OBJET : cette procédure décrit les dispositions internes de gestion des incidents de sécurité et des violations de données personnelles gérées par Total Marketing France (TMF) et ses filiales, en application du Règlement Général sur la Protection des Données à caractère personnel (RGPD). Elle complète et précise les documents initiés par le groupe Total et les bonnes pratiques de la CNIL.

PERIMETRE D'APPLICATION ET CIBLE : cette procédure s'applique à toutes les activités de la société « Total Marketing France » et ses filiales. Les exigences qu'elle contient s'adresse à tous les collaborateurs impliqués dans le traitement de données personnelles et en particulier les responsables de traitements, les relais protection des données personnelles ou Data Privacy Liaison (DPL) et les délégués à la protection des données personnelles ou Data Protection Officer (DPO).

DATE D'APPLICATION : **01/01/2021**

| REVISION | | Date d'application | N° version | Objet | | |
|---|---|---|---|---|---|---|
| | | 01/01/2021 | 0 | Création de la procédure | | |
| | | | ENTITE | NOM | DATE | VISA |
| Circuit de validation | Métier | Rédacteur | FR/SG | Luc HOBON | 30/12/2020 | ✓ |
| | HSEQ | Vérificateur | FR/HSEQ/MEO | Pascal POTERALA | 30/12/2020 | ✓ |
| | Métier | Approbateur | FR/SG | Emmanuel de FOURNAS | 06/01/2021 | ✓ |

DOCUMENTS REFERENCES

- Règlement UE 2016/679 : Le règlement général sur la protection des données – RGPD
- Document Groupe : Fiche Pratique_Decision notification en cas de violation – FR
- Documents Branche M&S : Kit de conformité Data Breach M&S (documents DB.000 à DB.007)
- Règle TMF : CR FR HSEQ 102 : « Actions correctives, Actions préventives (ACP) »
- Règle TMF : GM FR HSEQ 801 : « Manuel de gestion de crise »

Table des matières

SIGLES ET DEFINITIONS :

| Sigle / terme | Définition |
|---|---|
| Accountability | Principe majeur du RGPD impliquant que le responsable de traitement doit être en mesure à tout moment de démontrer sa conformité au RGPD |
| BDPL | Branch Data Privacy Lead ou Coordinateur Branche Protection des Données Personnelles |
| CNIL | Commission Nationale de l'Informatique et des Libertés<br>C'est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. |
| Donnée personnelle | Toute information relative à une personne physique, identifiée ou identifiable, que celle-ci agisse à titre personnel ou professionnel |
| DPL | Data Privacy Liaison ou Relais Protection des Données Personnelles dans une entité |
| DPO | Data Protection Officer ou Délégué à la protection des données personnelles |
| Entité | Structure qui dispose d'une connaissance métier lui permettant d'opérer et de maitriser le traitement de données personnelles |
| Evènement de sécurité | Fait qui peut altérer la sécurité d'un traitement et qui peut après analyse être qualifié d'incident de sécurité |
| Incident de sécurité | Un événement qui altère la sécurité d'un traitement avec l'apparition d'un impact potentiel |
| Notification de violation de données personnelles | Exigence règlementaire d'information (CNIL et / ou les personnes concernées) à la suite d'une violation de données avérée qui présente un risque pour les droits et les libertés des personnes physiques |
| Responsable de Traitement (RT) | Personne qui définit, seule ou conjointement avec d'autres, les finalités et les moyens du traitement de données personnelles. Il donne des instructions et contrôle le sous-traitant.<br>Il est garant de la conformité RGPD de ses traitements et en particulier de la bonne exécution de cette procédure au sein de son entité. |
| RGPD | Règlement Général sur la Protection des Données à caractère personnel<br>Le règlement n° 2016/679, dit Règlement Général sur la Protection des Données à caractère personnel (RGPD, ou encore GDPR, de l'anglais General Data Protection Regulation), est un règlement de l'Union européenne, directement applicable dans les Etats de l'UE, qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. |
| Registre des violations de données personnelles | Registre consignant les faits concernant les violations de données personnelles, leurs effets et les mesures prises pour y remédier |
| Sous-traitant (ST) | Traite les données pour le compte et sous l'instruction du Responsable de Traitement |
| Traitement de données personnelles | Il s'agit de toute opération (ou tout ensemble d'opérations) effectuée à l'aide de procédés automatisés ou non et appliquée à des données personnelles. Tout traitement doit avoir une base juridique et une finalité déterminée préalablement au recueil des données et à leur exploitation. |
| Violation de données personnelles | Incident de sécurité entraînant (de manière accidentelle ou illicite) la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles (transmises, conservées ou traitées d'une autre manière), ou l'accès non autorisé à de telles données |

## 1. Principes généraux sur les incidents de sécurité et les violations de données personnelles

### 1.1. Rappel règlementaire

Le Règlement Général sur la Protection des Données (« *RGPD* ») introduit de nouvelles exigences en cas de violation de données personnelles :

- Obligation de notifier à l'autorité de contrôle[1] la violation lorsqu'elle est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées[2]. Cette notification auprès de l'autorité de contrôle doit se faire dans les meilleurs délais et, si possible 72 heures au plus tard après avoir pris connaissance de la violation[3] . Tout dépassement du délai de 72 heures doit être justifié lors de la notification ;

- Obligation de communiquer aux personnes concernées la violation de données personnelles lorsqu'elle est susceptible d'engendrer un risque élevé pour leurs droits et libertés[4]. Cette notification doit se faire dans les meilleurs délais ou peut être ordonnée par l'autorité de contrôle qui a été notifiée ;

- Obligation de documenter les violations de données personnelles[5], y compris celles non notifiées, en indiquant les faits, ses effets et les mesures prises pour y remédier.

### 1.2. Précisions terminologiques

- Incident de sécurité

« Un incident de sécurité est un évènement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien. »[6] Exemples : utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc.

Voici la définition des critères qui permettent de caractériser des informations ou des données.

| Critères | Définition |
|---|---|
| Disponibilité | Aptitude à disposer, de l'information lorsque le processus métier l'exige, et à maintenir cette capacité dans le temps |
| Intégrité | Propriété d'une information qui lors de son traitement (transmission, stockage, ...) ne subit aucune altération ni modification volontaire ou accidentelle |
| Confidentialité | Propriété d'une information qui ne doit pas être divulguée à des personnes ou des entités non autorisées |

L'incident de sécurité peut être déclenché par une action frauduleuse, accidentelle, par négligence ou inadvertance.

- Incident de sécurité de données personnelles

Un incident de sécurité de données personnelles est un évènement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'une donnée personnelle.
Cette procédure s'intéresse uniquement aux incidents de sécurité qui concernent des données personnelles.
Les incidents de sécurité qui ne touchent pas de données personnelles doivent être gérés selon d'autres procédures.

*Exemples de donnée personnelle : un numéro de téléphone, une adresse email, une adresse IP, une immatriculation de véhicule (etc.) dès lors qu'il est possible de faire le lien entre cette information et une personne physique.*

[1] Une autorité de contrôle est une « *autorité publique indépendante qui est instituée par un Etat membre de l'Union européenne* ». En France, il s'agit de la CNIL : la Commission Nationale de l'informatique et des libertés ; en Belgique, il s'agit de l'APD : l'Autorité de Protection des Données.
[2] Une personne concernée par une violation de données est une personne physique identifiée ou identifiable. Est réputée être « *une personne physique identifiable* », une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
[3] Article 33 du RGPD
[4] Article 34 du RGPD
[5] Article 33 (5) du RGPD
[6] Selon le glossaire de l'ANSSI

- Violation de données personnelles

Une violation de données est définie comme une « *violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* »[7].

Tous les incidents de sécurité de données personnelles ne constituent pas nécessairement des violations de données personnelles. En revanche, toutes les violations de données personnelles sont des incidents de sécurité.

Il est important de distinguer :
- la violation d'une règle de conformité des données personnelles qui n'engendre pas de risque pour une personne physique *(exemple : un manquement à l'inscription au registre d'un traitement de données personnelles)* ;
- d'une violation de données personnelles (*exemple : une consultation par des personnes non habilitées à des données personnelles)*.

Il est essentiel de distinguer clairement une violation de données personnelles, d'un traitement non conforme de données personnelles.
En effet, la faiblesse d'un dispositif de sécurité ou de confidentialité ne constitue pas en tant que telle une violation de données personnelles, même si elle contrevient à l'obligation de sécurité imposée par le RGPD. Pour qu'un défaut de sécurité entre dans le champ d'une violation de données personnelles, il est nécessaire d'avoir pu constater qu'il y a un risque pour les droits et les libertés des personnes physiques.

Lors de leur identification et afin d'évaluer les impacts, les violations de données peuvent être classées en trois catégories, une même violation pouvant concerner plusieurs catégories.

- **Violation de confidentialité** : divulgation ou accès des données à la suite d'une action frauduleuse, accidentelle ou par négligence ou par inadvertance

*Exemple : les fiches clients d'un site web marchand sont accessibles à des pirates qui volent les données personnelles pour les utiliser de façon malveillante.*

- **Violation de disponibilité :**

- perte d'accès ou de contrôle aux données par le responsable de traitement de façon temporaire ou durable ;
- destruction partielle ou totale des données à la suite d'une action frauduleuse ou accidentelle, c'est-à-dire qu'elles n'existent plus à un moment donné (ou durablement) dans une forme utilisable pour le responsable de traitement.

*Exemple : un logiciel malveillant qui chiffre et / ou bloque des données personnelles des clients rendant ainsi impossible la réalisation des prestations prévues au contrat (attaque de type « ransomware »), entrera dans cette catégorie. Les données seront toujours existantes mais indisponibles sans l'obtention d'un moyen pour les débloquer comme par exemple une clé de déchiffrement.*

- **Violation d'intégrité** : modification de façon non souhaitée des données à la suite d'une action frauduleuse, accidentelle, ou par négligence ou par inadvertance.

*Exemple : un logiciel malveillant qui modifie les adresses postales des clients contenues dans leurs fiches client, impactant ainsi la bonne livraison des commandes passées.*

[7] Articles 4 (12) du RGPD

### 1.3. Obligation de notifier l'autorité de contrôle

#### 1.3.1. Obligation de notifier l'autorité de contrôle dans les 72 heures en cas de risque

Le responsable du traitement doit notifier la violation de donnée à l'autorité de contrôle compétente lorsque cette dernière est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

Cette notification doit avoir lieu dans les meilleurs délais et si possible, dans les 72 heures après avoir pris connaissance de la violation. Encore faut-il que le responsable du traitement ait pu, dans ce délai, identifier si la violation présentait un risque pour les droits et libertés des personnes concernées, tout dépassement du délai de 72 heures devant toutefois être justifié lors de la notification.

#### 1.3.2. A quel moment le responsable du traitement "prend connaissance" de la violation ?

Le responsable du traitement devrait être en mesure de prouver à quel moment il a pris connaissance de la violation dans la mesure où il s'agit du point de départ du délai de notification.

Selon les autorités[8], le responsable du traitement a « pris connaissance » de la violation de données dès lors qu'il a un degré raisonnable de certitude qu'un incident de sécurité ayant conduit à la compromission de données personnelles s'est produit.

En pratique, une première investigation rapide peut être nécessaire afin de recueillir des éléments permettant de confirmer avec un degré raisonnable de certitude la réalité de la violation de données.

*Exemple*
*Les autorités considèrent que si une personne informe le responsable du traitement qu'elle a reçu un faux e-mail de sa part contenant des données personnelles la concernant, cette information ne fera que suggérer qu'une violation de données a eu lieu. Si après une première investigation, des indices révélant un accès non autorisé aux données sont recueillis, le responsable du traitement sera alors considéré comme ayant pris connaissance de l'incident.*

#### 1.3.3. Gestion des délais et notifications complexes

Si le responsable du traitement ne dispose pas de toutes les informations requises, il peut les fournir au fur et à mesure qu'il en prend connaissance[9]. Il est toutefois recommandé de l'indiquer à l'autorité de contrôle dès la première notification et de donner les raisons du retard si l'échelonnement implique le dépassement du délai de 72 heures.

Il est également possible de faire une notification commune pour des violations similaires qui se sont produites sur une courte période. Le temps de l'investigation de toutes les violations peut éventuellement justifier un retard.

#### 1.3.4. Contenu de la notification à l'autorité de contrôle

La notification doit contenir les éléments suivants[10] :
- Une description de la nature de la violation de données, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de données personnelles concernées ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel il est possible d'obtenir plus d'informations ;
- Une description des mesures prises ou envisagées, y compris des mesures visant à atténuer les éventuelles conséquences négatives ;
- Une description des conséquences probables de la violation de données.

#### 1.3.5. A quelle autorité notifier en cas d'une violation de données personnelles ?

En application du RGPD et sans préjudice des lois locales, lorsque l'on est en présence d'un seul responsable de traitement, celui-ci devra notifier la violation à l'autorité de contrôle du pays dans lequel il est établi, et ce indépendamment de la citoyenneté des personnes dont les données ont été compromises.

[8] WP250 "Guidelines on Personal data breach notification under regulation 2016/679" adoptées le 3 octobre 2017
[9] Article 33 (4) du RGPD
[10] Article 33 (3) du RGPD

En application du RGPD et sans préjudice des lois locales, lorsque l'on est en présence de plusieurs responsables de traitement, chaque responsable devra notifier la violation à son autorité de contrôle et indiquer une volumétrie de données compromises et de personnes concernées propre à ses activités, si cette distinction est possible. Même dans cette hypothèse, la notification sera toujours faite indépendamment de la citoyenneté des personnes dont les données ont été compromises.

Le RGPD ne retient pas le critère de la nationalité et de la résidence des personnes mais uniquement le lieu d'établissement du responsable de traitement. Toutefois, les lois nationales d'adaptation au RGPD doivent être analysées car certaines peuvent imposer de notifier une violation en fonction de la citoyenneté ou de la résidence des personnes dont les données sont compromises.

Il est donc recommandé de notifier une violation à toutes les autorités de contrôle des pays où se trouve une filiale de Total qui était responsable de traitement des données violées. En effet, les pouvoirs d'injonction et d'investigation à la suite d'une notification restent locaux et il peut y avoir des spécificités de droit local qui s'appliqueront dans un pays et pas dans un autre.

Qu'est-ce qu'une autorité chef de file ?
C'est l'autorité nationale qui « assume la responsabilité principale de la gestion d'une activité de traitement transfrontalier, par exemple lorsqu'une personne concernée introduit une réclamation concernant le traitement de ses données à caractère personnel[11] ». La désignation de cette autorité en tant qu'autorité chef de file dépendra du lieu de l'établissement principal du responsable du traitement en Europe.
L'existence d'une autorité chef de file ne change pas les règles de notification détaillées ci-dessus : elle n'a pas vocation à gérer la violation de données personnelles pour l'ensemble des autorités des pays concernés.

### 1.4. Obligation de notifier aux personnes concernées dans les meilleurs délais en cas de risque élevé

Lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit informer la personne concernée de la violation de données dans les meilleurs délais[12] afin qu'elle puisse prendre les précautions nécessaires (cf. Annexe 4).

#### 1.4.1. Notion de "meilleurs délais" et coopération avec les autorités

En pratique, le délai de notification peut varier en fonction de la nécessité d'atténuer un risque immédiat de dommage (notification immédiate) ou de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation de données ou la survenance de violations similaires (délai plus long). La notification devrait également être effectuée en coopération étroite avec l'autorité de contrôle, dans le respect des directives de cette dernière et / ou d'autres autorités compétentes, telles que les autorités répressives[13] .

Ainsi, à moins qu'une notification immédiate des personnes concernées ne soit nécessaire, le responsable du traitement peut, dans le cadre de la notification de violation de données, demander conseil à l'autorité de contrôle pour évaluer la nécessité de communiquer aux personnes concernées, cette dernière pouvant également obliger le responsable du traitement à notifier les personnes concernées.

#### 1.4.2. Contenu et mode de notification des personnes concernées

Le contenu de la notification des personnes concernées est similaire à celle qui doit être faite aux autorités à l'exception de la description de la nature de la violation qui doit être expliquée en des termes clairs et simples. Elle devrait également inclure toute recommandation visant à atténuer les effets négatifs de la violation de données[14].

La notification devrait, en principe, être effectuée directement auprès de la personne concernée à moins que cela implique un effort disproportionné. Dans ce cas une communication publique ou une mesure similaire doit être mise en œuvre pour que les personnes concernées soient informées[15].

[11] Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant dans sa version révisée et adoptée le 5 avril 2017.
[12] Article 34 (1) du RGP
[13] Considérant 86 du RGPD
[14] Article 34 du RGPD et considérant 86
[15] Article 34 (3) (c) du RGPD

#### 1.4.3. Exception à l'obligation de notification

La notification n'est plus obligatoire[16] :

- Dès lors que des mesures de protection technique et organisationnelle appropriées ont été appliquées aux données personnelles concernées et ont, en particulier, rendu les données incompréhensibles à toute personne non autorisée (ex : chiffrement) ; ou
- Si des mesures ultérieures garantissant que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser, ont été mises en œuvre.

### 1.5. Obligation de documenter toutes les violations de données

Le responsable du traitement doit documenter toutes les violations de données personnelles dans un registre des violations, y compris celles qui n'ont pas fait l'objet d'une notification. Les informations devant figurer dans ce registre sont celles qui, a minima, doivent être communiquées à l'autorité de contrôle lors d'une notification de violation de données personnelles (voir point 1.3 ci-dessus). Elles sont notamment les suivantes :

- Descriptif de la violation des données ;
- Date de la découverte de la violation ;
- Origine(s) et cause(s) de la violation ;
- Nombre et nature des données compromises ;
- Nombre et catégories de personnes concernées par la violation ;
- Informations relatives aux conséquences prévisibles pour les personnes de la violation ;
- Mesures de sécurité prises avant et après la violation.

Les autorités recommandent également que le responsable du traitement motive dans le registre la décision de ne pas notifier une violation en justifiant notamment que :

- La violation n'était pas susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques (voir point 2 ci-dessus) ;
- Le responsable[17] du traitement a mis en œuvre des mesures de protection techniques et organisationnelles appropriées et régulièrement vérifiées ;
- La communication de cette violation exigerait des efforts disproportionnés.

### 1.6. Rôle du sous-traitant

Les sous-traitants ont l'obligation de notifier au responsable du traitement toute violation de données dans les meilleurs délais après en avoir pris connaissance[18].

Les autorités considèrent que, dès lors que le sous-traitant a pris connaissance de la violation, le responsable du traitement est supposé en avoir aussi pris connaissance ; aussi, elles recommandent que le sous-traitant notifie immédiatement au responsable du traitement toute violation ayant eu lieu, des informations supplémentaires sur la violation pouvant être fournies ultérieurement en fonction de l'avancement de l'investigation. Il est donc important de prévoir ces conditions de notification immédiate dans les contrats avec les sous-traitants et de s'assurer que les mesures techniques et organisationnelles sont mises en place.

### 1.7. Les sanctions

L'autorité de contrôle compétente est susceptible de prononcer une amende administrative pouvant s'élever jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu, pour toute violation des obligations incombant aux responsables du traitement et aux sous-traitants en application des articles 33 et 34 du RGPD dont notamment :

- Le défaut de notification à l'autorité et le cas échéant, aux personnes concernées, par le responsable du traitement, dans les délais impartis et sans pouvoir justifier d'un éventuel retard ;
- Le défaut de notification du responsable du traitement par le sous-traitant de toute violation de données dans les meilleurs délais ;
- La notification incomplète effectuée par le responsable du traitement.

[16] Article 34 (3) (a) et (b) du RGPD

[17] Article 33 (1) du RGPD

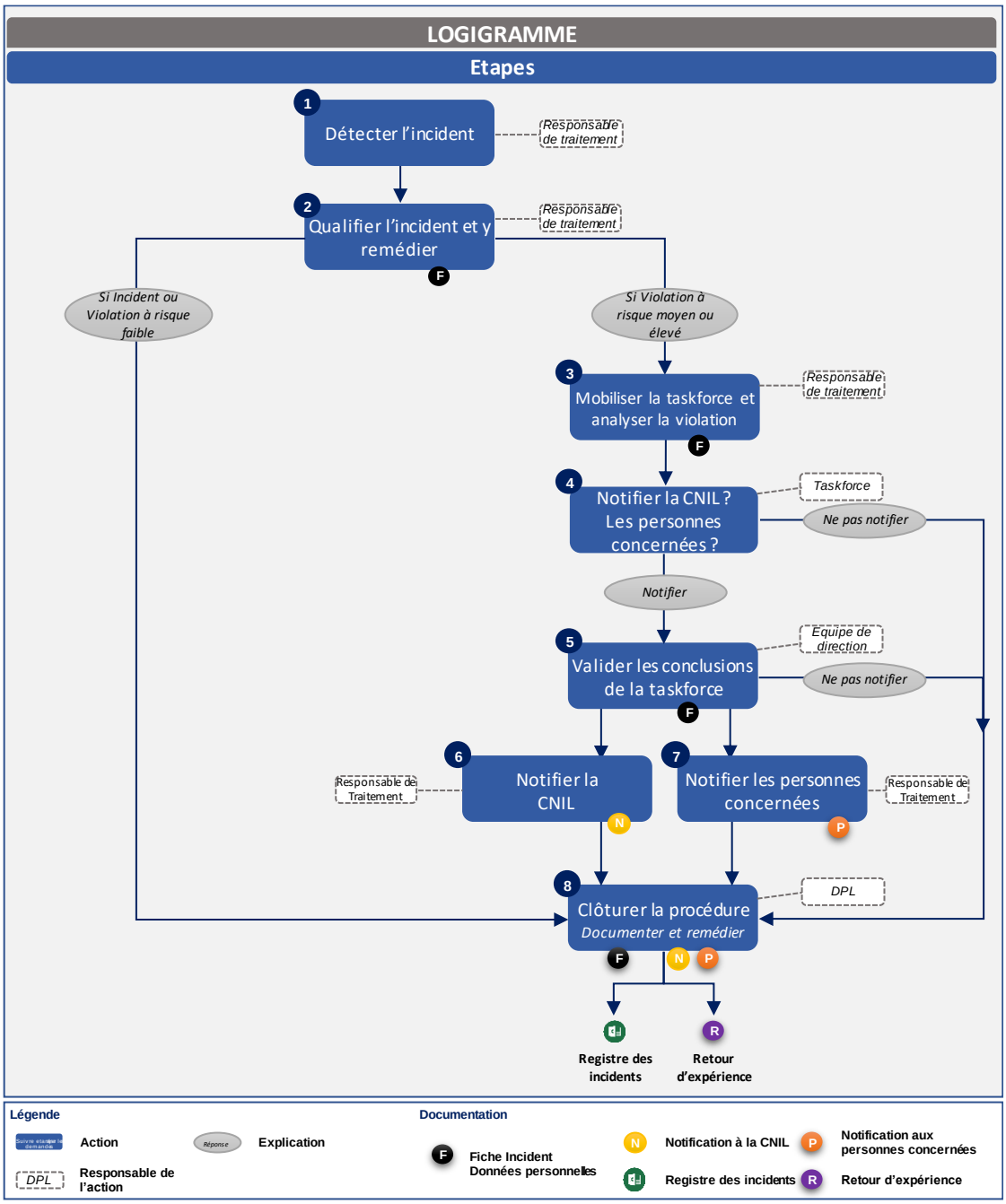
[18] [18] Article 33 (2) du RGPD

## 2. Gestion et traitement des incidents de sécurité et des violations de données personnelles

Le responsable de traitement est la personne qui définit les finalités et les moyens du traitement des données personnelles. Dans le cas de traitements réalisés par Total Marketing France, il est précisé que chaque membre du comité directeur est en charge du bon respect de la réglementation pour les activités de son périmètre de responsabilité.
Pour les traitements réalisés par une filiale de TMF, il est précisé que le directeur / la directrice de la filiale est en charge du bon respect de la réglementation pour les activités de son périmètre de responsabilité.
Chaque responsable de traitement (membre du comité directeur ou directeur / directrice de filiale) désigne au sein de son entité le service en charge de la gestion des violations de données.

Le responsable de traitement mène des actions de sensibilisation auprès des collaborateurs pour la bonne compréhension de la règlementation et que tout incident de sécurité puisse être évité ou pris en charge.
Chaque entité peut s'appuyer en interne sur un relais protection des données personnelles ou Data Privacy Liaison (DPL). Il est également possible de solliciter le délégué à la protection des données ou Data Protection Officer (DPO) lorsque le responsable de traitement en a nommé un.

**À tout moment, le DPL / DPO / Juriste peut être sollicité par l'entité pour l'aider à traiter un incident de sécurité.**



### 2.1. Etape 1 : Détecter un incident de sécurité de données personnelles

Un incident de sécurité est un évènement qui peut altérer des données personnelles avec un impact potentiel :
- Perte de confidentialité : par leur divulgation ou leur accès non autorisés ;
- Perte de disponibilité : par leur destruction partielle ou totale, temporaire ou durable, ou par l'impossibilité d'y accéder ou de les contrôler, temporairement ou durablement ;
- Perte d'intégrité : par leur modification non souhaitée.

Pour plus de détails, reportez-vous au chapitre 1.2 de cette procédure.

Un incident de sécurité peut être détecté et remonté par une ou plusieurs parties prenantes de l'entreprise : collaborateurs Total, sous-traitants externes, fournisseurs, clients, CNIL, etc.

Il peut avoir lieu à n'importe quel moment et dans n'importe quel service ou métier (Commerce, Marketing, RH, IT, etc.). L'entité droit procéder à une investigation préliminaire permettant de valider la pertinence de l'alerte et sa réelle existence. Toute alerte doit faire l'objet d'une analyse par l'entité afin de déterminer sa gravité ainsi que son étendue.

L'entité prend en charge l'incident de sécurité afin d'y remédier le plus rapidement possible et, si cela s'avère nécessaire, d'être en capacité de notifier la violation à la CNIL dans les 72 heures règlementaires. Il est donc primordial de sensibiliser les parties prenantes de TMF à l'importance de remonter tout incident de sécurité potentiel détecté.

Dès la détection de l'incident, l'entité doit lancer des actions afin de mettre un terme à l'incident de sécurité et de sécuriser les données personnelles.

### 2.2. Etape 2 : Qualifier l'incident de sécurité de données personnelles et y remédier

Tout au long de cette étape, l'entité doit associer le Data Privacy Liaison (« DPL ») concerné et si besoin le Data Privacy Officer (« DPO ») du périmètre.

L'entité doit rapidement déterminer si l'incident de sécurité est susceptible d'engendrer un risque afin, le cas échéant, de pouvoir le notifier à l'autorité de contrôle et aux personnes concernées dans les délais impartis. Il n'existe pas de définition précise de « risque » ou de « risque élevé » dans le RGPD.

Il convient, à cet effet, de prendre en compte les circonstances spécifiques de l'incident dont notamment :
- le type d'incident (confidentialité, disponibilité, intégrité) ;
- le type, le volume et la sensibilité des données (ex : données de carte de paiement, données de santé) ;
- le nombre et le type de personnes concernées (ex : personne vulnérable telle que salarié) ;
- les possibilités d'identification des personnes (ex : adresse IP ou prénom & nom) ;
- les caractéristiques du responsable du traitement ;
- les risques médiatiques et réputationnels pour le responsable de traitement ;
- et les risques d'effets collatéraux pour les personnes concernées (risques susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral telle qu'une discrimination, une usurpation d'identité, une perte financière, une atteinte à la réputation ou une perte de confidentialité de données protégées par le secret professionnel).

*Exemple : Les autorités considèrent, par exemple, que l'attaque d'une plateforme de vente en ligne et la publication des données (login, mot de passe, historique d'achat) est susceptible d'engendrer un risque élevé. Les données impactées par l'attaque sont les données d'authentification du consommateur (login, mot de passe), qui entraîne un risque de révélation d'une situation sociale (l'historique d'achat). En revanche, le vol d'un CD de sauvegarde de données chiffrées n'est pas susceptible d'engendrer de risque si les données sont chiffrées en conformité avec l'état de l'art en matière d'algorithme de chiffrement et si la clé de déchiffrement n'a pas été compromise.*

#### 2.2.1. Actions correctives

L'entité met en place, dans les plus brefs délais, des actions correctives pour tout incident de sécurité.
Ces actions doivent être documentées dans la « Fiche violation de données personnelles », et suivies tout au long de cette procédure.

En fonction de la nature de l'incident, l'entité peut s'appuyer sur des acteurs spécialisés comme :
- le propriétaire de l'application / outil ;
- l'interlocuteur informatique interne (par exemple : Business Delivery Manager) ou externe ;
- le spécialiste de la sécurité des systèmes d'information : par exemple, Responsable de la Sécurité des Systèmes d'Information (RSSI) ou Cyber Security Officer (CSO), Chief Information Security Officer (CISO), etc.

*Exemple 1 : Découverte d'un fichier contenant des données personnelles stockées sur un serveur partagé accessible à toute l'organisation. La première action consiste à retirer ce fichier pour le stocker dans un espace protégé accessible uniquement par les personnes habilitées.*

*Exemple 2 : Découverte d'une faille de sécurité sur un site web où les fiches clients sont accessibles par n'importe quelle personne. La première action consiste à rendre inaccessible les fiches clients (déconnecter le site web) puis faire corriger cette faille par le service informatique ou par le prestataire en charge de l'exploitation de ce site web afin de sécuriser les fiches clients.*

### 2.2.2. Compléter la « Fiche violation de données personnelles »

L'entité complète une « Fiche violation de données personnelles » pour chaque incident de sécurité sur des données personnelles, indépendamment de sa fréquence, de sa nature ou de son niveau d'impact, y compris s'il résulte d'un incident en cascade.

Cette fiche sera utilisée et enrichie par la taskforce si celle-ci est mobilisée.

Si l'incident détecté n'engendre aucun impact sur la confidentialité, la disponibilité, ou bien l'intégrité, il est considéré comme un simple incident de sécurité. Dans ce cas, il n'est donc pas nécessaire de réaliser une analyse d'impact (se reporter directement à la paragraphe 2.8).

Toutefois, si cet incident engendre au moins un impact sur la confidentialité, la disponibilité, ou bien l'intégrité des données personnelles, il est alors qualifié de violation de données personnelles. Il est donc important et obligatoire de procéder à l'analyse d'impact (cf. paragraphe 2.2.3) qui permettra d'évaluer le niveau de risque de cette violation.

### 2.2.3. Réaliser une analyse d'impact

L'entité évalue si la violation de données personnelles est susceptible d'engendrer un risque faible, moyen ou élevé pour les droits et libertés des personnes concernées en complétant avec la « Fiche violation de données personnelles ».

| **Procédure** | **Fiche de violation de données personnelles V1.2** |
|---|---|
| Risque faible | Evaluation de la violation pour les personnes = NEGIGEABLE |
| Risque moyen | Evaluation de la violation pour les personnes = LIMITE ou IMPORTANT |
| Risque fort | Evaluation de la violation pour les personnes = MAXIMAL |

L'entité doit également analyser et apprécier le risque en fonction de sa connaissance du métier et des spécificités liées à son activité.

RAPPEL : vous pouvez à tout moment solliciter le DPL / DPO / Juriste de votre entité.

Si la violation présente seulement un risque faible pour les droits et libertés des personnes concernées, il n'est pas nécessaire de mobilier la taskforce (se reporter directement au paragraphe 2.8).

**Il est important de documenter tous les incidents de sécurité y compris ceux sans impact ou avec un impact à risque faible**.
En cas de développement inattendu et / ou tardif, la recherche de l'origine du problème est facilitée par la consultation des « Fiches violation de données personnelles » (répertoriées dans le registre des violations).

En revanche, si l'impact est à risque moyen ou élevé, l'entité mobilise dans les plus brefs délais la taskforce (se reporter à l'étape suivante).

### 2.3. Etape 3 : Mobiliser une taskforce

#### 2.3.1. Saisine de la taskforce

Lorsqu'un incident de sécurité impactant des données personnelles est qualifié de violation à risque moyen ou élevé, le responsable de traitement mobilise dans les plus brefs délais la taskforce.

Dans certaines situations, le responsable de traitement peut décider de déclencher une cellule de crise (cf. GM FR HSEQ 801 : « Manuel de gestion de crise »). La taskforce s'inscrit pleinement dans la cellule de crise.

#### 2.3.2. Composition de la taskforce

Cette taskforce est composée de :
- L'opérationnel qui dispose d'une connaissance métier lui permettant de maitriser le traitement de données personnelles ;
- Le responsable de l'entité concernée ;
- Le Data Privacy Lead (DPL) concerné ;
- Le Data Protection Officer (DPO) du périmètre concerné le cas échéant ;
- Le Local Entreprise & Industrial Cyber Security Officer (L-XCSO) de l'entité ;
- Le Local Entreprise & Industrial Cyber Security Officer (L-XCSO) de Total Marketing France ;
- Le Chief Information Security Officer (CISO) de la direction informatique si l'application est dans son périmètre ou celui du prestataire informatique si l'application n'est pas gérée en interne dans le groupe Total ;
- Le juriste en charge des questions de protection de la donnée en lien avec le juriste en charge du métier concerné ;
- Le Responsable de la communication de l'entité concernée.

La taskforce peut se faire assister de toute autre personne pour mener à bien sa mission.

#### 2.3.3. Mission de la taskforce

La taskforce analyse la violation de donnée personnelles à l'aide de la « Fiche violation de données personnelles » préalablement renseignée par l'entité.

Chaque membre de la taskforce utilise ses connaissances et ses compétences pour compléter, enrichir l'analyse préalable, et mener des investigations complémentaires. L'objectif est de s'assurer que l'analyse est exhaustive.

*Exemple 1 : Si un fichier stocké sur espace partagé (ou dans un outil ou une application) et contenant des données personnelles a été piraté, il faut déterminer si un ou plusieurs autres fichiers avec des données personnelles stockés au même endroit ont été piratés ou non.*

*Exemple 2 : Si une faille de sécurité sur un site web est détectée, deux cas de figure se présentent :*
*- Si l'entité a sélectionné un prestataire IT sans l'implication de la direction informatique, c'est à l'opérationnel de prendre en charge les investigations avec son prestataire ;*
*- Si l'entité a sélectionné la direction informatique pour exploiter le site web, c'est à la direction informatique (RSSI ou CISO) de prendre en charge les investigations.*

Le juriste doit aider à la qualification du risque et évaluer le préjudice subi par l'entreprise ainsi que par les personnes concernées, sur la base des informations fournies par le métier et les équipes IT. Par ailleurs, il étudie avec la taskforce la nécessité d'un dépôt de plainte.

Toute action prise afin de gérer une violation de données personnelles doit être consignée par écrit afin de pouvoir démontrer la diligence de l'entité à stopper la violation, en vue d'en minimiser l'impact pour les personnes concernées et pour le Groupe.

La taskforce est aussi chargée de documenter et tracer la gestion de la violation en gardant une copie de l'ensemble des documents complétés.
La taskforce désigne un responsable de la mise à jour des documents issus de sa réflexion.

#### 2.3.4. Reporting au sein du réseau Protection des Données Personnelles

Le DPL concerné, membre de la taskforce, doit tenir informer son Branch Data Privacy Lead (« BDPL »), ainsi que le Corporate Data Privacy Lead (« CDPL ») jusqu'à la fin de cette procédure.
Cette information continue leur permet de suivre le déroulement des étapes et d'apporter, si besoin, assistance et conseil.

### 2.4. Etape 4 : Faut-il notifier la CNIL et les personnes concernées ?

#### 2.4.1. Particularité de la notification à l'autorité de contrôle

La notification n'est pas anodine pour l'entité car en notifiant, elle déclare à l'autorité de contrôle qu'elle a subi une violation et s'expose à la suspicion d'un défaut de sécurité informatique, et donc un risque d'investigation par l'autorité de contrôle et de poursuites en indemnisation de la part des personnes concernées par la violation.
Il appartient à l'entité d'évaluer le risque et la gravité de celui-ci afin de décider de la nécessité de la notifier à l'autorité compétente.

Le délai des 72 heures imposé par le RGPD pour la notification à l'autorité court à partir du moment où l'investigation a permis de confirmer avec un degré raisonnable la réalité de la violation.

#### 2.4.2. Les cas possibles de notification

En fonction de l'analyse de la violation réalisée par la taskforce, trois cas se présentent.

Ce tableau est donné à titre indicatif et reste applicable dans la majorité des cas de violation. Toutefois, c'est à la taskforce de déterminer s'il faut notifier ou non l'autorité de contrôle et les personnes concernées.

| | **Aide à la décision** | | |
|---|---|---|---|
| **Niveau de risque selon l'analyse d'impact** | **Notification CNIL ?** | **Notification personnes concernées ?** | **Commentaire** |
| **Risque faible** | Non | Non | |
| **Risque moyen** | Oui | Non | *L'autorité de contrôle peut ordonner la notification aux personnes concernées et cela malgré les conclusions de l'analyse réalisée en interne* |
| **Risque élevé** | Oui | Oui | |

A l'aide du tableau ci-dessus, la taskforce émet une recommandation sur la réalisation ou non d'une notification à l'autorité de contrôle et aux personnes concernées.

La taskforce rend compte au BDPL ainsi qu'au CDPL, puis soumet ces recommandations pour validation à l'équipe de direction.

### 2.5. Etape 5 : Valider les recommandations

Avant toute notification à la CNIL et aux personnes concernées, les informations qui seront communiquées doivent être validées par le directeur de l'entité concernée, les juristes en charge des questions de protection des données personnelles, le responsable de la communication et la direction générale de l'entité juridique.

### 2.6. Etape 6 : Notifier la violation à la CNIL

Pour rappel, la notification de violation à la CNIL n'est réalisée que lorsque l'analyse d'impact a démontré un niveau de risque moyen ou élevé pour les droits et les libertés des personnes, ou lorsque la taskforce l'a jugé nécessaire en cas de risque faible. En tout état de cause, la direction générale est préalablement informée de cette notification à la CNIL.

La notification de la violation se fait directement sur le site web de la CNIL en renseignant un formulaire en ligne. L'interface de saisie comporte de nombreuses étapes ne permettant pas de revenir en arrière et de modifier des informations déjà saisies. Il faut donc renseigner le fichier Excel **« Aide à la saisie de la notification à la CNIL »** avant de débuter la saisie en ligne.

Pour rappel, la notification à l'autorité de contrôle doit être réalisée dans un délai de 72 heures imposé par le RGPD à partir du moment où l'investigation a permis de confirmer avec un degré raisonnable la réalité de la violation. Si ce délai ne peut être respecté, il est possible de notifier l'autorité de contrôle plus tard, à condition de pouvoir justifier le retard.

Si les investigations menées ne permettent pas d'obtenir l'exhaustivité des informations exigées par la CNIL, il est possible de réaliser dans un premier temps une « notification initiale » dans les 72 heures règlementaires, puis de réaliser dans un second temps une « notification complémentaire / modifiée » une fois que l'ensemble des informations est disponible.

Le DPO (point de contact officiel vis-à-vis de la CNIL) est en charge de la notification de la violation de données. En cas d'absence du DPO ou si l'entité n'a pas désigné un DPO, voici par ordre de priorité, les acteurs en charge de cette notification :
- Le Data Privacy Lead (« DPL ») ;
- Le juriste en charge des questions de protection de la donnée ;
- Le Branch Data Privacy Lead (« BDPL ») ;
- Le responsable de l'entité concernée.

Lors de la saisie de la notification sur le formulaire en ligne, il est important de relire attentivement et d'enregistrer sous format PDF le « récapitulatif avant envoi » de l'étape 5.
Par ailleurs, il est demandé de sauvegarder la confirmation de notification et notamment le numéro de notification et la date et l'heure d'enregistrement. Ces deux informations sont indispensables pour pouvoir le cas échéant, finaliser ou modifier la notification initiale.
Enfin, un email de confirmation est envoyé à l'adresse de courrier électronique renseignée sur le formulaire.
Tous ces éléments cités ci-dessus doivent être conservés selon le principe d'« *accountability ».*

Remarque : Lorsque cela est nécessaire, la CNIL prend contact avec l'entreprise dans un délai de 2 mois à compter de l'enregistrement de la notification pour vérifier que des mesures ont été prises préalablement et / ou postérieurement à la violation.
Par exemple, elle indique au responsable les améliorations à mettre en œuvre sur l'utilisation d'un algorithme de chiffrement adapté ou l'optimisation de la gestion des mots de passe.
Elle peut également renvoyer les responsables vers les services de police pour porter plainte, ou vers la plateforme cybermalveillance.gouv.fr afin de trouver une information ou un prestataire.

### 2.7. Etape 7 : Notifier la violation aux personnes concernées

Pour rappel, la notification de violation aux personnes concernées n'est réalisée que lorsque l'analyse d'impact a démontré un niveau de risque élevé pour les droits et les libertés des personnes, ou lorsque la taskforce l'a jugé nécessaire en cas de risque faible ou moyen. En tout état de cause, la direction générale est préalablement informée de cette notification aux personnes concernées.

Le responsable de traitement assisté du DPL (et du DPO) procède dans les meilleurs délais à l'information des personnes concernées pour leur permettre de minimiser les risques sur leur vie privée.

Le responsable de traitement doit se faire assister d'un juriste et / ou d'une personne chargée de communication au sein du Groupe afin d'adapter les modalités de communication selon les catégories de personnes concernées (collaborateurs en interne ou clients / prospects / fournisseurs en externe) et en fonction des risques encourus.

La notification des personnes concernées doit être faite dans les meilleurs délais et dans des termes **clairs et simples** et inclure toute recommandation visant à atténuer les effets négatifs de la violation de données[19].
Cf. Annexe 5 - Exemple de communication d'une violation de données aux personnes concernées.

*Exemple de recommandation : changement de mot de passe des utilisateurs d'un service, vérification de l'intégrité des données de leur compte en ligne, sauvegarde de ces données sur un support personnel, etc.*

La notification doit comporter les éléments suivants :
- Description de la violation des données (dont la date de la violation) ;
- Explication des mesures de sécurité existantes ;
- Description des conséquences probables de la violation de données personnelles ;
- Description des mesures prises ou qui vont être prises pour remédier à la violation de données personnelle, « y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. » ;
- Un point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Les coordonnées publiques (courrier électronique générique [boîte partagée] ou adresse postale) du DPL (ou du DPO si celui-ci a été désigné).

En fonction du nombre de personnes concernées et des moyens disponibles (centre d'appel existant, site web adapté, etc.), le point de contact désigné doit être capable d'absorber un nombre de sollicitations important.

*Exemple : Numéro de téléphone dédié pour répondre aux sollicitations, une page web dédiée avec des explications détaillées, création d'une adresse mail spécifique, etc.*

Pour rappel, la CNIL peut ordonner la notification aux personnes concernées : elle doit, alors, être effectuée selon les exigences définies par l'autorité et cela malgré les conclusions de l'analyse réalisée en interne.

### 2.8. Etape 8 : Clôturer la procédure : Documenter et remédier

Cette étape doit être réalisée, qu'il s'agisse d'un simple incident de sécurité ou d'une réelle violation de données personnelles.

#### 2.8.1. Registre des violations et documentation

La documentation doit consigner les faits concernant les incidents de sécurité et les violations de données personnelles, leurs effets et les mesures prises pour y remédier. Elle peut être contrôlée par la CNIL dans l'objectif de vérifier le respect des obligations en matière de violations.

Pour tout incident de sécurité et pour toute violation de données personnelles, le DPL concerné doit :
1. Compléter le registre des violations de données personnelles
2. Archiver la documentation suivante dans les plus brefs délais :
   - La **« Fiche violation de données personnelles »** complétée ;
   - Le fichier « Aide à la saisie de la notification à la CNIL », le cas échéant ;
   - Une copie numérique du « récapitulatif avant envoi » (étape 5) de la / les notification(s) faite(s) à la CNIL, le cas échéant ;
   - Une copie numérique de la « confirmation de notification » à la CNIL avec le numéro de notification, et la date et l'heure d'enregistrement, le cas échéant ;
   - Une copie numérique de l'email de confirmation de la notification à la CNIL, le cas échéant ;
   - Une copie numérique de l'information qui a été communiquée aux personnes concernées par la violation, le cas échéant.

[19] Article 34 (2) du RGPD

### 2.8.2. Plan d'actions correctives et préventives

L'entité s'assure que les actions correctives (initiées à l'étape 2- paragraphe 2.2.1) pour remédier à l'incident de sécurité ou la violation de données sont finalisées. Si une notification à la CNIL a été faite, il est important d'assurer un suivi rigoureux et précis, car la CNIL peut intervenir et demander des compléments d'information dans les deux mois suivant la notification.

Afin d'éviter que cela se reproduise, l'entité mène une analyse approfondie des causes qui ont abouti à l'incident de sécurité ou la violation de données personnelle. Elle est en charge de la définition et de la mise en œuvre d'un plan d'actions en cohérence avec la procédure « Actions correctives, Actions préventives (ACP) » (CR FR HSEQ 102).

L'entité communique le suivi du plan d'actions au DPL de son entité et au DPO.
Le DPL contrôle la bonne application de ce dernier.

### 2.8.3. Retour d'expérience de la violation de données personnelles

La taskforce est chargée de mener une analyse a posteriori de la gestion de la violation de données personnelles dans un objectif d'amélioration continue du dispositif.
Les résultats de cette analyse sont à communiquer au Branch Data Privacy Lead (« BDPL »).

L'entité assistée de son DPL rédige un retour d'expérience. Ce REX a pour objectif :
- d'entretenir la vigilance des collaborateurs à partir d'un exemple concret de la violation de donnée,
- d'informer les collaborateurs sur les causes immédiates et fondamentales qui ont conduit à l'évènement,
- de recommander des actions à mettre en œuvre pour réduire la probabilité et / ou la gravite d'un évènement similaire,
- d'accroitre la compétence professionnelle,
- de garder la mémoire des évènements et de leurs enseignements.

Le DPL concerné, membre de la taskforce, doit tenir informer son Branch Data Privacy Lead (« BDPL »), ainsi que le Corporate Data Privacy Lead (« CDPL ») de la clôture de la procédure de gestion de la violation.

**Annexe 1 : Fiche violation de données personnelles**

Le modèle de fiche est élaborée, maintenue et diffusée par le groupe Total.
Sa référence dans le système documentaire de Total Marketing France est : CR FR GOUV PDP 002 Annexe 1.

**Annexe 2 : Aide à la saisie de la notification CNIL**

Le modèle de fichier excel est élaboré, maintenu et diffusée par Total Marketing France.
Sa référence dans le système documentaire de Total Marketing France est : CR FR GOUV PDP 002 Annexe 2.

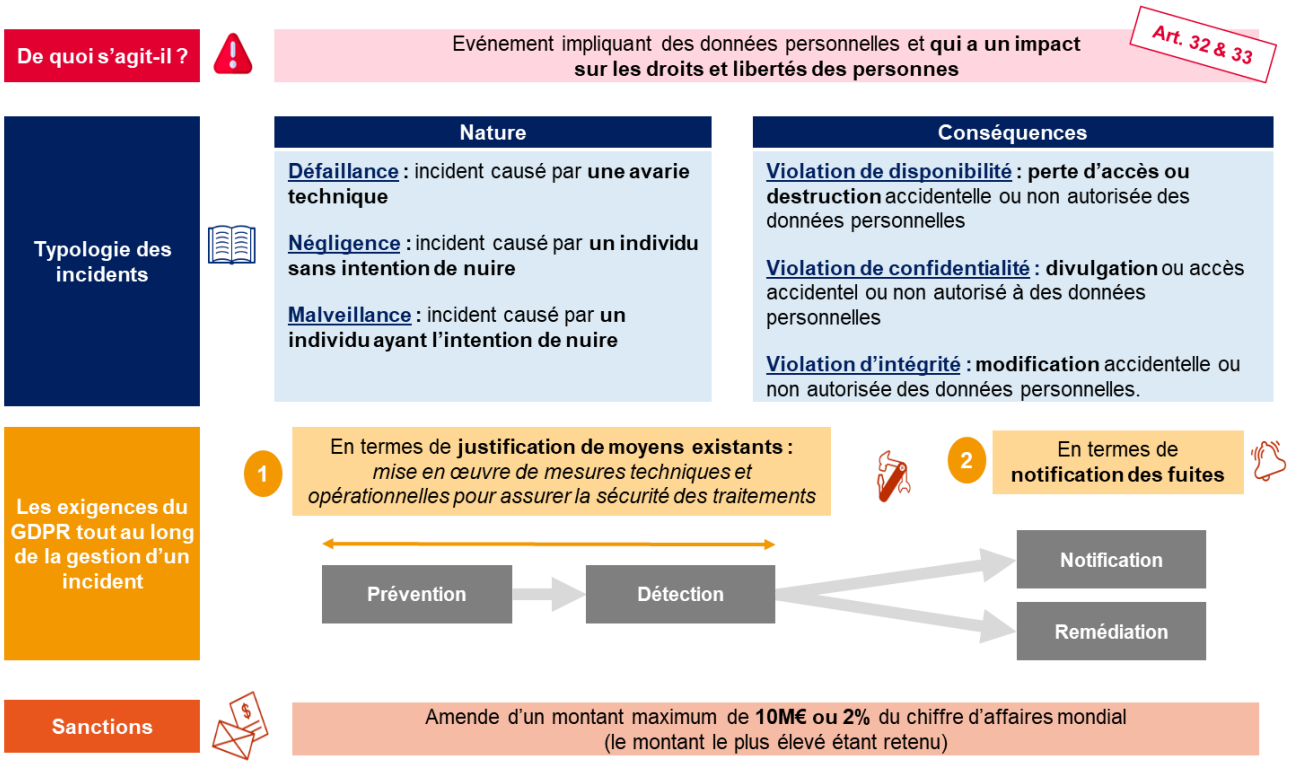
**Annexe 3 : Registre des violations des données personnelles**

Le modèle de fichier registre est élaboré, maintenu et diffusée par la branche Marketing & Services.
Sa référence dans le système documentaire de Total Marketing France est : CR FR GOUV PDP 002 Annexe 3.

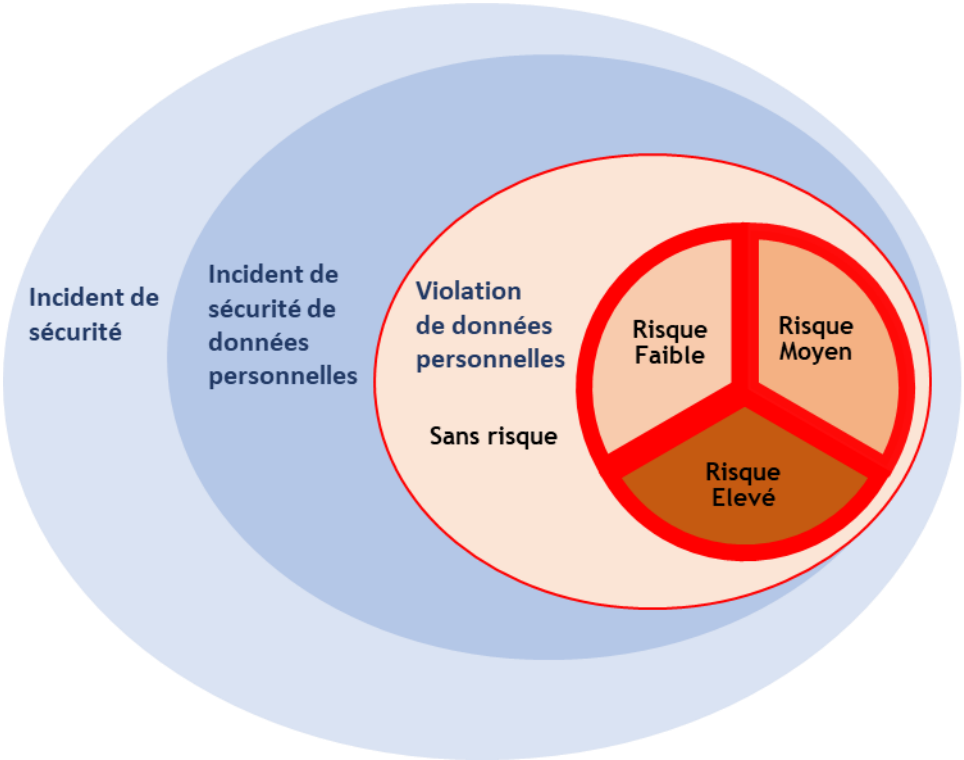
**Annexe 4 : Template REX violation des données personnelles**

Le template REX (retour d'expérience) est élaboré, maintenu et diffusée par la branche Marketing & Services.
Sa référence dans le système documentaire de Total Marketing France est : CR FR GOUV PDP 002 Annexe 4.

## Annexe 5 : Synoptique de la gestion d'une violation de données personnelles




## Annexe 6 : Typologie incident de sécurité → violation de données personnelles



**Annexe 7 : Exemples d'évènements, d'incidents de sécurité et de violation de données personnelles**

| Exemple | Qualification de l'évènement | Explication |
|---|---|---|
| Un collaborateur dépose par inadvertance un fichier Excel chiffré sur un espace partagé en ligne de son organisation. Il s'aperçoit de son erreur rapidement et supprime ce fichier | Evènement de sécurité | Il s'agit d'un simple évènement de sécurité sans impact sur la confidentialité, disponibilité et d'intégrité car le fichier chiffré est accessible uniquement par ce collaborateur |
| ***Le collaborateur constate que l'opération de chiffrement de son fichier n'a pas fonctionné*** | | |
| Seules des personnes habilitées de son entité ont accès à cet espace partagé | Evènement de sécurité | Ce fichier est accessible uniquement par des personnes habilitées qui auraient pu se procurer ce fichier autrement. Il n'y a donc pas de perte de confidentialité. |
| Le fichier est accessible par des personnes non habilitées mais qui appartiennent à l'organisation | Incident de sécurité | Cet évènement de sécurité est qualifié d'incident de sécurité car il y a un risque de perte de confidentialité |
| ***Le fichier Excel contient des données personnelles de collaborateurs*** | | |
| Les données personnelles présentes dans ce fichier sont des données d'identification (nom, prénom, numéro de téléphone, adresse professionnelle) accessibles sur l'annuaire | Incident de sécurité sur données personnelles | Cet incident de sécurité est qualifié d'incident de sécurité sur données personnelles car le fichier comporte des données personnelles de collaborateurs accessibles |
| Les données personnelles présentes dans ce fichier sont des données de vie professionnelle : diplômes, formations | Violation de données personnelles avec risque faible | Cet incident de sécurité est qualifié de violation de données personnelles avec un impact à risque faible sur les droits et libertés des personnes concernées |
| Les données personnelles présentes dans ce fichier sont des données de vie personnelle : adresse de domicile | Violation de données personnelles avec risque moyen | Cet incident de sécurité est qualifié de violation de données personnelles avec un impact à risque moyen sur les droits et libertés des personnes concernées |
| Les données personnelles présentes dans ce fichier sont des données sensibles : données de santé | Violation de données personnelles avec risque élevé | Cet incident de sécurité est qualifié de violation de données personnelles avec un risque élevé sur les droits et libertés des personnes concernées |
| ***Le fichier Excel contient des données personnelles de clients*** | | |
| Les données personnelles présentes dans ce fichier sont des données d'identification : prénom, nom | Violation de données personnelles avec risque faible | Cet incident de sécurité sur données personnelles est alors qualifié de violation de données personnelles avec un impact à risque faible sur les droits et libertés des personnes concernées |
| Il y a en plus dans ce fichier les données suivantes : adresse mail, numéro de téléphone | Violation de données personnelles avec risque moyen | Cet incident de sécurité sur données personnelles est alors qualifié de violation de données personnelles avec un impact à risque moyen sur les droits et libertés des personnes concernées |
| Le fichier comporte en plus les données personnelles suivantes : IBAN, pièce d'identité | Violation de données personnelles avec risque élevé | Cet incident de sécurité sur données personnelles est alors qualifié de violation de données personnelles avec un risque élevé sur les droits et libertés des personnes concernées |

| Exemples | Qualification | Notifier l'autorité ? | Notifier les personnes concernées ? | Notes/Recommandations |
|---|---|---|---|---|
| Perte d'un disque dur / clé USB contenant des données chiffrées avec un outil habilité par le Groupe | Evènement de sécurité | Non | Non | L'outil de chiffrement habilité par le Groupe garantit un niveau élevé de protection. Les données ne sont pas accessibles. |
| Un responsable de traitement possède un site victime d'une cyberattaque, des données personnelles sont recueillies / volées | Violation de confidentialité | Oui | Oui | La notification doit être réalisée à l'autorité de contrôle du pays où est domicilié le responsable de traitement. |
| Une coupure de courant de quelques minutes entraine un incident dans un centre d'appels qui fait que les clients ne peuvent plus le contacter ni accéder à leur dossier. | Incident de sécurité (disponibilité) | Non | Non | Si la notification n'apparaît pas obligatoire, le responsable doit en revanche documenter cet incident dans son registre. |
| Un cybercriminel contacte le responsable de traitement pour obtenir une rançon après avoir hacké le système via un *ransomware qui crypte les données*.<br><br>Les données n'ont pas été volées mais sont effectivement inaccessibles et le traitement n'est plus opérationnel. | Violation de disponibilité | Oui | Oui | Si les données étaient sauvegardées (*backup*) et donc récupérables, le responsable n'aurait pas besoin de notifier à l'autorité ou aux personnes concernées car il n'y aurait pas de violation de disponibilité. Cependant si l'autorité prend connaissance de cet incident par un autre biais, une investigation concernant la sécurité mise en œuvre par le responsable doit être menée. |
| Une personne téléphone au service paie, pour signaler qu'elle a reçu le bulletin de paie de quelqu'un d'autre. Le responsable du traitement entreprend une enquête de courte durée (dans les 24 heures) et établit avec une certitude raisonnable qu'une violation de données personnelles a eu lieu et si elle présente un défaut systémique susceptible d'affecter ou d'avoir affecté d'autres personnes. | Violation de confidentialité | Oui | Seulement les personnes concernées s'il est avéré que les autres personnes ne sont pas impactées | Si plus tard le responsable découvre que davantage d'individus sont affectés, une mise à jour doit être adressée à l'autorité et le responsable doit informer les autres personnes potentiellement touchées par la violation. |
| Un responsable de traitement exploite une plateforme marketplace et possède des clients dans plusieurs États membres. Sa plateforme subit une cyberattaque et les noms d'utilisateurs, les mots de passe et l'historique des achats sont publiés en ligne par l'attaquant. | Violation de confidentialité | Oui | Oui | Le responsable de traitement doit prendre des mesures, par exemple en forçant la réinitialisation des mots de passe des comptes affectés, ainsi que d'autres mesures pour limiter les risques.<br>La notification doit être réalisée aux autorités de contrôle de tous les pays (états membres) où sont domiciliés les clients. |

**Annexe 8 : Récapitulatif des documents à renseigner**

| Etape | Support | Action à réaliser | Objectif du support | Responsable de la mise à jour des documents | Durée de conservation |
|---|---|---|---|---|---|
| Etape 2<br>***Qualifier l'incident de sécurité de données personnelles*** | **Fiche violation de données personnelles** | Création | • décrire l'incident de sécurité et ses conséquences<br>• détailler les mesures prises pour y remédier<br>• évaluer l'impact de l'incident de sécurité sur les personnes concernées | Entité | 5 ans |
| Etape 3<br>***Mobiliser une taskforce*** | **Fiche violation de données personnelles** | Mise à jour | • décrire l'incident de sécurité et ses conséquences,<br>• détailler les mesures prises pour y remédier<br>• évaluer l'impact de l'incident de sécurité sur les personnes concernées<br>• justifier la recommandation de la taskforce de notifier ou non<br>• déterminer la nécessité de notifier ou non l'autorité de contrôle et/ou les personnes concernées | Responsable nommé au sein de la taskforce | 5 ans |
| Etape 6<br>***Notifier la violation à la CNIL*** | **Aide à la saisie de la notification à la CNIL** | Création puis mise à jour si nécessaire | • identifier les éléments à renseigner à la CNIL en cas de notification | DPO sinon DPL | 5 ans |
| Etape 8<br>-<br>***Clôturer la procédure : Documenter et remédier*** | **Registre des violations** | Alimenter le registre | • consigner les faits,<br>• ajouter tous les documents utilisés : fiche violation de données personnelles, confirmation de notification CNIL, message de notification aux personnes, … | DPL | 5 ans |
| | **Retour d'expérience** | Création | • analyser la gestion des événements ;<br>• proposer des axes d'améliorations | Entité / DPL | 5 ans |

**Annexe 9 : Exemple de communication d'une violation de données aux personnes concernées**

*[L'entité doit adapter tout élément surligné en jaune dans les exemples suivants en fonction du contexte de la violation de données personnelles et ses conséquences sur les droits et libertés des personnes.]*

---

Madame, Monsieur,

Le Groupe Total est fortement engagé dans la protection de vos données personnelles.

Malgré tous les efforts déployés au quotidien dans l'ensemble de nos activités, nous avons été victimes le XXX d'un [piratage informatique, incident de sécurité, violation de données personnelles].
Certaines de vos données personnelles gérées par [Entité – exemple : le Club Total de Total Marketing France] ont été dérobées / divulguées / consultées. Il s'agit :
- de votre nom et de votre prénom ;
- de votre numéro de téléphone mobile ;
- de votre adresse courriel.
- xxxx

Conformément au Règlement Général sur la Protection des Données (RGPD), Total Marketing France a informé la CNIL.

Nous ne pouvons exclure que ces données personnelles puissent être utilisées par des tiers à des fins publicitaires (par courriel ou sms), d'hameçonnage (« phishing ») ou de tentatives d'escroquerie.

A ce titre, nous vous recommandons d'être particulièrement vigilants vis-à-vis de messages inhabituels, cherchant à usurper l'identité de Total Marketing France ou d'une autre entreprise, et qui vous inviteraient à communiquer des informations personnelles ou des données d'identification, à ouvrir une pièce jointe ou encore à cliquer sur un lien vers un site internet.

Pour plus de précisions sur les moyens de protections de vos données personnelles, nous vous invitons à consulter le site www.cybermalveillance.gouv.fr/bonnes-pratiques.

[Si données sensibles] Si vous avez subi des dommages et / ou des préjudices liés à cet incident, nous vous conseillons de contacter le dispositif d'assistance aux victimes d'actes de cybermalveillance : www.cybermalveillance.gouv.fr afin de porter plainte.

Nous vous assurons que les équipes de Total Marketing France sont mobilisées pour résoudre et limiter les impacts de cette attaque informatique.

Si vous avez des questions concernant cet incident, vous pouvez également nous contacter à XXX (*Numéro de téléphone dédié pour répondre aux sollicitations, une page web dédiée avec des explications détaillées, création d'une adresse mail spécifique, etc.*).

Nous nous excusons pour cet incident et tenons à vous assurer que Total Marketing France accorde la plus grande vigilance à la sécurité et à la protection de vos données personnelles.

Signature

Fonction

**Annexe 10 : Exemple de communication au sujet d'une violation de données personnelle avec perte de disponibilité mais sans perte de confidentialité (fuite de données personnelles)**

*[L'entité doit adapter tout élément surligné en jaune dans les exemples suivants en fonction du contexte de la violation de données personnelles et ses conséquences sur les droits et libertés des personnes.]*

---

Madame, Monsieur,

Le Groupe Total est fortement engagé, depuis plusieurs années, dans la protection de vos données.

Malgré tous les efforts que nous déployons chaque jour pour nous protéger de la cybercriminalité, nous avons été victimes d'une cyberattaque de nos systèmes d'information le XXX.

Nos équipes sont mobilisées pour résoudre et limiter les impacts de cette attaque informatique permettant une reprise progressive des activités.

Le retour à la normale de nos activités a été rendu possible grâce aux mesures de précaution prises immédiatement après l'attaque, notamment la déconnexion des systèmes afin de protéger les activités commerciales et les opérations des clients.

Selon des analyses approfondies, réalisées avec nos équipes informatiques ainsi que par des experts et des spécialistes externes, aucun élément n'indique, à ce stade, que des données personnelles de quelque sorte que ce soit aient été divulguées, dérobées ou consultées.

Nous avons déposé plainte et travaillons de concert avec les autorités compétentes afin de protéger les intérêts de nos clients et de nos partenaires.

Total Marketing France reste pleinement mobilisé pour vous assurer la meilleure qualité de services et s'excuse pour toute gêne occasionnée.

Signature

Fonction