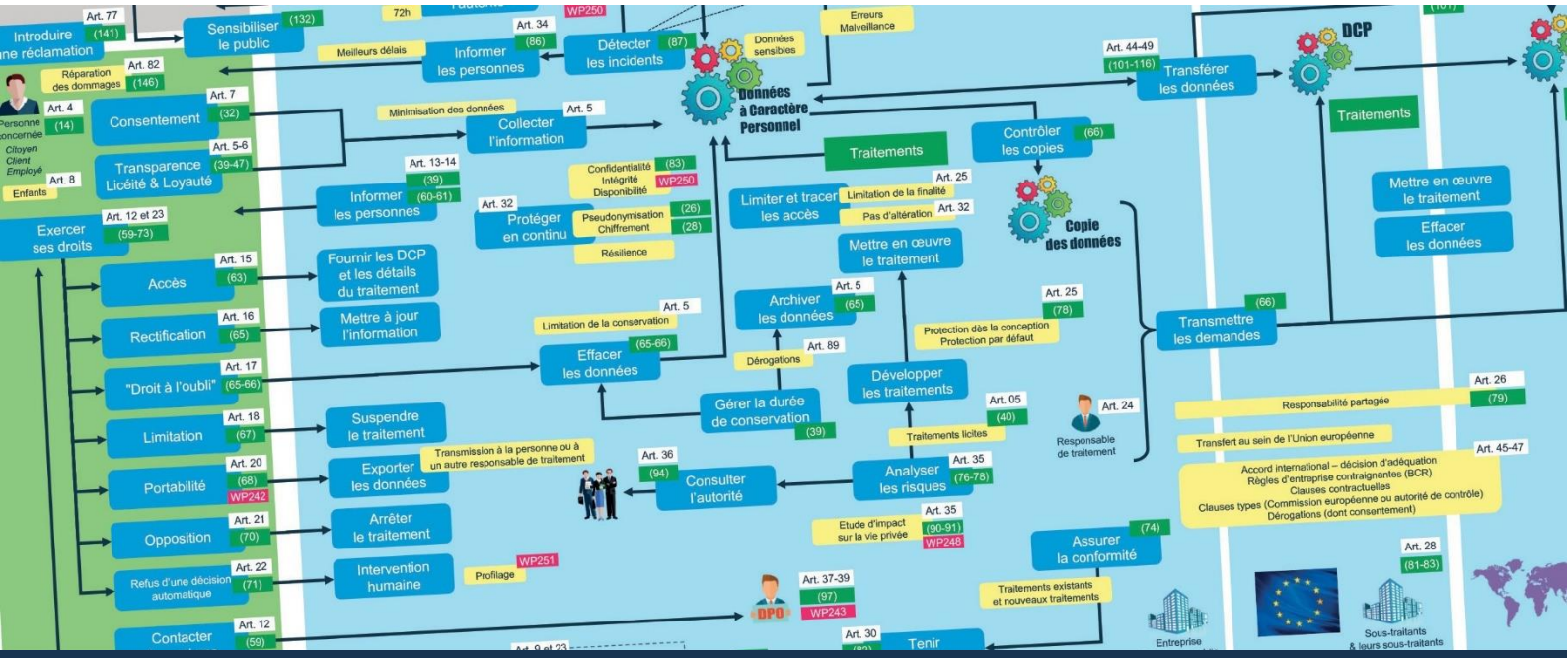
LES FICHES PRATIQUES du CLUSIF - RGPD



QU'EST-CE QU'UNE VIOLATION DE DONNÉES PERSONNELLES ?

1. DÉFINITIONS

Le règlement européen introduit l'obligation de notifier à la CNIL les violations de données à caractère personnel et, dans certains cas, de les communiquer aux personnes dont les données personnelles ont été affectées par cette violation. Elles concernent les données personnelles issues des traitements mis en œuvre au sein de l'entreprise ou de l'administration.

Le RGPD définit dans son article 4 une « *violation de données à caractère personnel* » comme étant « *une violation de la sécurité entraînant, la destruction accidentelle ou illicite, la perte, l'altération, la divulgation ou l'accès non autorisé à des données personnelles transmises, stockées ou autrement traitées (numériques ou papier)* ».

Les violations sont classées selon les trois natures (*cf. exemples en annexe 1*) :

1. Violation de la confidentialité, lorsqu'il y a un accès ou une divulgation non autorisée éventuellement accidentelle à des données personnelles ;
2. Violation de l'intégrité, en cas de modification non autorisée ou accidentelle des données personnelles ;
3. Violation de disponibilité, en cas de perte accidentelle ou d'accès non autorisé ou destruction de données personnelles.

Une violation affecte les données à caractère personnel ou la vie privée d'une personne concernée lorsqu'il peut en résulter, par exemple, un vol ou une usurpation d'identité, un dommage physique, une humiliation grave ou une atteinte à la réputation.

2. UNE PREMIÈRE NÉCESSITÉ EST DE POUVOIR DÉTECTER LES VIOLATIONS

Une organisation doit être mise en place pour détecter un événement de sécurité et traiter les principales alertes.

Les sources de détection de violations peuvent être issues à la fois d'une analyse des journaux de logs, des résultats de tests d'intrusion ou d'audits, de piratages constatés, de constatations physiques ou numériques, de divulgations constatées.

Les détections potentielles sont signalées au délégué à la protection des données pour enregistrement, documentation et instruction de la violation dans le cadre d'un processus interne préalablement validé.

Toutes les violations de données personnelles sont des incidents de sécurité sur le système d'information à traiter comme tels.

Dans tous les cas, la violation de données doit être documentée en interne.

3. DÉCLARATION DE LA VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL AUPRÈS DE LA CNIL (RGPD, ART. 33)

En cas de violation de données à caractère personnel, le responsable du traitement à caractère personnel concerné ou son représentant en notifie la violation en question à l'autorité de contrôle compétente (CNIL). Cette notification s'effectue en coordination avec le délégué à la protection des données (DPO) et le responsable de la sécurité des systèmes d'information (RSSI), dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

La notification doit, à tout le moins :

- Décrire la nature de la violation de données à caractère personnel (cf. annexe 2) y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Décrire les conséquences probables de la violation de données à caractère personnel ;
- Décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

4. COMMUNICATION DE LA VIOLATION AUX PERSONNES CONCERNÉES (RGPD, ART. 34)

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé (cf. annexe 3, *RGPD, considérant 75*) pour les droits et libertés d'une personne physique, la direction Métier, après approbation du bon niveau hiérarchique, communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les conséquences probables et les mesures prises.

La communication à la personne n'est pas nécessaire dans l'une des hypothèses suivantes :

- La communication aux personnes exigerait des efforts disproportionnés. Dans ce cas, il sera recommandé de procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière efficace.
- Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, la CNIL peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication.

5. ORGANISATION DE LA COMMUNICATION EN CAS D'INFORMATION DES PERSONNES CONCERNÉES PAR LA VIOLATION (ANNEXE 4)

- La violation de données à caractère personnel concerne les agents de l'entreprise ou de l'administration : il incombe au directeur des ressources humaines de mettre en œuvre la communication adaptée à la gravité de la violation.

- La violation de données à caractère personnel concerne les usagers, clients ou administrés : il incombe au directeur de l'activité concernée de mettre en œuvre la communication adaptée à la gravité de la violation en coordination avec le directeur de la communication dans les situations nécessitant une communication de masse.

- La violation de données à caractère personnel concerne des salariés d'un partenaire conventionné : il incombe au directeur porteur de la convention de mettre en œuvre une communication adaptée à la gravité de la violation en coordination avec le partenaire.

ANNEXE 1 : EXEMPLE TYPE D'UNE VIOLATION

- Équipement perdu ou volé ;
- Papier perdu, volé ou laissé accessible dans un endroit non sécurisé ;
- Courrier perdu ou ouvert avant d'être retourné à l'envoyeur ;
- Piratage, logiciel malveillant (par exemple rançongiciel) et/ou hameçonnage ;
- Mise au rebus de documents papier contenant des données personnelles sans destruction physique ;
- Mise au rebus d'appareils numériques contenant des données personnelles sans effacement sécurisé ;
- Publication non volontaire d'informations ;
- Données de la mauvaise personne affichées sur le portail de l'utilisateur ;
- Données personnelles envoyées à un mauvais destinataire ;
- Informations personnelles divulguées de façon verbale.

ANNEXE 2 : EXEMPLE TYPE DE CAUSE(S) DE VIOLATION

- Acte interne malveillant ;
- Acte interne accidentel ;
- Acte externe malveillant ;
- Acte externe accidentel.

ANNEXE 3 : RISQUE ÉLEVÉ – CONSIDÉRANT 75 – RGPD

https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32016R0679

Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est **susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral**, en particulier :

- lorsque le traitement peut donner lieu à une **discrimination**, à un **vol ou une usurpation d'identité**, à une **perte financière**, à **une atteinte à la réputation**, à une **perte de confidentialité de données protégées par le secret professionnel**, à un **renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important** ;
- lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel ;
- lorsque le traitement concerne des données à caractère personnel qui révèlent **l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions**, ou encore à des mesures de sûreté connexes ;
- lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels ;
- lorsque le **traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables**, en particulier les enfants ;
- ou lorsque le **traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées**.

ANNEXE 4 : RÉCAPITULATIF DES SITUATIONS

ACTIONS	ACTEUR	CAS 1 : La violation n'engendre **pas de risques** sur les personnes	CAS 2 : La violation engendre un **risque** sur les personnes	CAS 3 : La violation engendre un **risque élevé** sur les personnes
1. Mise à jour du registre interne	DPO / RSSI	X	X	X
2. Notification à la CNIL (dans les 72 heures)	DIRECTION METIER + DPO / RSSI		X	X
3. Communication aux personnes concernées	3a. Agents (interne) : DRH 3b. clients / usagers : DIRECTION METIER + DIRECTION COMMUNICATION 3c. clients / usagers Partenaires : DIRECTION METIER + Partenaire			X