des données
 - Droit d'opposition aux décisions individuelles automatisées et profilage
 - Droit d'introduire une réclamation auprès d'une autorité de contrôle

Droit d'accès

- Toute personne physique justifiant de son identité peut obtenir une copie des données personnelles la concernant et accéder à toute information disponible quant à l'origine de celles-ci, ainsi qu'aux informations permettant de connaître et de contester la logique du traitement en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à son égard (art. 15)
- Lorsque la personne présente sa demande par voie électronique, les informations demandées sont communiquées sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement (art. 12.3)

Droit d'opposition

- Le droit d'opposition pour motifs légitimes : toute personne physique a le droit de s'opposer pour des motifs légitimes à ce que des données personnelles la concernant fassent l'objet d'un traitement, sauf si celui-ci résulte d'une obligation légale. Le responsable d'un traitement auprès duquel un droit d'opposition a été exercé doit informer sans délai de cette opposition tout autre responsable de traitement qu'il a rendu destinataire des données personnelles qui font l'objet de l'opposition (art 21)
- Le droit d'opposition non subordonné aux motifs légitimes : toute personne physique a le droit de s'opposer, quels qu'en soient les motifs, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale. Les personnes concernées doivent être en mesure d'exprimer leur opposition avant la validation définitive de leurs réponses

Droit de rectification

- Toute personne physique justifiant de son identité peut demander au responsable de traitement de rectifier les données personnelles la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite (art. 16)
- Lorsque les données ont été transmises à un tiers, le responsable de traitement ayant procédé à leur rectification doit également en informer ce destinataire sans délai, lequel doit à son tour modifier son traitement.

Droit à l'effacement (

- Toute personne peut demander l'effacement de ses données personnelles par le responsable de traitement (art. 17) lorsque :
 - a) les données ne sont plus nécessaires au vu des finalités pour lesquelles elles ont été collectées ;
 - b) la personne concernée retire son consentement (lorsque celui-ci constituait la base juridique du traitement) et il n'existe pas d'autre fondement juridique au traitement ;
 - c) la personne concernée s'oppose à un traitement basé sur l'exécution d'une mission d'intérêt public ou sur des intérêts légitimes, pour des raisons tenant à sa situation particulière, et il n'existe pas de motif légitime impérieux pour le traitement ;
 - d) la personne concernée s'oppose au traitement de ses données à des fins de prospection ;
 - e) les données ont été traitées de manière illicite ;
 - f) la loi applicable requiert l'effacement de ces données ;
 - g) les données ont été collectées en lien avec les offres de services de la société de l'information et concernent un enfant.

Droit à l'effacement (

- Lorsque le responsable de traitement a rendu les données publiques et est obligé de les effacer, il doit prendre des mesures raisonnables au vu de la technologie disponible et des coûts de mise en œuvre, pour informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel ou toute copie ou reproduction de celles-ci.
- Le droit à l'oubli ne s'applique pas si la conservation des données est nécessaire à l'exercice du droit à la liberté d'expression, au respect d'une obligation légale de conserver les données ou à l'exécution d'une tâche d'intérêt public, dans le domaine de la santé publique ou pour des besoins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ou pour l'établissement, l'exercice ou la défense de droits en justice.

Droit à la limitation du traitement

- La personne concernée a le droit d'obtenir du responsable de traitement la limitation du traitement (art. 18) lorsque
 - a) L'exactitude des données est contestée par la personne concernée, pendant une durée permettant au responsable de traitement de vérifier l'exactitude des données ;
 - b) Le traitement est illicite ;
 - c) Le responsable de traitement n'a pas besoin des données mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
 - d) La personne concernée s'est opposée à un traitement basé sur l'exécution d'une mission d'intérêt public ou sur des intérêts légitimes, pour des raisons tenant à sa situation particulière, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable de traitement prévalent sur ceux de la personne concernée.

- Lorsque le traitement a été ainsi limité, les données personnelles ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public.

Droit à la portabilité (

- Le droit à la portabilité permet à une personne de recevoir les données personnelles la concernant, dans un format structuré, couramment utilisé et lisible par machine (art. 20)
 - La personne concernée peut, par la suite,
 - transmettre ces données à un autre responsable de traitement ou,
 - lorsque cela est techniquement possible, demander que les données personnelles soient transmises par le responsable de traitement directement au nouveau responsable de traitement.
- Celui qui détient les données ne peut s'opposer à la mise en œuvre de ce droit, qui s'exerce à titre gratuit (art. 12.5)
- La présence de données relatives à des tiers (faisant souvent partie de l'entourage de la personne concernée, à l'exemple d'un carnet de contacts) dans les données demandées dans le cadre d'une portabilité ne peut justifier en elle-même un rejet de la demande de portabilité.

Droit à la portabilité (

- L'exercice de ce droit à la portabilité est précisément encadré :
 - Il ne peut s'appliquer qu'à des données contenues dans des traitements automatisés, ce qui exclut les données contenues dans les fichiers dits « papiers »;
 - Il ne peut s'appliquer qu'à des données personnelles traitées sur la base du consentement de la personne concernée ou dans le cadre d'un traitement nécessaire à l'exécution d'un contrat passé par elle. Ainsi, les données personnelles traitées sur la seule base de l'intérêt légitime du responsable de traitement ne peuvent faire l'objet d'une demande de portabilité
- Les lignes directrices du G29 sur « le droit à la portabilité » du 5 avril 2017 ont notamment précisé l'étendue des données concernées par ce droit. Celui-ci s'applique aux données fournies par la personne concernée c'est-à-dire transmises au responsable de traitement ou les données générées par l'activité de la personne concernée.

Droit d'opposition au profilage (

- La personne concernée a le droit de ne pas être soumise à une décision résultant exclusivement d'un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire, ainsi que le « profilage » (art. 22)
 - Le « profilage » s'entend par toute forme de traitement automatisé de données à caractère personnel visant à évaluer certains aspects personnels liés à une personne physique, notamment par l'analyse et la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles ou les intérêts, la fiabilité ou le comportement, ou la localisation et les déplacements (art. 4).
- Ce droit ne s'applique pas lorsque (exceptions):
 - a) la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement,
 - b) la décision est autorisée par la législation de l'Union ou d'un État membre à laquelle le responsable du traitement est soumis;
 - c) la décision est fondée sur le consentement explicite de la personne concernée.

Droit d'opposition au profilage (

- Ces exceptions au droit d'opposition ne s'appliquent pas lorsque les décisions automatisées sont fondées sur un traitement de données sensibles (au sens de l'article 9)
 - sauf si la personne a donné son consentement explicite, ou
 - que celui-ci soit exclu par le droit de l'Union ou la loi de l'État membre, ou
 - que le traitement est considéré comme nécessaire pour des raisons d'intérêt public sur le fondement du droit de l'Union ou de la loi de l'État membre
- Lorsque ce droit d'opposition (aux décisions individuelles automatisées et au profilage) ne s'applique pas, la personne a le droit d'obtenir une intervention humaine de la part du responsable du traitement, et ce afin d'exprimer son point de vue et de contester la décision.

Droit d'introduire une réclamation

- Toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du règlement (art. 77)
 - La personne peut introduire cette réclamation auprès de l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise.

Modalités de réponse à une demande (1)

Délais de réponse à une demande d'exercice d'un droit (art. 12.3)

- Les informations sur les mesures prises à la suite d'une demande formulée doivent être communiquées dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande.
- Ce délai peut être prolongé de deux mois au besoin, compte tenu de la complexité et du nombre des demandes. Dans ce cas, la personne concernée doit être spécialement informée des motifs du report, dans un délai d'un mois à compter de la réception de la demande.
- Si le responsable du traitement ne donne aucune suite à la demande formulée par la personne concernée, il informe celle-ci des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle, et cela sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande.

Modalités de réponse à une demande (2)

Principe de gratuité (art. 12.5)

- Le responsable ne peut exiger aucun paiement pour procéder à toute communication et prendre toute mesure nécessaire à l'exercice des droits des personnes concernées
- Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives (ex. caractère répétitif) le responsable peut
 - soit exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées
 - soit refuser de donner suite à ces demandes (en démontrant le caractère manifestement infondé ou excessif de la demande)

Plan de la formation

- 1 Contexte et vue d'ensemble du GDPR
- 2 Principes, définitions et champs d'application
- 3 Projet de mise en conformité
- 4 Principes relatifs aux traitements de données
- 5 Droits des personnes concernées
- 6 Obligations et responsabilités des acteurs du traitement
- 7 Méthodologies et outils du consultant

Obligations et responsabilités

Le principe de responsabilisation (« accountability ») impose indirectement aux responsables de traitements et/ou sous-traitants la mise en place d'un **système de management de la protection des données à caractère personnel**

1	MAINTENIR UNE ORGANISATION INTERNE LIÉE À LA PROTECTION DES DONNÉES		
2	MAINTENIR UN INVENTAIRE DES TRAITEMENTS	3	VÉRIFIER LA CONFORMITÉ DES TRAITEMENTS
4	MAINTENIR DES DOCUMENTS SUPPORT	5	COMMUNIQUER, SENSIBILISER ET FORMER
6	GÉRER LES RÉCLAMATIONS ET LES CONTENTIEUX	7	GÉRER LES RISQUES DES TIERS
8	GÉRER LES RISQUES DE SÉCURITÉ DE L'INFORMATION	9	GÉRER LES VIOLATIONS DE DONNÉES
10	SUPERVISER ET CONTRÔLER LA CONFORMITÉ		

Maintenir une organisation interne

Obligations

- Obligation de désigner un délégué à la protection des données (DPO) en fonction de la nature des traitements mis en œuvre (art. 37 et 38)
- Obligation de formaliser les responsabilités des différents acteurs (art. 39)

Activités (exemples)

- Désigner un Délégué à la Protection des Données (DPO) en formalisant une lettre de mission
- Définir les moyens et le budget alloués au DPO
- Définir un réseau de référents à la protection des données dans les directions et/ou entités de l'organisation
- Formaliser une politique de protection des données à caractère personnel (interne et/ou externe), intégrant notamment les rôles et responsabilités des différents acteurs

Désignation du DPO (6)

- Un responsable de traitement ou un sous-traitant doit obligatoirement désigner un Délégué à la protection des données (DPO, Data Protection Officer) (art. 37 et lignes directrices du G29 du 13/12/2016):
 1. Lorsque le traitement est effectué par une autorité ou un organisme public
 2. Lorsque les activités de base consistent en des traitements 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
 - « activités de base » : le traitement de données patients par un hôpital, une entreprise en charge de la sécurité de lieux accueillant du public ...
 - « à grande échelle » : chaînes de restaurant exploitant les données de géolocalisation de leurs clients, les données traitées à des fins de publicité comportementale par un moteur de recherche, les données traitées par des fournisseurs d'accès à internet
 - « suivi régulier et systématique » : la fourniture de services de télécommunications, l'email retargeting, le profiling et le scoring visant à par exemple à évaluer les risques de fraudes, le suivi de la localisation, notamment via des applications mobiles, la publicité comportementale, le suivi des indicateurs de bien-être ou de santé via des objets connectés, les voitures connectées, etc.
 3. Lorsque les activités de base consistent en des traitements à grande échelle de données sensibles (art. 9) ou de données relatives à des condamnations et infractions pénales
- La désignation d'un DPO est recommandée dans les autres cas ...

Désignation du DPO (7)

- Un groupe d'entreprises peut désigner un seul DPO à condition que celui-ci soit joignable à partir de chaque lieu d'établissement.
- Le DPO doit être désigné sur la base de ses compétences en droit, en matière de protection des données, et sur sa capacité à remplir sa mission.
 - Soit un membre du personnel
 - Soit une personne exerçant ses missions sur la base d'un contrat de service (ex. avocat, cabinets spécialisé ...)
- Le responsable de traitement ou le sous-traitant doit publier les coordonnées du DPO et les communiquer à l'Autorité de contrôle

Fonction du DPO

Le DPO doit être associé à toutes les **questions** relatives à la protection des données à caractère personnel

Le DPO doit disposer des **ressources nécessaires** pour exercer ces missions, et entretenir ses connaissances spécialisées

Le DPO est soumis au **secret professionnel** ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions

Le DPO ne doit pas exercer par ailleurs des fonctions ou des activités susceptibles de provoquer un **conflit d'intérêts** avec l'exercice de ses missions

Le DPO ne doit recevoir **aucune instruction** en ce qui concerne l'exercice des missions, et **reporte au niveau le plus élevé** de la direction

Statut et responsabilités du DPO

- Le DPO ne bénéficie pas du statut de salarié protégé qui est réservé aux seuls représentants du personnel
 - Le DPO ne peut être relevé de ses fonctions ou pénalisé du fait de l'exercice de ses missions (sauf, probablement, en cas de manquements graves dûment constatés et qui lui sont directement imputables)
- La désignation d'un DPO n'emporte pas transfert à celui-ci de la responsabilité pénale qui incombe au responsable du traitement
 - La mise en place d'une délégation de pouvoir serait sans effet, les fonctions de DPO étant incompatibles avec celles de responsable du traitement.
 - En principe, seul le responsable du traitement est pénalement responsable en cas de violation des dispositions (sauf si une complicité punissable peut être établie)

Missions du DPO (1)

Les missions légales définies par l'art. 39

1

une mission d'avis et de conseil

- Informer et conseiller le responsable du traitement ou le sous-traitant (et ses salariés) sur les obligations qui leur incombent en vertu du GDPR et d'autres dispositions en matière de protection des données
- Conseiller le responsable de traitement dans la réalisation des analyses d'impact relative à la protection des données (PIA)

une mission de contrôle

2

- Contrôler la conformité des traitements au GDPR, à d'autres dispositions (de l'UE ou de l'État membre concerné) en matière de protection des données et aux règles internes (répartition des responsabilités, sensibilisation et formation du personnel participant aux traitements, audits ...)

une mission de point de contact avec l'Autorité de contrôle

3

- Etre le point de contact de l'autorité de contrôle sur les questions liées au traitement de données à caractère personnel (notamment pour la consultation préalable suite à une analyse d'impact relative à la protection des données)
- Coopérer avec l'Autorité de contrôle

Missions du DPO (2)

- Au-delà des missions légales (minimum), le DPO peut se voir confier d'autres missions concernant la protection des données
 - Ces missions confiées au DPO doivent faire l'objet d'une formalisation (ex. lettre de mission DPO)

Organisation de la gestion de la conformité GDPR

- Identifier les sources (personnes, services) potentielles de traitements au sein de l'entreprise/collectivité
- Identifier et recenser les traitements
- Définir et mettre en œuvre les procédures et l'organisation relative à la conformité
- Mettre en place une procédure d'échange d'information pour toute évolution ou nouveau traitement

Instruction des demandes et réclamations

- Collecter et transmettre les demandes et les réclamations des personnes concernées
- Mettre en place une procédure de suivi et de réponse dans le délai imparti
- Informer le responsable des traitements sur l'état des lieux des plaintes et des requêtes et de leurs instructions

Élaboration et suivi du registre des traitements

- Établir la fiche pour l'identification des traitements
- Mettre à jour la fiche en fonction des évolutions des traitements
- Émettre les recommandations nécessaires à la mise en conformité des informations contenues dans le registre
- Assurer l'accessibilité du registre de traitement (ou liste des traitements) et sensibiliser les salariés

Elaboration d'un Compte-rendu d'activité

- Décrire son activité au sein d'un bilan annuel incluant les demandes et réclamations
- Présenter ses actions futures et les recommandations
- Négocier les moyens nécessaires à la mise en œuvre des actions

Maintenir un inventaire des traitements

Obligations

- Obligation pour les organisations (>250 employés ou risques sur la vie privée) de tenir à jour un registre des activités de traitements (art. 30)

Activités (exemples)

- Définir un modèle de fiche de registre intégrant à minima l'ensemble des informations visées à l'art. 30
- Réaliser un inventaire initial des traitements de données mis en œuvre, et les porter au registre des activités des traitements
- Définir et mettre en place une procédure pour la remontée des informations associées aux nouveaux traitements ou à la modification des traitements existants

Registre des activités de traitement

- Obligation de tenir un registre des activités de traitement effectuées sous la responsabilité du responsable de traitement ou par le sous-traitant (art. 30)
 - Exception pour les organisations <250 salariés, sauf risque sur les droits/libertés, ou traitement non occasionnel ou données sensibles ou relatives à des condamnations
 - Définition du contenu des registres en fonction de la qualité de responsable de traitement ou de sous-traitant : nom et coordonnées (y compris du DPO), finalité, catégories de personnes et données, catégories des destinataires, transfert hors UE, délais d'effacement, description générale des mesures de sécurité techniques et organisationnelles, ...
 - Obligation de mettre le registre à la disposition de l'autorité de contrôle sur demande.

Vérifier la conformité des traitements

Obligations

- Obligation de respecter pour chaque traitement les « principes relatifs au traitements des données à caractère personnel » (art. 5.2)
- Obligation d'intégrer la protection des données dès la conception et par défaut (art. 25)

Activités (exemples)

- Définir et mettre en œuvre une procédure d'analyse de la conformité (des traitements existants et des nouveaux traitements) au regard des principes relatifs aux traitements
 - Réaliser une évaluation de la conformité des traitements sur l'ensemble des traitements existants
 - Intégrer l'activité d'analyse de la conformité des traitements dans le cycle de vie des projets de l'organisation

« Privacy by design & by default »

- Obligation pour le responsable de traitement de mettre en œuvre les mesures techniques et organisationnelles, compte tenu des risques du traitement, nécessaires au respect de la protection des données personnelles **dès la conception** du produit ou du service (art. 25.1)
 - Cette obligation consiste notamment à veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »)
- Obligation pour le responsable de traitement d'adopter des mesures consistant à limiter **par défaut** le traitement de données à caractère personnel à ce qui est strictement nécessaire, en ce qui concerne la quantité de données traitées, leur accessibilité et leur période de conservation (art. 25.2)
- Possibilité d'avoir recours à un mécanisme de certification approuvé (conformément à l'art. 42) afin de démontrer le respect de ces obligations

« privacy Impact Assessment »

- Obligation de réaliser pour les « traitements à risque », **une analyse d'impact sur la protection des données à caractère personnel** afin de déterminer les mesures appropriées à prendre et démontrer la conformité à la réglementation européenne (art. 35.1)
 - Les « **traitements à risques** » sont définis comme les traitements qui compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (en particulier par le recours à de nouvelles technologies)
- Liste (non-exhaustive) d'**hypothèses où l'analyse d'impact** est requise (art. 35.3)
 - **L'évaluation systématique des aspects personnels** propres à des personnes physiques, sur la base d'un traitement automatisé, incluant le profilage, et sur laquelle sont fondées des décisions produisant des effets juridiques les concernant ou les affectant gravement
 - **Le traitement à grande échelle des catégories de données sensibles** visées à l'article 9.1 ou des données relatives à des condamnations pénales et à des infractions visées à l'article 10
 - **La surveillance systématique à grande échelle** d'une zone accessible au public

(Guide G29 précisant l'obligation de réaliser une analyse d'impact (DPIA) lorsque le traitement correspond à au moins 2 critères sur une liste de 10 critères définis)

Critères de réalisation d'un PIA

PIA obligatoire

1. L'Autorité de Contrôle l'exige (liste publiée)
2. Le traitement remplit au moins 2 des critères suivants :
 - a. Evaluation/scoring (y compris le profilage) ;
 - b. Décision automatique avec effet légal ou similaire ;
 - c. Surveillance systématique ;
 - d. Collecte de données sensibles ;
 - e. Collecte de données personnelles à large échelle ;
 - f. Croisement de données ;
 - g. Personnes vulnérables (employés, patients, personnes âgées, enfants, etc.) ;
 - h. Usage innovant (utilisation d'une nouvelle technologie) ;
 - i. Exclusion du bénéfice d'un droit/contrat.

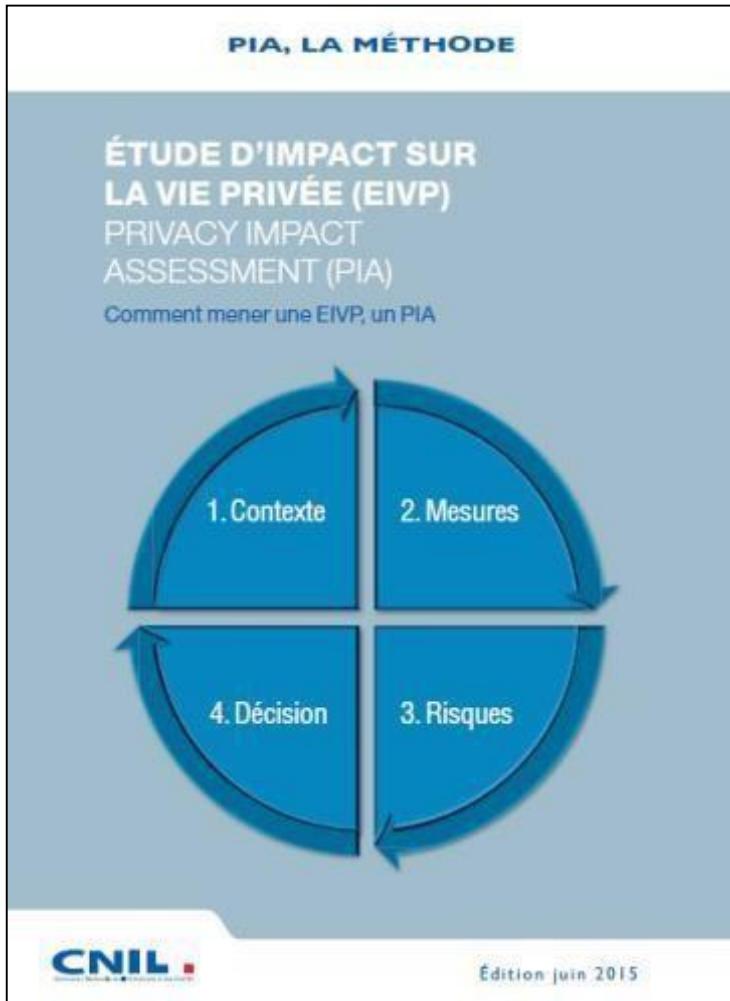
PIA non-obligatoire

1. Le traitement ne présente pas de risque élevé pour les droits et libertés des personnes concernées.
2. La nature, la portée, le contexte et les finalités du traitement envisagé sont très similaires à un traitement pour lequel un PIA a déjà été mené.
3. Le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public qu'il ait une base juridique, que ce droit réglemente cette opération de traitement et qu'un PIA ait déjà été menée lors de l'adoption de cette base juridique.
4. Le traitement correspond à une exception déterminée par l'Autorité de contrôle

Méthodologie et contenu d'un PIA

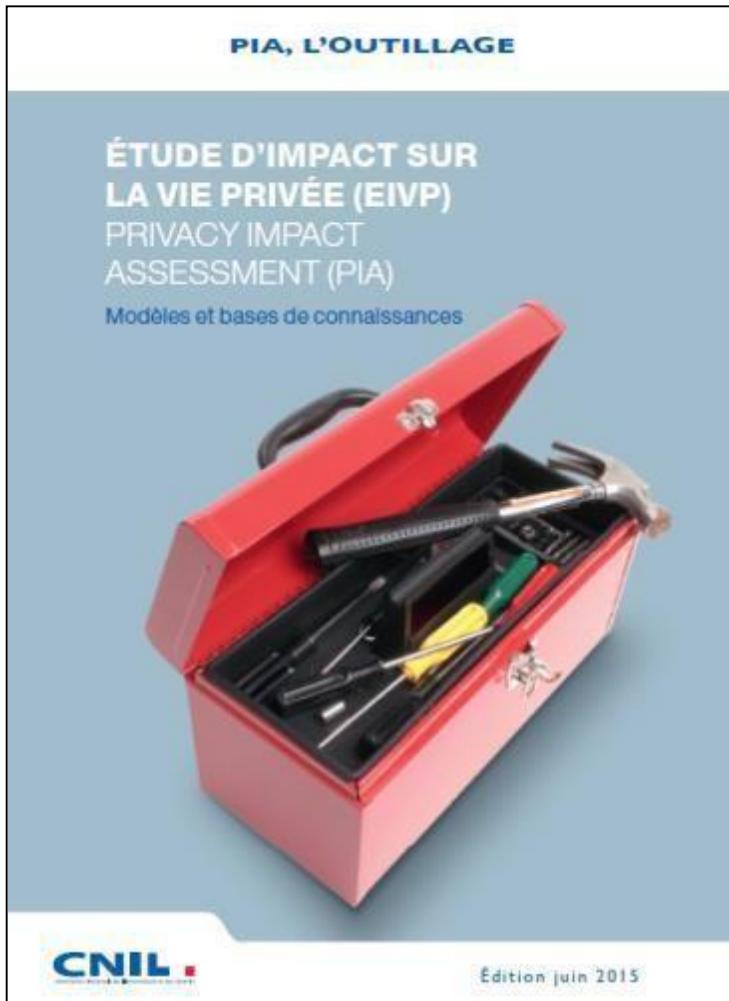
- Contenu de l'analyse d'impact (art. 35.7)
 - Une **description systématique des activités** traitements envisagés et des finalités poursuivies (et le cas échéant, une description des intérêts légitimes poursuivis par le responsable)
 - Une **analyse de la nécessité et de la proportionnalité** des activités de traitement au regard des finalités poursuivies
 - Une **évaluation du risque** pour les droits et libertés des personnes concernées
 - Les **mesures envisagées pour atténuer ce risque** y compris les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité du traitement avec le règlement, en tenant compte des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées
- Implication du délégué à la protection des données (DPO) pour conseiller le responsable de traitement (art. 35.2)

Guide « EIVP » publiés par la CNIL (1)



- Guide décrivant la manière d'employer la méthode EBIOS dans le contexte spécifique « Informatique et libertés »
- Etude d'impact sur la vie privée (PIA) visant :
 - Le **respect des principes juridiques** en matière de protection de la vie privée
 - La **gestion des risques liés à la sécurité** des DCP et ayant un impact sur la vie privée des personnes concernées

Guides « EIVP » publiés par la CNIL (2)



- Guide fournissant des modèles et des bases de connaissance pour réaliser une étude PIA
 - Outilage pour **l'étude de contexte** : description des données, des supports ...
 - Outilage pour **l'étude des mesures** : mesures de nature juridique et mesures de sécurité
 - Outilage pour **l'étude des risques** : sources de risques, événements redoutés, menaces, risques
 - Outilage pour la **validation du PIA** : évaluation des mesures de nature juridique et des risques résiduels

Outil PIA publié par la CNIL



- Outil open source publié par la CNIL en nov. 2017 (version bêta)
 - Description du traitement
 - Evaluation de la conformité aux principes fondamentaux
 - Evaluation des mesures/risques de sécurité

Consultation de l'Autorité et révision

- Obligation de **consulter l'autorité de contrôle** si le responsable de traitement **ne parvient pas à réduire le risque élevé** par des mesures appropriées (art. 36.1) ou si le **droit de l'Etat membre** l'exige (art. 36.5)
 - Le responsable doit communiquer à l'Autorité de contrôle différentes informations relatives au traitement : finalités, mesures et garanties prévues, coordonnées du DPO, analyse d'impact et tout autre information demandée par l'autorité (art. 36.3)
 - L'Autorité de contrôle dispose d'un délai de huit semaines (pouvant être prolongé de six semaines si la complexité du traitement l'exige) pour conseiller le responsable du traitement si elle estime qu'il n'a pas suffisamment identifié ou atténué le risque inhérent au traitement (art. 36.2)
 - Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandé pour les besoins de la consultation (art. 36.2)
- Mettre en place une procédure de révision afin de s'assurer que le traitement soit effectué conformément à l'analyse d'impact (art. 35.11)
 - Revue à réaliser au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Maintenir des documents supports

Obligations

- Obligation de respecter et être en mesure de démontrer le respect des principes relatifs aux traitements de données (art. 5.2)

Activités (exemples)

- Définir les mentions d'information et modèles de recueil du consentement des personnes concernées
 - Mention d'information générale concernant la mise en œuvre d'un traitement de données personnelles, mention à intégrer au bas d'un formulaire de collecte des données personnelles, mention d'information en cas de transfert de données en dehors de l'UE, mention relative à la mise en œuvre d'un dispositif de vidéosurveillance
- Définir des modèles de clause de confidentialité
 - Engagement de confidentialité relatif aux données à caractère personnel à destination du personnel, clause de confidentialité en cas de sous-traitance ...
- Définir les clauses contractuelles « standards » en matière de protection des données à caractère personnel pour la sous-traitance

Communiquer, sensibiliser et former

Obligations

- Obligation de sensibilisation et de formation du personnel participant aux opérations de traitement de données à caractère personnel (art. 39)
- Obligation générale de transparence et d'information des personnes concernées par les traitements (art. 12, 13 et 14)

Activités (exemples)

- Réaliser des actions de communication spécifiques à destination du personnel et des IRP
- Réaliser des actions de sensibilisation/formation à destination des acteurs internes susceptibles de participer aux opérations de traitements de données à caractère personnel
- Mettre en place un outil de communication externe (politique de l'organisation, contact DPO, mentions d'information ...)

Gérer les réclamations / contentieux (

Obligations

- Obligation de mettre en œuvre les mesures appropriées pour procéder à l'exercice des droits (accès, rectification, effacement ...) des personnes concernées (art. 12)
 - Objectif pour le responsable de traitement / sous-traitant de réduction des risques de non-conformité associés au respect de droits des personnes ou au modalités d'exercice de ces droits (délais de réponse, contenu des communications ...)
- Obligation générale de coopération avec l'Autorité (art. 31) en cas de demande ou de contrôle
 - Objectif pour le responsable de traitement / sous-traitant de réduction des risques de contentieux engagés par l'Autorité en cas d'absence ou défaut de communication/coopération

Gérer les réclamations / contentieux (

Activités (exemples)

- Définir et mettre en œuvre une procédure de gestion des réclamations et des demandes relatives à l'exercice des droits des personnes (accès, rectification, effacement ...) comprenant a minima les modalités d'exercice, les rôles et responsabilité et les délais de communication
 - Rédiger des modèles de réponse aux demandes et réclamations des personnes concernées par le traitement (en fonction des métiers)
 - Mettre en place un tableau de pilotage et de suivi des réclamations et des demandes relatives à l'exercice des droits de personnes
- Définir et mettre en œuvre une procédure de gestion des demandes et des contrôles de l'Autorité de contrôle intégrant à minima les rôles et responsabilités, les modalités et règles applicables et le suivi/contrôle par le DPO dans le cadre des demandes adressées par le service des plaintes de l'autorité, d'un contrôle réalisé par l'autorité ou d'une procédure contentieuse engagée par l'autorité

Gérer les risques des tiers

Obligations

- Obligation de contractualisation des activités des sous traitants sur les traitements des données à caractère personnel l'objet (art. 28)
 - Objectif pour le responsable de traitement / sous-traitant de réduction des risques de non-conformité liés à l'absence/défaut de contractualisation et du non-respect de la réglementation par les sous-traitants

Activités (exemples)

- Identifier l'ensemble des sous-traitants traitant des données à caractère personnel pour le compte du Groupe (à partir des bases de contrats et de l'inventaire des traitements)
- Revoir et mettre à jour pour chaque sous-traitant les obligations contractuelles en matière de protection de données à caractère personnel conformément aux dispositions du règlement

Contractualisation avec les sous-traitants

- Le responsable du traitement ne doit faire appel uniquement qu'à des sous-traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour le respect du règlement.
- Le traitement par un sous-traitant est régi par un contrat écrit ou un autre acte juridique précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du règlement :
 - Objet et durée du traitement
 - Nature et finalité du traitement
 - Types de données personnelles
 - Catégories des personnes concernées
 - Obligations et droits du responsable de traitement
 - Obligations et droits du sous-traitant

Obligations du sous-traitant

1. Une obligation de transparence et de traçabilité

Agir sur instruction documentée du responsable de traitement

Demander l'autorisation écrite préalable avant le recrutement d'un sous-traitant (sous-traitant du sous-traitant)

Mettre à la disposition toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits

2. La prise en compte des principes de protection des données dès la conception et par défaut

3. Une obligation de garantir la sécurité des données traitées

Soumettre les employés qui traitent les données à une obligation de confidentialité.

Notifier sans délai toute violation de ses données

Mettre en œuvre toutes les mesures de sécurité appropriées pour garantir un niveau de sécurité adapté aux risques

Au terme de la prestation (et selon les instructions du responsable de traitement) : supprimer toutes les données ou les renvoyer au responsable de traitement, et détruire les copies existantes (sauf obligation légale de les conserver)

4. Une obligation d'assistance, d'alerte et de conseil

- Alerter immédiatement le responsable du traitement en cas d'instruction supposée pouvant constituer une violation des règles en matière de protection des données

Aider le responsable de traitement dans la réponse aux demandes d'exercice des droits des personnes

Conseiller le responsable de traitement à garantir le respect des obligations en matière de sécurité du traitement, de notification de violation de données et d'analyse d'impact relative à la protection des données.

Gérer les risques de sécurité

Obligations

- Obligation de mettre en œuvre les mesures permettant de garantir une sécurité et une confidentialité appropriées des données personnelles et du traitement des données (art. 32)

Activités (exemples)

- Définir une procédure d'évaluation des risques (sur la vie privée) et d'identification/sélection des mesures de sécurité appropriées
 - Réaliser une évaluation des risques et mesures de sécurité pour les traitements existants
 - Intégrer l'activité d'évaluation des risques et d'identification/sélection des mesures de sécurité appropriées dans le cycle de vie des projets de l'organisation
- Définir et mettre en œuvre une procédure d'audit périodique de l'efficacité des mesures de sécurité

Obligation de sécurité (1)

- Obligation de mettre en œuvre les mesures permettant de garantir une sécurité et une confidentialité appropriées des **données personnelles et du traitement des données (art. 32)**
 - **Mention explicite du risque** en tant que critère principal pour la mise en œuvre des mesures techniques et organisationnelles appropriée
- Critères généraux d'appréciation des mesures appropriées (art. 32.1):
 - **L'état de l'art et les coûts de l'implémentation des mesures** de sécurité en tenant compte de la nature, la portée, le contexte et les finalités du traitement aussi bien que de la vraisemblance et de la gravité du risque d'atteinte aux droits et libertés de la personne concernée
 - **L'objet et l'origine du risque** (risques pour le traitement des données lui-même) : la destruction accidentelle ou illégale, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel transmises, stockées ou faisant l'objet d'un traitement de données

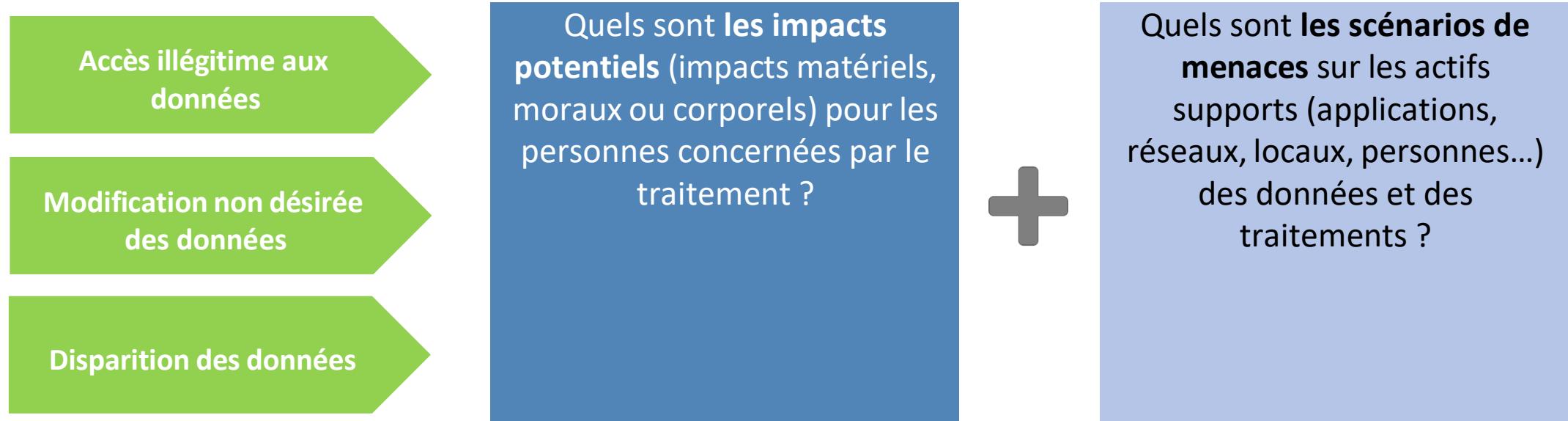
Obligation de sécurité (2)

- Enumération de **quatre catégories de mesures** qui pourront être, entre autres, appropriées selon les besoins (art. 32.1)
 - **Chiffrement et Pseudonymisation**
 - **Capacité d'assurer**, de manière permanente, **la confidentialité, l'intégrité, la disponibilité, et la résilience** des systèmes et des services de traitement
 - **Aptitude à restaurer la disponibilité et l'accès aux** données dans un délai raisonnable en cas d'incident physique ou technique
 - **Mise en place d'un processus régulier** de test et d'évaluation des mesures techniques et organisationnelles prises pour garantir la sécurité du traitement
- Possibilité d'appliquer un **Code de conduite** ou **mécanisme de certification** comme un élément pour démontrer la conformité aux exigences du devoir de sécurité (art. 32.3)

Recommandation de la CNIL

- La CNIL propose un ensemble de « recommandations » à destination des responsables de traitements pour garantir la sécurité des données
 - Guide « La sécurité des données personnelles »
 - Guides et outillage pour « l'étude d'impact sur la vie privée (PIA) », incluant notamment un guide des bonnes pratiques (mesures) pour traiter les risques
 - Délibération CNIL 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe
 - Check-list « Évaluer le niveau de sécurité des données personnelles de votre organisme »

Evaluation des risques



Outillage CNIL pour « l'étude d'impact sur la vie privée (PIA) » pouvant être utilisé pour l'évaluation des risques, et notamment « échelles et règles pour estimer les risques »

Sélection des mesures de sécurité

Check-list CNIL « Évaluer le niveau de sécurité des données personnelles de votre organisme » (51 mesures de sécurité génériques organisées en 17 chapitres) pouvant être utilisée pour identifier/sélectionner les mesures existantes et les contre-mesures requises en fonction des risques évalués

- 1. SENSIBILISATION DES UTILISATEURS
- 2. AUTHENTIFICATION DES UTILISATEURS
- 3. GESTION DES HABILITATIONS
- 4. TRAÇABILITÉ DES ACCÈS ET GESTION DES INCIDENTS
- 5. SÉCURISATION DES POSTES DE TRAVAIL
- 6. SÉCURISATION DE L'INFORMATIQUE MOBILE
- 7. PROTECTION DU RÉSEAU INFORMATIQUE INTERNE
- 8. SÉCURISATION DES SERVEURS
- 9. SÉCURISATION DES SITES WEB
- 10. SAUVEGARDE ET CONTINUITÉ D'ACTIVITÉ
- 11. ARCHIVAGE SÉCURISÉ
- 12. ENCADRER LA MAINTENANCE ET LA DESTRUCTION DES DONNÉES
- 13. GESTION DE LA SOUS-TRAITANCE
- 14. SÉCURISATION DES ÉCHANGES AVEC D'AUTRES ORGANISMES
- 15. PROTECTION DES LOCAUX
- 16. ENCADREMENT DES DÉVELOPPEMENTS INFORMATIQUE
- 17. UTILISATION DES FONCTIONS CRYPTOGRAPHIQUES

Gérer les violation de données

Obligations

- Obligation de notifier les violations de sécurité des données
 - à l'Autorité de contrôle (dans les meilleurs délais et 72 heures au plus tard après en avoir pris connaissance) et/ou
 - aux personnes concernées « en cas de risque élevé pour leurs droits et libertés » (dans les meilleurs délais)

Activités (exemples)

- Définir et mettre en œuvre une procédure de gestion des violations des données à caractère personnel (identification et qualification des violations, notification aux Autorités et/ou aux personnes concernées (modèles de communiqués), gestion de crises (responsabilités et critères d'escalade), ...)
- Définir et mettre en œuvre une procédure pour tenir à jour un registre des violations des données personnelles
- Mettre en place une architecture de journalisation et de surveillance des événements de sécurité

Notification à l'Autorité de contrôle (7)

- Définition de « violation de données à caractère personnel » comme « *Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données [...], ou l'accès non autorisé à de telles données* » (art. 4)
- Obligation pour **le responsable de traitement** de notifier toute violation de données à caractère personnel à l'Autorité de contrôle (art. 33.1)
 - **dans les meilleurs délais** et, si possible, **72 heures au plus tard** après en avoir pris connaissance
 - **sauf si la violation ne paraît pas faire courir de risque aux droits et libertés individuelles des personnes concernées**
- Obligation pour **le sous-traitant** de notifier le responsable de traitement de toute violation dans les meilleurs délais (art. 33.2)

Notification à l'Autorité de contrôle (8)

■ Contenu minimal de la notification (art. 33.3)

- La **nature de la violation** avec si possible, les catégories et le nombre approximatif de personnes et les catégories et le nombre approximatif d'enregistrements de données concernés
- Les **nom et coordonnées** du DPO ou d'un **autre point de contact** auprès duquel des informations supplémentaires peuvent être obtenues
- Les **conséquences probables de la violation** de données à caractère personnel
- Les **mesures prises ou que le responsable du traitement propose de prendre** pour remédier à la violation de données à caractère personnel (et notamment les mesures pour en atténuer les éventuelles conséquences négatives)

■ Obligation de tenir **un registre des toutes les violations de données à caractère personnel** » (art. 33.5)

- Conservation d'une trace documentée de chaque violation indiquant son contexte, ses effets et les mesures prises pour y remédier
- Mise à disposition de l'Autorité de contrôle pour vérifier le respect de l'obligation de notification

Communication aux personnes

- Obligation pour le responsable de traitement de **notifier à la personne concernée** les violations de données susceptibles d'exposer les personnes physiques à un risque élevé à leurs droits et libertés (art. 34.1)
 - **dans les meilleurs délais**
 - **dans des termes clairs et simples** au moins : la nature de la violation de données à caractère personnel, les conséquences probables, les mesures prises ou que le responsable propose de prendre, un point de contact (art. 34.2)
- **Exceptions** à l'obligation de communication aux personnes (art. 34.3) :
 - Mise en œuvre (en amont) de **mesures de protection** techniques et organisationnelles appropriées (ex. chiffrement)
 - Mise en œuvre des **mesures ultérieures** qui garantissent que le risque élevé n'est plus susceptible de se matérialiser
 - Risque d'entraîner des efforts disproportionnés (dans ce cas communication publique ou similaire pour informer les personnes)
- Possibilité pour l'autorité de contrôle d'exiger du responsable du traitement la communication de la violation des données à caractère personnel aux personnes concernées (art. 34.4)

Synthèse des obligations

Gravité de la violation



La violation est susceptible d'engendrer **un risque élevé pour les droits et libertés des personnes physiques**

La violation est susceptible d'engendrer **un risque pour les droits et libertés des personnes physiques**

Registre des violations

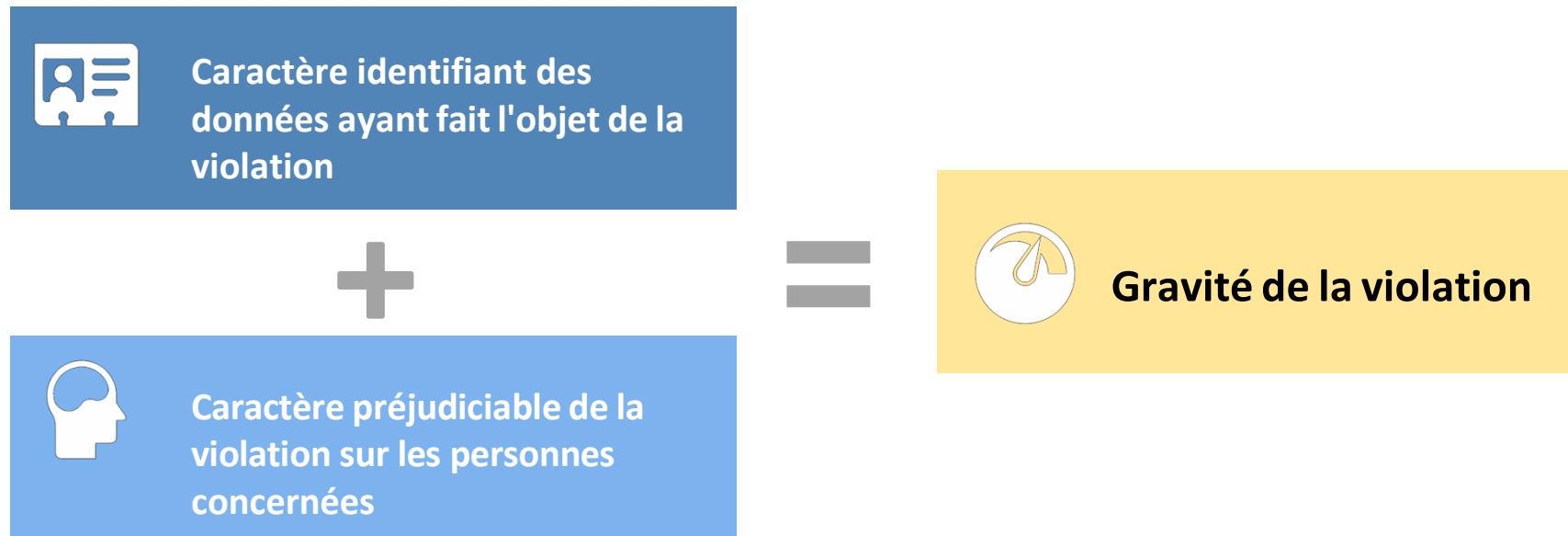
Notification à l'Autorité de Contrôle

La violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques

Registre des violations

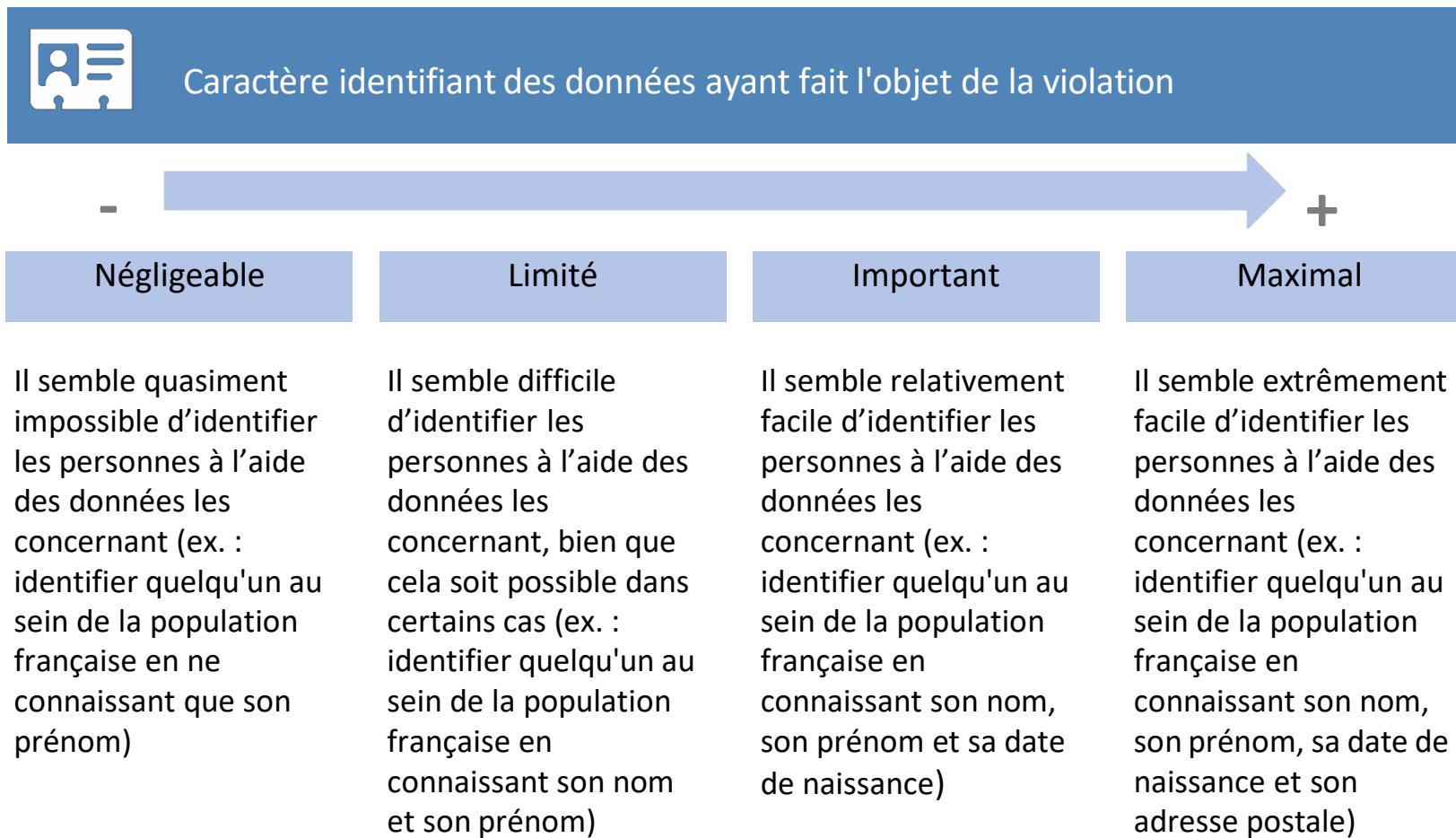
Evaluation de la gravité de la violation

L'évaluation de la gravité de la violation vise à déterminer si la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, et si celui constitue un risque élevé ou non



- La CNIL met à disposition un outil d'analyse (auto-évaluation) de la gravité d'une violation de données à caractère personnel
- Le G29 a adopté le 03/10/2017 des lignes directrices apportant des précisions et des exemples

Evaluation du caractère identifiant



Evaluation du caractère préjudiciable



Caractère préjudiciable de la violation sur les personnes concernées



Négligeable Limité Important Maximal

Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, simple contrariété...)

Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourraient surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, affection physique ou psychologique mineure...)

Les personnes concernées pourraient connaître des conséquences significatives, qu'elles pourraient surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, affection physique ou psychologique grave...)

Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée ou permanente, décès...)

Exemples de violations de données (

EXEMPLES	NOTIFICATION À L'AUTORITÉ DE CONTRÔLE	COMMUNICATION AUX PERSONNES CONCERNÉES	NOTES
Un responsable a stocké une sauvegarde chiffrée de données personnelles sur un CD-ROM. Le CD-ROM a été volé lors d'un cambriolage.	Non	Non	Tant que les données sont chiffrées avec un algorithme à l'état de l'art et que la clé de chiffrement n'est pas comprise, il n'est pas nécessaire de notifier la violation
Des données personnelles ont été dérobées lors d'une cyber-attaque sur un site Web sécurisé géré par le responsable de traitement.	Oui, si il y a des conséquences potentielles pour les personnes concernées	Oui, en fonction de la nature des données affectées et la sévérité des conséquences potentielles	L'obligation de communication aux personnes analysées dépend du cas d'espèce (ex. non-requis pour une newsletter liée à une émission TV, mais requis pour un point de vue politique)
Une brève coupure de courant de plusieurs minutes au niveau du centre d'appel avec pour conséquence que les clients ne peuvent pas appeler le responsable de traitement et accéder à leurs dossiers.	Non	Non	L'incident doit cependant être consigné/documenté dans le registre des violations
Un responsable de traitement subit une attaque de type « ransomware » entraînant le chiffrement de toutes les données. Aucune sauvegarde n'est disponible et les données ne peuvent être restaurées. Les investigations confirment que l'action du ransomware se limite au chiffrement, et qu'aucun autre malware n'est présent sur le système.	Oui, il y a des conséquences potentielles pour les personnes concernées en raison de la perte des données	Oui, en fonction de la nature des données affectées et des conséquences potentielles de la perte des données	S'il y avait eu une sauvegarde disponible et que les données pouvaient être restaurées en temps utile, il n'aurait pas été nécessaire de notifier la violation à l'Autorité ou aux personnes concernées.

Exemples de violations de données (

EXEMPLES	NOTIFICATION À L'AUTORITÉ DE CONTRÔLE	COMMUNICATION AUX PERSONNES CONCERNÉES	NOTES
Une personne contacte le Centre d'appel d'une banque pour signifier qu'il a reçu le relevé mensuel d'une autre personne Le responsable du traitement mène une enquête rapide (cad. dans les 24 heures) et établit avec une assurance raisonnable qu'une violation de données personnelles a eu lieu et qu'il s'agit d'un défaut systémique qui pourrait affecter d'autres personnes.	Oui	Seules les personnes affectées sont averties si cela représente un risque élevé et qu'il est clair que les autres personnes ne sont pas affectées par l'incident	Si après des investigations supplémentaires il est relevé que d'autres personnes sont affectées par l'incident, le responsable doit faire une mis-à-jour de sa notification à l'Autorité et informer ces autres personnes en cas de risque élevée
Un e-commerçant subit une cyberattaque, et les logins, mots de passe et historique des achats sont publiés en ligne par l'attaquant	Oui	Oui, cela pourrait entraîner un risque élevé	Le responsable de traitement doit prendre les mesures appropriées pour réduire le risques (ex. forcer la réinitialisation des mots de passe)
Une société d'hébergement de site Web (un sous-traitant) identifie une vulnérabilité permettant aux utilisateurs d'accéder aux détails des comptes de tous les autres utilisateurs.	En tant que sous-traitant, l'hébergeur doit informer ses clients concernés (les responsables de traitement) sans délai indu. Les responsables de traitement sont « informés » de la violation les concernant dès lors qu'ils ont été avisés par leur sous-traitants (sur la base des investigations réalisées par le sous-traitant). Les responsables de traitement doivent alors notifier l'Autorité de contrôle.	S'il n'y a probablement pas de risque élevé pour les personnes concernées, ils n'ont pas besoin d'être notifiés.	La société d'hébergement de site Web (sous-traitant) doit cependant tenir compte des autres obligations de notification (ex. directive NIS pour les fournisseurs de service numérique). S'il n'y a aucune preuve d'exploitation de cette vulnérabilité, le responsable de traitement peut ne pas notifier cette violation, mais doit l'inscrire sur le registre des violations.

Exemples de violations de données (

EXEMPLES	NOTIFICATION À L'AUTORITÉ DE CONTRÔLE	COMMUNICATION AUX PERSONNES CONCERNÉES	NOTES
Les dossiers médicaux sont indisponibles 30 heures en raison d'une cyberattaque	Oui, l'hôpital est tenu de notifier la violation à l'Autorité de contrôle en raison du risque élevé sur la santé et la vie privée des patients	Oui, communication aux personnes affectées par la violation.	
Les données personnelles de 5000 étudiants sont envoyées par erreur sur la mauvaise liste de diffusion avec plus de 1000 destinataires.	Oui	Oui, en fonction de la nature des données affectées et la sévérité des conséquences potentielles	
Un e-mail de marketing est envoyé aux destinataires dans le champ "to:" ou "cc:", permettant ainsi à chaque destinataire de voir l'adresse e-mail des autres destinataires	Oui, notifier l'Autorité de contrôle peut être obligatoire si un grand nombre de personnes est touché, si des données sensibles sont révélées (par exemple une liste de diffusion d'un psychothérapeute) ou si d'autres facteurs présentent des risques élevés (par exemple, le courrier contient les mots de passe initiaux).	Oui, en fonction de la nature des données affectées et la sévérité des conséquences potentielles	La notification peut ne pas être nécessaire si aucune donnée sensible n'est révélée et si seulement un nombre mineur d'adresses e-mail est révélé.

Superviser et contrôler la conformité

Obligations

- Obligation de mettre en œuvre les mesures pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à la réglementation (art. 5, 24 et 39)

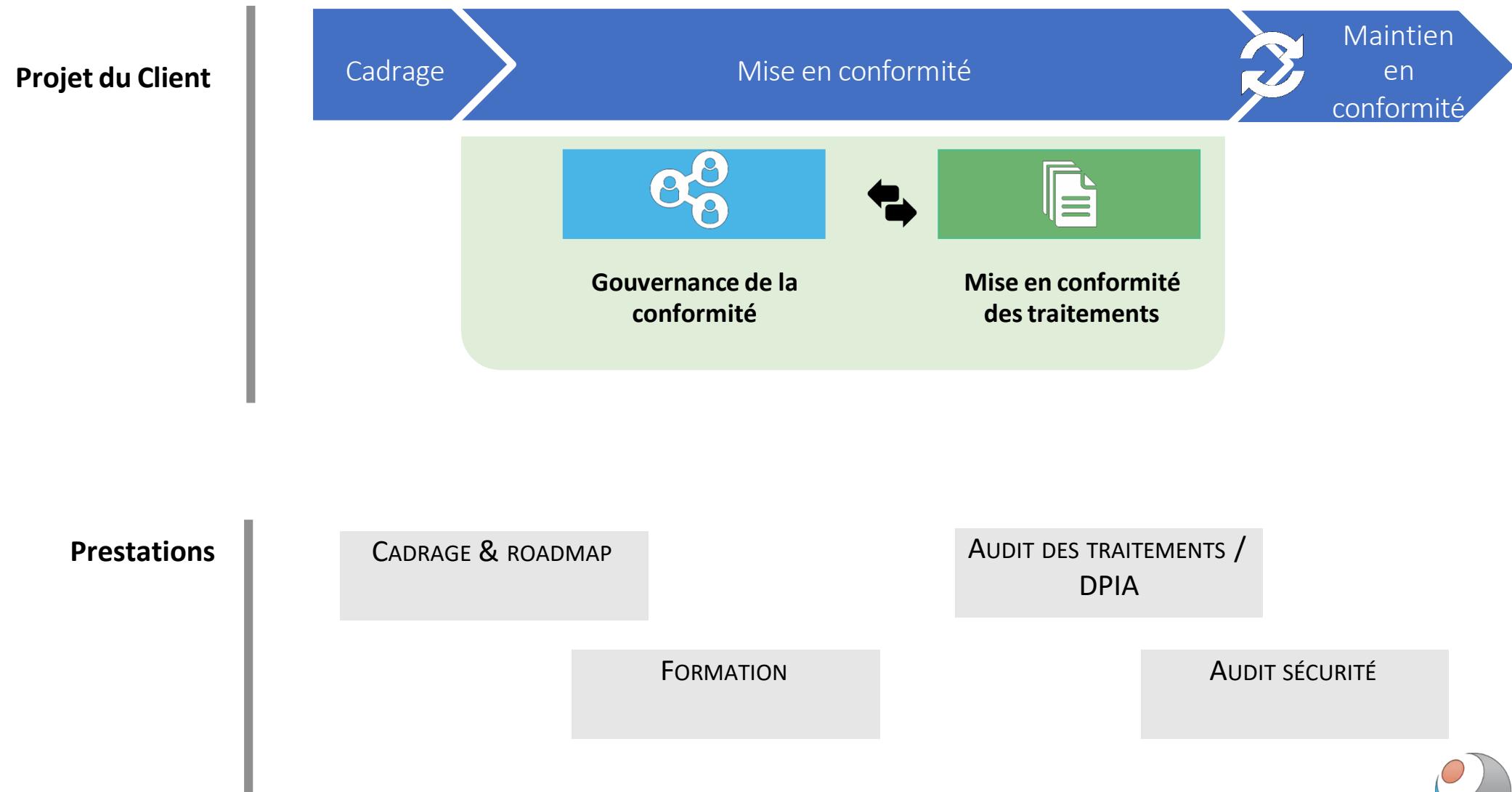
Activités (exemples)

- Organiser et planifier des opérations de contrôle interne
 - Définir la méthodologie et le référentiel d'audit de la protection des données à caractère personnel (label audit CNIL)
 - Planifier des opérations d'audit interne de la protection des données à caractère personnel (pour les traitements présentant les risques les plus importants)
- Organiser l'administration des preuves de conformité
 - Mettre en place un outil de gestion documentaire des preuves de conformité
 - Définir une procédure de gestion/conservation des preuves de conformité (information sur les traitements, modèles et clausiers, politique et procédures ...)

Plan de la formation

- 1 Contexte et vue d'ensemble du GDPR
- 2 Principes, définitions et champs d'application
- 3 Projet de mise en conformité
- 4 Principes relatifs aux traitements de données
- 5 Droits des personnes concernées
- 6 Obligations et responsabilités des acteurs du traitement
- 7 Méthodologies et outils du consultant

Prestations GDPR



Prestation Cadrage & roadmap (1)

Réunion de lancement et préparation de la mission



Activités

- Réunion de lancement avec le « Comité projet » (directions juridiques, risques & conformité, sécurité, système d'information)
- Récupération et analyse des documents existants : organisation & activités du client, formalités CNIL, politique et/ou procédure de sécurité informatique
- Identification des personnes à impliquer, et planification des interventions (entretiens et ateliers)



Outils & supports

- Supports de réunion de lancement utilisés

Prestation Cadrage & roadmap (2)



Activités

- Entretiens avec les représentants des directions/services du Client pour identifier (et caractériser) les principaux traitements :
 - Ressources Humaines
 - Services généraux
 - Marketing / Commerce
 - Achat
 - IT
 - Production / métier , etc.



Outils & supports

- Fiche de description des traitements
- Fiche d'entretien

Traitements types (exemples)

Ressources Humaines

- Gestion du personnel
- Gestion de la paie
- Gestion du recrutement
- Gestion des contentieux (personnel)
- Dispositif d'alertes professionnelles
- Gestion des activités sociales/culturelles du CE

Service IT

- Cyber-surveillance des salariés (proxy Internet, contrôle d'utilisation de la messagerie)
- Cyber-surveillance : logs de sécurité des systèmes et sites Web
- Gestion de la téléphonie

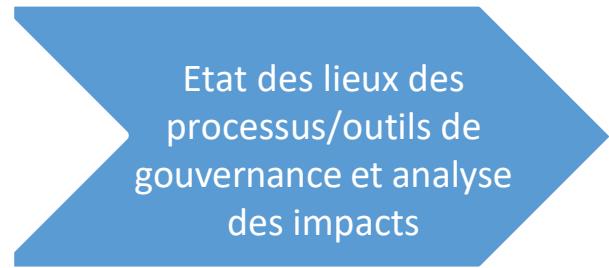
Service Généraux

- Contrôle d'accès sur les lieux de travail
- Vidéosurveillance des locaux

Production / métier

- Gestion des horaires de travail
- Géolocalisation des véhicules/salariés
- Ecoute et enregistrement des conversations téléphoniques
- Gestion de la traçabilité des actions de production

Prestation Cadrage & roadmap (3)



 Activités	 Outils & supports
<ul style="list-style-type: none">▪ Ateliers thématiques avec les interlocuteurs identifiés :<ul style="list-style-type: none">▪ Rappel des obligations et présentation des activités génériques associés▪ Identification des axes de mise en œuvre dans le contexte du Client▪ Entretiens complémentaires sur la base des résultats/travaux des ateliers	<ul style="list-style-type: none">▪ Exemples de supports d'ateliers thématiques utilisés dans les différents projets▪ Formation GDPR

Ateliers thématiques

1 Organisation de la gouvernance de la protection des données

- Rôles et responsabilités
- Délégué à la Protection des Données (DPO)

2 Procédures et outils transverses de gestion de la conformité

- Procédures et outils de gestion de la conformité
- Gestion des réclamations et du contentieux
- Sensibilisation, communication et formation des opérationnels

3 Sécurité des systèmes d'information et des données

- Sécurité des traitements et risques « privacy »
- Gestion des violations de données à caractère personnel

4 Système d'information et projets IT

- Intégration de la « Privacy » dans la gouvernance projet
- Impacts de l'évolution des droits des personnes sur l'IT
- Encadrement des relations contractuelles avec les sous-traitants

Le nombre et la nature des ateliers thématiques doivent être adaptés à la taille, l'organisation et le contexte du Client

Prestation Cadrage & roadmap (4)



Elaboration de la
roadmap de mise en
conformité



Activités

- Elaborer une proposition de « feuille de route de mise en conformité »
 - Identification, description et priorisation des actions de mise en conformité (organisation/procédures de gouvernance et actions d'évaluation/mise en conformité des traitements)
 - Proposition de planning et porteurs des actions
- Présenter et faire valider la proposition de « feuille de route »

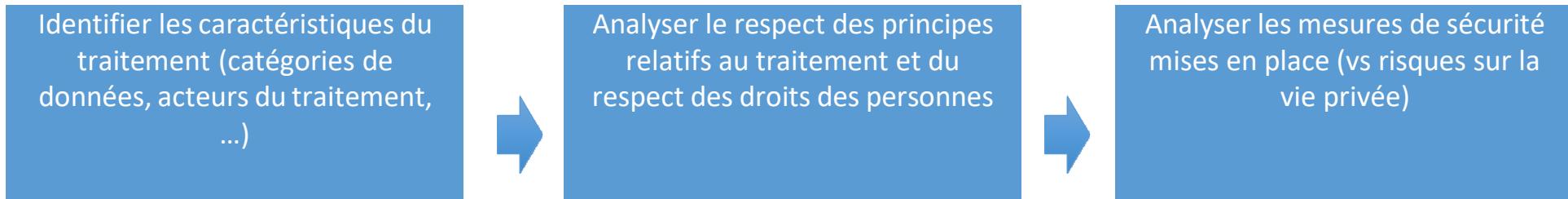


Outils & supports

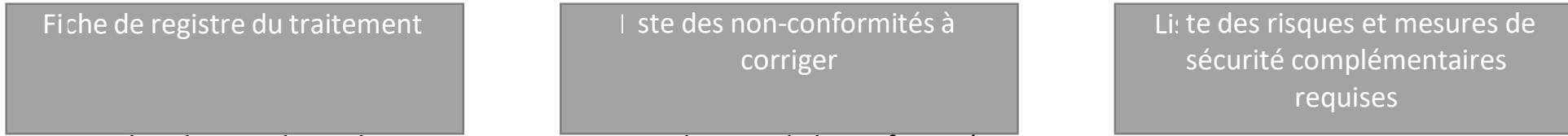
- Framework de « gouvernance » avec actions génériques à adapter/compléter
- Outil d'évaluation de la conformité
- (Autre Option : « Label Gouvernance » de la CNIL)

Audit des traitements / DPIA (

Etapes



Résultats



Activités

- | Etapes | Résultats | Activités |
|---|---|---|
| Identification des caractéristiques du traitement | Fiche de registre du traitement | 1. Atelier de travail avec les représentants métiers
2. Entretiens complémentaires avec les représentants métiers, représentants systèmes d'information et/ou sous-traitant |
| Analysis of principle respect | Liste des non-conformités à corriger | 1. Evaluation de la conformité aux principes / droits des personnes
2. Entretiens complémentaires avec les représentants métiers et/ou direction juridique
3. Validation par la direction juridique |
| Analysis of security measures | Liste des risques et mesures de sécurité complémentaires requises | 1. Entretiens avec représentants systèmes d'information, sécurité et/ou sous-traitant
2. Validation des risques avec représentants métiers et sécurité
3. Validation par la direction sécurité |

Audit des traitements / DPIA (

Identifier les caractéristiques du traitement (catégories de données, acteurs du traitement, ...)



Réaliser/documenter la description des caractéristique du traitements



Acteurs et responsabilités



Catégories des données et durées de conservation



Catégories de destinataires



Catégories de personnes concernées par le traitement



Données sensibles



Transferts de données hors de l'Union Européenne

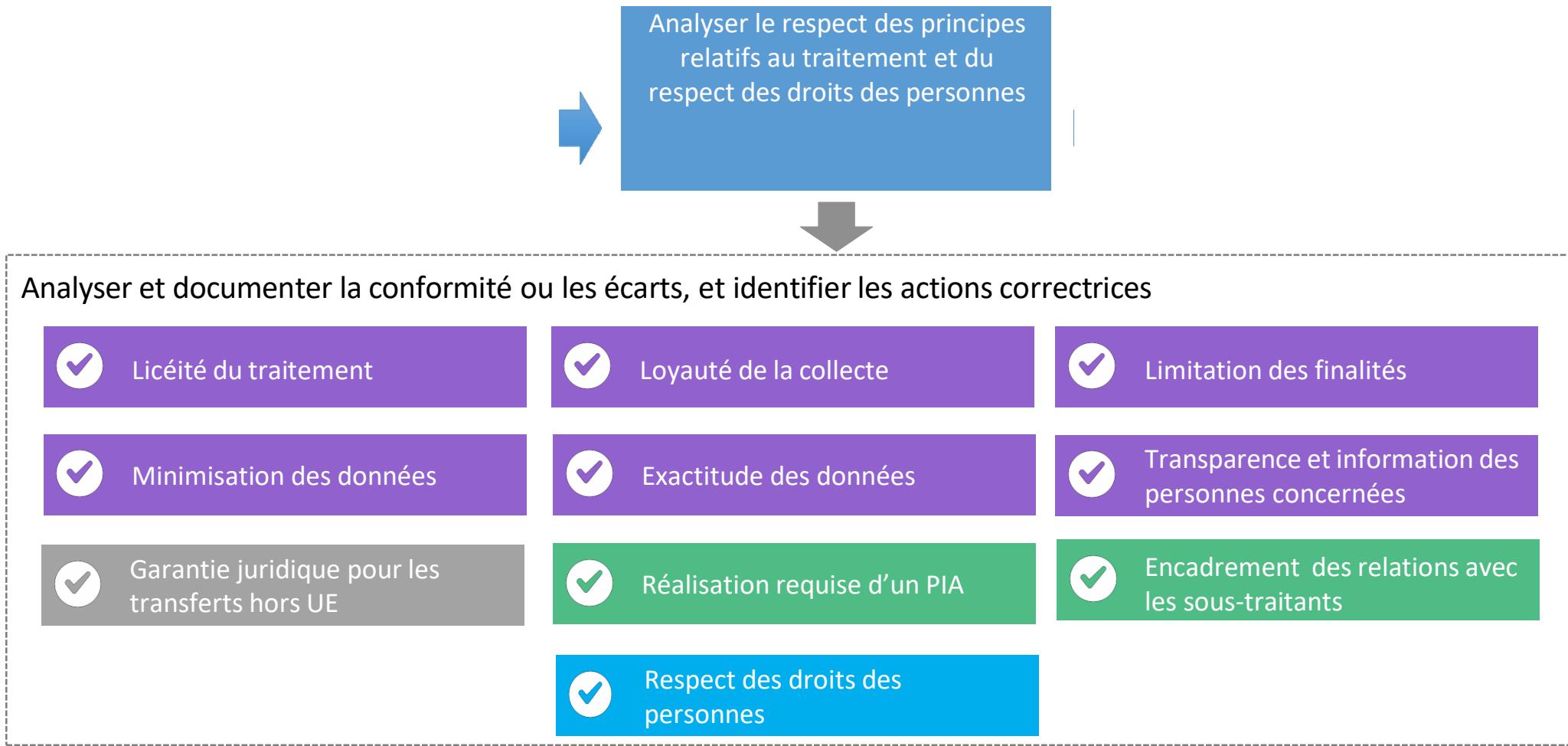


Description des opérations de traitement (création/collecte, exploitation/stockage, transfert, destruction/transfert)

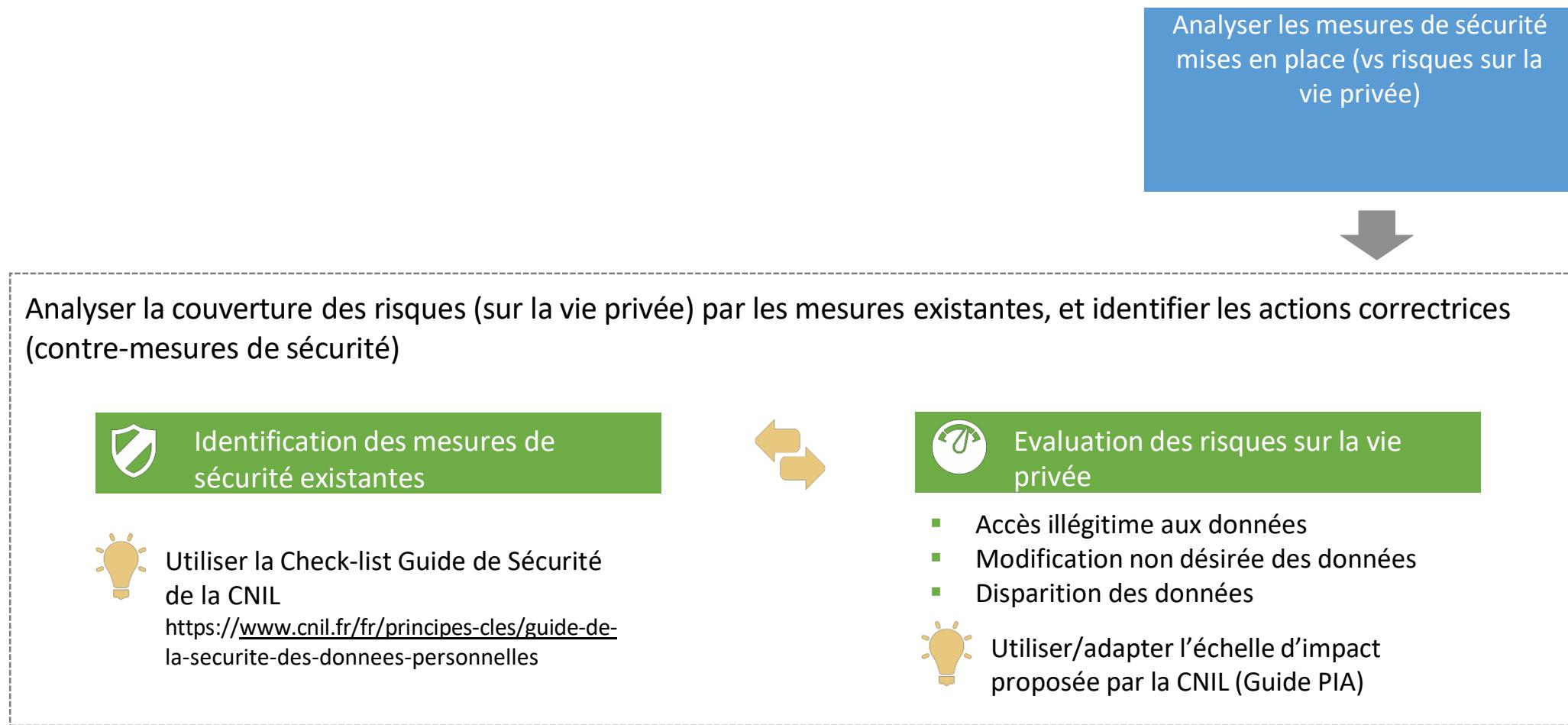


Utiliser les informations disponibles dans les formalités (déclaration/autorisation) par le Client et/ou les normes/dispenses de la CNIL

Audit des traitements / DPIA (3)



Audit des traitements / DPIA (4)



Autres textes réglementaires et/ou institutionnels

- LIL 3
 - Adaptation de la loi Informatique et Libertés de 1978 pour répondre aux exigences du GDPR
- Directive NIS (Network and Information Security)
 - Définit des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne
- RGS (Référentiel Général de Sécurité)
 - A pour objet le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives et s'impose ainsi à elles comme un cadre contraignant tout en étant adaptable et adapté aux enjeux et besoins de tout type d'autorité administrative
- PSSIE (Politique de Sécurité des Systèmes d'Information de l'État)
 - La PSSIE fixe les règles de protection applicables aux systèmes d'information de l'État
- ...