Guide de gestion de violation de données personnelles

Dernière mise à jour : avril 2023

TABLE DES MATIÈRES

Introduction

Le présent guide de gestion des violations de données personnelles prévoit des mécanismes et des procédures à suivre par le groupe GREGOIRE-BESSON (composé des sociétés suivantes : la société GREGOIRE-BESSON, la société SOUCHU et la société SOCIETE NOUVELLE FENET) (ci-après « le Groupe ») afin d'anticiper la survenance d'une violation de données personnelles et de gérer au mieux cette dernière.

Le présent guide indique également les obligations du Groupe victime d'une telle violation.

Tous les termes suivis d'un astérisque sont définis dans le glossaire.

Ce document n'est qu'un guide à destination du Groupe et chacun des comportements à suivre devra être adapté à la situation de fait.

1. Qu'est-ce qu'une violation de données personnelles ?

➢ **Définition et concept**

L'article 4.12 du Règlement Général sur la Protection des Données* (dit RGPD) définit la violation de données personnelles comme "*une violation de la sécurité entraînante, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données*".

Plus simplement, il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière volontaire ou involontaire, ayant comme conséquence de compromettre l'intégrité*, la confidentialité* ou la disponibilité* de données personnelles.

Une violation de données personnelles pour le Groupe est donc un incident de sécurité qui affecte des données à caractère personnel détenues par le Groupe.
La faille de sécurité peut être de tout ordre (logique, physique, voire organisationnel).

L'existence d'une faille de sécurité au sein du Groupe révèle l'insuffisance des mesures en place au sein du système d'information du Groupe, ou l'absence de mesures techniques et organisationnelles, pourtant requises au titre de la conformité RGPD.

➢ **Exemples concrets de violation de données personnelles**

Incident de sécurité	Conséquence sur les données personnelles
Perte d'un ordinateur portable professionnel ou d'une clef USB contenant des données personnelles	Atteinte à la confidentialité des données personnelles
Erreur de manipulation dans le système d'information d'une clinique médicale qui engendre des données erronées sur les dossiers des patients Introduction non autorisée par des étudiants dans le système d'information de leur établissement scolaire pour modifier leurs notes	Atteinte à l'intégrité des données personnelles
Perte d'accès par un hôpital de ses données à cause d'un ransomware ou d'une panne de courant	Atteinte à la disponibilité des données personnelles

2. Comment détecter et anticiper au maximum la survenance d'une violation de données personnelles ?

➢ **La détection et la remontée des incidents informatiques par un système interne de signalement au sein du Groupe**

Tout événement susceptible d'être un incident de sécurité peut être détecté et signalé :
- soit par une personne qui est responsable ou a connaissance d'un fait ou d'une menace pour le

Groupe, tel le comportement d'une personne, le dysfonctionnement d'une application ou d'un équipement informatique (salarié du Groupe, client du Groupe ou prestataire du Groupe, Délégué à la Protection des Données Personnelles (DPO)* ou Référent à la Protection des Données Personnelles du Groupe si ce dernier n'a pas procédé à la désignation officielle d'un DPO) ;
- soit par l'équipe informatique du Groupe lors de la constatation d'une anomalie ou via un dispositif de supervision informatique interne au Groupe ;
- soit par un acteur externe de la sécurité informatique via des moyens techniques (outils informatiques et physiques ou sites spécialisés de détection d'incidents de sécurité) mis en œuvre par le Groupe.

Le signalement par toute personne doit être effectué dans les meilleurs délais auprès du Groupe par l'envoi d'un email à l'adresse suivante : rgpd@gb-group.co

➢ **La détermination d'une cellule de crise « équipe de gestion des incidents informatiques »**

La personne qui a reçu l'alerte au sein du Groupe en accuse réception et la transmet le plus rapidement à l'équipe chargée de la gestion des incidents informatiques (ci-après « l'équipe de gestion »), qui est composée des personnes suivantes :

- dirigeant du Groupe / équipe de direction ;
- Délégué / Référent à la Protection des Données Personnelles du Groupe ;
- directeur commercial / marketing du Groupe ;
- chef du service communication / relations externes du Groupe ;
- responsable de la sécurité physique et informatique / RSSI /DSI du Groupe ;
- membres désignés du service informatique du Groupe ;
- responsable RH du Groupe.

Il est à noter que les prestataires externes spécialisés en gestion informatique ou en sécurité informatique et auxquels le Groupe fait appel doivent être intégrés à l'équipe de gestion.
Si le Groupe sous-traite entièrement la gestion et la maintenance de son système d'information, la personne ayant reçu l'alerte en interne transmettra immédiatement cette alerte aux équipes supports du ou des prestataires informatiques du Groupe. Le Groupe doit se faire aider par ses prestataires et s'en remettre à leurs compétences pour le traitement des incidents informatiques du Groupe.

Nota Bene : La composition de l'équipe de gestion peut varier notamment en fonction de la structure, de la taille du Groupe et des postes présents au sein du Groupe.
Il est important que chaque service du Groupe soit représenté au sein de l'équipe de gestion et donc d'inclure à cette équipe toutes les compétences.
Le rôle de chaque membre de l'équipe de gestion est défini ci-après.

Le rôle de chaque membre de l'équipe de gestion n'est pas définitif et peut évoluer notamment en fonction des postes présents au sein du Groupe, du contexte et de la situation de fait.

Cependant, il est primordial que chaque personne connaisse son rôle et ses responsabilités afin de ne pas bloquer le fonctionnement du plan de réponse et de ne pas entraver son efficacité.

- **Le Délégué / Référent à la Protection des Données Personnelles** :

Il dirige et coordonne l'équipe de gestion.
C'est lui qui supervise l'exécution du plan de réponse aux incidents de sécurité. Il assure en interne comme en externe la communication et la transmission d'informations en temps réel sur l'incident de sécurité ayant conduit à une violation de données personnelles et doit être capable de répondre dans les meilleurs délais à toute question relative à l'incident de sécurité et de donner toutes les informations en sa possession sur la violation de données.

Son avis doit être impérativement pris en compte quant à la détermination de l'existence d'une violation de données personnelles et il participe activement à l'évaluation du risque de cette violation. Il a également le rôle de notifier à la CNIL, en étroite coordination avec le RSSI/DSI, le cas échéant, la violation.
Enfin, il doit rendre compte du rapport de synthèse sur la violation au dirigeant du Groupe.

- **Le RSSI/ DSI et les membres désignés de l'équipe informatique** :

Ils sont chargés de neutraliser la menace et de confiner l'incident de sécurité au plus vite. Ils doivent mener des recherches et rassembler des renseignements pour comprendre et apporter du contexte à l'incident de sécurité. Ils participent à l'élaboration du rapport de synthèse.

- **Le dirigeant / l'équipe de direction** :

Il /elle fournit les ressources nécessaires à l'équipe de gestion pour l'exécution et l'amélioration du plan de réponse aux incidents de sécurité ainsi que toute ressource nécessaire pour la sensibilisation des salariés et des collaborateurs du Groupe. De manière plus générale, il / elle doit informer solennellement l'ensemble des salariés des orientations du Groupe en matière de protection et définir la manière dont il entend que la sécurité soit intégrée dans tous les domaines d'activités ayant une incidence sur le niveau de sécurité du Groupe.
Il / elle veille à ce que l'équipe de gestion reçoive l'adhésion requise et des moyens suffisants Le dirigeant /l'équipe de direction n'a pas besoin d'être présent lors de l'analyse de l'incident et de l'évaluation du risque de l'incident.
Toutefois, il est essentiel de le /la mettre régulièrement au courant des avancées ainsi que de lui présenter les conclusions du rapport de synthèse post-incident ayant conduit à la violation de données.

- **Le chef du service des ressources humaines** :

Il va soutenir les efforts de l'équipe de gestion et renseigner cette dernière si un employé est impliqué dans l'incident de sécurité.

- **Le chef des relations publiques / service communication / relations clients / relations externes** :

Il aide à gérer en coordination avec le Délégué / Référent à la Protection des Données Personnelles les communications après l'incident de sécurité, notamment si la violation de données doit être signalée rapidement.

- **Directeur commercial / marketing :**

Le directeur commercial analyse la politique du Groupe pour penser et réfléchir à une stratégie commerciale efficace après la survenance de la violation au sein du Groupe si cette dernière a fragilisé économiquement du Groupe, a eu un impact sur ses ventes et si du fait de la violation les concurrents du Groupe ont eu accès à des données confidentielles et pu deviner certaines stratégies commerciales du Groupe.

Tous les membres de l'équipe de gestion se doivent de coopérer, d'aider au maximum l'équipe informatique et le RSSI/DSI à endiguer l'incident de sécurité, ils doivent communiquer entre eux sur et pendant toute la durée de l'incident de sécurité ayant conduit à la violation de données.

Nota Bene :

➔ Il est à noter que les prestataires externes spécialisés en gestion informatique ou en sécurité informatique et auxquels le Groupe fait appel peuvent tout à fait faire partie de l'équipe de gestion.

➔ Si le Groupe sous-traite entièrement la gestion et la maintenance de son système d'information, la personne ayant reçu l'alerte en interne transmettra immédiatement cette alerte aux équipes supports du ou des prestataires informatiques du Groupe. Le Groupe doit se faire aider par ses prestataires et s'en remettre à leurs compétences pour le traitement des incidents informatiques.

➢ **L'élaboration d'un plan de réponse aux incidents informatiques**

Des mesures immédiates de sécurité peuvent être prises par l'équipe de gestion (équipe informatique et le RSSI /DSI) après la détection de l'incident, soit sous forme de consignes, pour la personne qui a détecté l'incident (ex : changement immédiat des mots de passe), soit par l'activation automatique de mécanismes de protection (ex : suppression des comptes utilisateurs non utilisés depuis un certain temps, restriction d'accès aux comptes utilisateurs).

Il est nécessaire que tout événement signalé soit enregistré par l'équipe informatique et le RSSI/DSI sous forme de fiche dans une base de données des incidents pour faire un suivi et pour catégoriser chaque événement.

L'enregistrement de l'incident comporte à minima les informations suivantes :
- date et heure de l'alerte ;
- origine de l'alerte (personne ou dispositif technique de sécurité) ;
- coordonnées de la personne déclarante ;
- description aussi précise que possible de l'événement constaté ;
- classification de l'incident (nature de l'incident) ;
- la catégorisation de l'incident en potentiel incident de sécurité ;
- les potentiels risques de sécurité engendrés par l'incident informatique ;
- les mesures de sécurité éventuellement prises après la déclaration de l'incident informatique.

En cas de doute et si besoin, l'équipe informatique et le RSSI peuvent procéder à des investigations plus poussées pour qualifier l'événement, telles que :
- l'impact financier pour le Groupe ;
- l'impact sur l'image du Groupe ;
- les impacts sur les salariés, clients ou partenaires du Groupe ;
- les risques de poursuite judiciaire pour le Groupe ;

A ce stade, il est fortement conseillé à l'équipe de gestion de tenir un journal horodaté et précis des actions réalisées depuis qu'elle a été informée d'un incident informatique.
Ce journal peut être tenu par le Délégué / Référent à la Protection des Données Personnelles.

La détermination d'un incident de sécurité et la mise en place de mesures adaptées

Dans un premier temps, l'équipe de gestion est chargée d'analyser, d'enquêter sur tout incident potentiel de sécurité, de déterminer s'il s'agit véritablement d'un incident de sécurité, si une violation de données personnelles a eu lieu et, le cas échéant, d'évaluer les risques de cette violation.

Avant toute analyse de l'incident par l'équipe de gestion et si jugées nécessaires, l'équipe informatique et le RSSI /DSI peuvent prendre certaines mesures d'urgence afin de limiter la progression et les conséquences de l'incident ; parmi elles :
- une communication ciblée de recommandation à tous les salariés du Groupe ;
- le débranchement du poste informatique infecté du réseau du Groupe pour le mettre en quarantaine ;

- la coupure des flux de messageries internes et / ou externes du Groupe.

L'équipe de gestion, si possible au complet effectue son analyse qui porte sur les éléments suivants :
-la nature de l'incident ;
-l'impact de l'incident / inventaire des dégâts ;
-le fait générateur / origine de l'incident / la ou les vulnérabilités du système d'information ;
-le périmètre du Groupe touché (applications, réseaux et téléphonie, serveurs, personnes concernées* : clients, fournisseurs, salariés, prestataires, etc.).

Les critères d'évaluation pris en compte doivent être mis à la disposition de toute l'équipe de gestion pour des questions de transparence et d'efficacité.
Si l'équipe informatique considère que l'incident n'est pas un incident de sécurité, elle renvoie cet incident aux différentes équipes supports pour traitement.

Si elle conclut à un incident de sécurité, elle doit mettre fin dans les meilleurs délais à cet incident et s'assurer qu'il soit maîtrisé le plus rapidement possible.

La détermination de la survenance d'une violation de données personnelles

La détermination du périmètre touché par l'incident est une étape fondamentale dans l'analyse de l'incident par l'équipe de gestion, car elle va permettre de savoir si des données personnelles ont été compromises et si cet incident de sécurité a entraîné une violation d'une partie ou de toutes ces données personnelles.
L'analyse doit être réalisée le plus tôt possible par l'équipe de gestion et aboutir rapidement afin de déterminer, avec un degré de certitude raisonnable, si une violation de données personnelles s'est produite.
Une violation de données sera caractérisée par l'équipe de gestion si les données compromises par l'incident de sécurité ont subi une atteinte à leur confidentialité, à leur disponibilité et / ou à leur intégrité.

Si l'équipe de gestion conclut à un incident de sécurité ayant entraîné une violation de données personnelles, elle doit impérativement et immédiatement mettre en place des mesures de sécurité « des mesures de protection techniques et organisationnelles appropriées »* pour endiguer l'incident de sécurité et éviter l'aggravation des conséquences de la violation de données personnelles.

Le RSSI /DSI et les membres du service informatique peuvent par exemple mettre en place :
-des restrictions temporaires d'accès aux réseaux ou aux applications comme des blocages ou des filtrages des accès ;
-l'activation automatique du système anti-virus et des pare-feu présents sur les ordinateurs ;
-la restauration de toutes les données qui auraient été exfiltrées ;
-le chiffrement de toutes les données présentes sur les serveurs du Groupe ;
-limiter l'accès aux données et changer les permissions pour limiter les modifications de données par des personnes non autorisées ;
-des journaux pour suivre les ajouts, modifications ou suppressions de données.

Le Délégué / Référent à la Protection des Données Personnelles :
- peut faire une communication ciblée auprès des salariés / utilisateurs comportant les mentions d'informations suivantes :
  - description de l'incident ;
  - faits encore en cours d'investigations ;
  - activités impactées en raison des restrictions mises en place ;
  - consignes de comportements (ne pas envoyer de mails externes, ne pas ouvrir les pièces

jointes ou signaler les mails suspects) ;
- heure prévisionnelle ou jour de retour à la normale.

-peut également faire une communication à ses filiales comprenant les informations suivantes :
- faits précis et description de l'incident ;
- recommandations d'actions à mettre en place (qui peuvent être les mêmes que celles mises en place au sein du Groupe touché) ;
- proposition d'actions coordonnées.

-peut aussi communiquer sur l'incident de sécurité aux externes (clients, assureurs, fournisseurs) sur :
- les faits précis et la description de l'incident ;
- les faits encore en cours d'investigation ;
- les activités impactées en raison des restrictions mise en place ;
- les consignes de comportement (changement des mots de passe etc.).

La gestion de crise du PCA / PRA*, si elle existe dans le Groupe, peut être déclenchée à ce stade si la situation s'est dégradée et l'impose.

L'évaluation du risque de la violation de données personnelles

Dans un second temps, il revient à l'équipe de gestion, au complet si possible, de déterminer s'il existe un risque pour les personnes concernées par les données compromises et, le cas échéant, d'évaluer la gravité de ce risque.

L'équipe de gestion devra agir le plus rapidement possible afin, le cas échéant, de pouvoir notifier la CNIL* et les personnes concernées de la violation dans les délais impartis.

Il s'agit d'évaluer la gravité et la probabilité de survenance des conséquences de cette violation. Il convient, à cet effet, de prendre en compte les circonstances spécifiques de la violation dont notamment le type de violation (confidentialité, disponibilité, intégrité) ; la nature, le volume et la sensibilité des données (ex : données de carte de paiement, données de santé) ; le nombre et type de personnes concernées (ex : personne vulnérable, mineur, patient) ; les possibilités d'identification des personnes et la gravité des conséquences (risques susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral tel 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).

L'équipe de gestion peut évaluer le niveau de risque lié à la violation de données personnelles au

moyen de l'échelle suivante :

Niveau de risque	Préjudice pour les personnes concernées
Aucun	Aucun préjudice
Faible	Préjudice probable
Moyen	Préjudice probable et grave
Élevé	Préjudice certain et extrêmement grave

Plus le niveau de risque sera élevé, plus le nombre de mesures techniques et organisationnelles visant à réduire l'impact du risque de la violation à mettre en œuvre par l'équipe de gestion sera important.

Il est tout à fait possible que des investigations plus poussées soient nécessaires en cas d'incident de sécurité complexe et pour lequel il est difficile de déterminer si une violation de données a eu lieu et l'impact de cette violation.
Le cas échéant, le Groupe pourra mandater des prestataires informatiques spécialisés chargés d'enquêter sur l'incident de sécurité ayant conduit à la violation.
Des mesures techniques et organisationnelles de sécurité supplémentaires à celles déjà prises par le Groupe pourront être mises en œuvre suite aux rapports d'investigations et en coordination avec ces experts.

- **La formation et la sensibilisation des salariés du Groupe**

Les cybercriminels exploitent de plus en plus le facteur humain pour générer leurs attaques.
En effet, ils profitent de l'inattention ou de la négligence des salariés du Groupe pour installer des programmes malveillants, infecter les systèmes et accéder à des informations confidentielles.
Ainsi, un mot de passe trop faible ou un simple clic par un salarié du Groupe sur une pièce jointe corrompue peuvent être à l'origine d'une attaque informatique ayant de graves conséquences financières et opérationnelles pour le Groupe.

La sensibilisation informatique et la sensibilisation à la protection des données personnelles régulière de tous les collaborateurs du Groupe est donc essentielle et doit être une priorité pour le Groupe.

Il est important de responsabiliser chaque salarié et collaborateur du Groupe en lui expliquant quels sont les risques et comment chacun d'entre eux peut agir au quotidien pour s'en prémunir.
Les programmes de sensibilisation doivent s'étaler tout au long de l'année pour être efficaces. Ces actions de sensibilisation peuvent prendre la forme de communications sur les cybermenaces et de rappels sur le bon comportement à adopter, de lettres d'information régulières, d'affiches dans des endroits visibles de tous, de formation individuelle ou mutualisée, de cours en e-learning, de campagne de prévention, etc.
Les formations peuvent être réalisées par des sociétés ou organismes de formation spécialisés et tiers au Groupe.

➢ **La préparation du Groupe à des scénarios de violation de données personnelles**

Le Groupe se doit de tester régulièrement le dispositif mis en place en organisant des exercices de crises et en établissant des scénarios de violations de données réalistes et adaptés au contexte du Groupe.
L'équipe de gestion (l'équipe de gestion, le RSSI/DSI et le Délégué / Référent à la Protection des Données Personnelles) peut identifier les principales actions à mettre en œuvre en fonction des scénarios de violation identifiés. Les résultats de ces exercices sont essentiels pour identifier les éventuelles faiblesses de la procédure de gestion des violations de données et s'assurer que tous les membres de l'équipe de gestion connaissent leur rôle.

➢ **Anticiper les risques grâce à l'évaluation de la sécurité informatique du Groupe**

Avant d'établir un plan de réponse à un incident de sécurité susceptible d'entraîner une violation de données personnelles, il est essentiel de savoir quelles données détient le Groupe et quels sont les risques encourus.

Il est important pour toute société de tenir un registre* recensant l'ensemble des données personnelles*traitées, les finalités des traitements, les destinataires des données, les durées de conservation et les mesures de sécurité mises en place. Ce premier travail de cartographie permet en effet d'identifier les traitements susceptibles de comporter un risque pour les droits et libertés des personnes et ceux qui portent sur des données sensibles.

Une analyse d'impact relative à la protection des données* devra par la suite être menée pour étudier plus en détail les risques propres à ces traitements.

Le Groupe peut également réaliser un auto-diagnostic pour évaluer son niveau de sécurité informatique. La CNIL a établi à cette fin une "check list" des mesures prises ou non par le Groupe : https://www.cnil.fr/sites/default/files/atoms/files/check_list_0.pdf Ces actions permettent d'identifier les dangers et les vecteurs d'attaques potentiels afin de mettre en place des mesures de prévention adéquates.

3. Quelles sont les obligations du Groupe en cas de violation de données personnelles ?

En cas de survenance d'une violation de données personnelles, comme évoqué précédemment, le Groupe se doit réagir de manière appropriée et au plus vite afin de mettre un terme à la violation et d'atténuer au possible ses conséquences.
A terme, elle doit également tirer les conséquences de la violation de données et renforcer sa sécurité en cas de défaillance.

Le Groupe est également soumis à plusieurs autres obligations, en vertu des articles 33 et 34 du RGPD.

L'étendue des obligations du Groupe est conditionnée à la détermination par l'équipe de gestion de l'existence et du niveau de risque que la violation fait encourir aux personnes concernées.

➢ **Si la violation présente un risque pour les personnes concernées**

Une violation faisant courir un risque aux personnes doit être notifiée à la CNIL.
La notification complète doit être transmise via un téléservice par le Groupe à la CNIL dans les meilleurs délais et au maximum dans un délai de 72h à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

Le formulaire de notification est directement accessible sur le site de la CNIL: https://notifications.cnil.fr/notifications/index. Le Groupe devra dans la mesure du possible renseigner les éléments suivants :

- une description de la nature de la violation de données, le type de violation y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de données à caractère personnel concernées ;
- le nom et les coordonnées du Délégué / Référent à la Protection des Données Personnelles ou d'un autre point de contact auprès duquel il est possible d'obtenir plus d'informations sur la violation ;
- 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.

Si le Groupe ne peut pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, le Groupe peut effectuer une notification en deux temps :

➔ Une notification initiale dans un délai de 72 heures si possible à la suite de la constatation de la violation.

Si le délai de 72 heures est dépassé, le Groupe doit expliquer, lors de la notification, les motifs du retard.

Néanmoins, celles-ci doivent rester exceptionnelles et fondées sur de réels motifs légitimes.

➔ Enfin, une notification complémentaire dès lors que les informations complémentaires sont disponibles.

Si une enquête approfondie, après une notification précoce, révèle que l'incident de sécurité a été endigué ou qu'aucune violation ne s'est réellement produite, le Groupe peut en informer l'autorité de contrôle.

Par exemple, si le Groupe informe l'autorité de contrôle de la perte d'une clé USB contenant des données à caractère personnel mais que cette clé USB est ensuite retrouvée mal rangée dans des locaux, il peut en informer l'autorité de contrôle par une notification complémentaire modifiant la notification initiale.

Aucune sanction n'est prévue en cas de notification d'un incident qui s'avère, en fin de compte, ne pas constituer une violation.

➢ **Si la violation présente un risque élevé pour les personnes concernées**

Une violation faisant courir un risque élevé aux personnes concernées doit être documentée en interne, notifiée à la CNIL et faire l'objet d'une information auprès des personnes concernées.

La notification à l'autorité de contrôle ne peut en aucun servir de justification à la non-communication de la violation aux personnes concernées lorsque celle-ci est nécessaire.

Le contenu de la notification aux personnes concernées est similaire à celle qui doit être faite à la CNIL.

La description de la nature de la violation et des mesures de sécurité mises en place doit être expliquées en des termes clairs et simples. Il est fortement conseillé au Groupe d'indiquer aux personnes concernées toute recommandation visant à atténuer les effets négatifs de la violation de données (ex : changement immédiat de mots de passe.)
La notification doit en principe, être effectuée par le Groupe directement auprès des personnes concernées, à moins que cela implique un effort disproportionné. Dans ce cas, une communication publique ou une mesure similaire doit être mise en œuvre par le Groupe pour que les personnes concernées soient informées de la violation de leurs données.

La notification n'est pas obligatoire :

- si 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) ;
- si des mesures ultérieures garantissant que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se produire, ont été mises en œuvre.

➢ **Si la violation ne présente pas de risque pour les personnes concernées**

Une violation ne faisant pas courir de risque aux personnes concernées devra simplement être documentée en interne dans un registre des violations des données personnelles*
Par exemple : si les données personnelles affectées par la violation sont déjà disponibles pour le public "données publiques" et qu'une divulgation desdites données n'est pas susceptible d'engendrer un risque pour les personnes concernées.

➢ **La documentation en interne /l'inscription de la violation dans un registre des violations des données personnelles**

Le Groupe doit documenter toute violation de données à caractère personnel, indépendamment de sa notification éventuelle à l'autorité de contrôle et aux personnes concernées. Le Groupe doit consigner des informations concernant la violation dans un registre des violations établi à cette fin.

Ce registre doit être tenu par la personne chargée de la sécurité des données au sein du Groupe et mis à jour régulièrement.

Il doit comprendre à minima :

- la date et l'heure de la violation
- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- la date de notification à la CNIL
- le cas échéant, la justification du retard ou de l'absence de notification auprès de la CNIL ou d'information aux personnes concernées.

La tenue à jour d'un tel registre permet de contrôler la conformité du Groupe au RGPD et d'assurer

un suivi notamment dans le cas d'un changement de circonstances qui pourrait obliger le Groupe a finalement notifier une violation de données passée (ex : une clé de chiffrement d'un fichier volé, dont une copie a été conservée, qui a été ultérieurement compromise).

Action / Risque	Pas de risque	Risque	Risque élevé
Notification à la CNIL	non	oui	oui
Notification aux personnes concernées	non	non	oui
Documentation en interne	oui	oui	oui

4. Que faire en cas de sous-traitance ?

➢ **Si le Groupe qui a subi la violation de données personnelles est sous-traitant et agit pour le compte et au nom d'un responsable de traitement**

Si le Groupe agit en tant que sous-traitant*, il doit informer dans les meilleurs délais (maximum de 48h) le responsable du traitement*. Cette information est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à la CNIL.

L'information doit être, au moins, accompagnée des éléments suivants :

- Une description de la nature de la violation de données à caractère personnel, 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 ;
- Une communication du nom et des coordonnées du Délégué / Référent à la Protection des Données Personnelles ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Une description des conséquences probables de la violation de données à caractère personnel ;
- Une description des mesures prises ou que le Groupe 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.

Le Groupe doit accompagner et aider le responsable de traitement dans le cadre de la notification d'une violation de données à caractère personnel à la CNIL en répondant aux demandes du responsable de traitement sans délai.

➢ **Si un des sous-traitants du Groupe est victime d'une violation de données personnelles**

Lorsqu'un sous-traitant du Groupe est victime d'une violation de données personnelles, ce dernier doit informer le Groupe des éléments cités ci-dessus dans les plus brefs délais et au plus tard dans les 48 heures à partir du moment où le sous-traitant a eu connaissance de cette violation.
Cette information doit être fournie au Référent à la Protection des Données Personnelles du Groupe en envoyant une communication à l'adresse suivante : rgpd@gb-group.co

Par la suite, le sous-traitant doit coopérer avec le Groupe, afin de permettre à celle-ci de respecter ses obligations en tant que responsable du traitement.

Nota Bene : il est possible d'envisager qu'un des sous-traitants notifie la CNIL au nom et pour le Groupe. Ce point doit être prévu au contrat qui lie le sous-traitant et le Groupe sans pour autant que cela ne délie le Groupe de ses obligations et de sa responsabilité.

5. Quid après la violation ?

➢ **La mise en œuvre de mesures correctrices et la revue post incident de la violation de données personnelles**

Une fois l'incident de sécurité maîtrisé, il est important que l'équipe de gestion, au complet si possible (le dirigeant n'a pas besoin d'être présent) rédige dans un temps raisonnable un rapport de synthèse comportant a minima :

- le bilan financier de l'incident ayant conduit à la violation ;
- le bilan processuel de l'incident ayant conduit à la violation ;
- la description la plus précise possible de l'incident de sécurité ayant conduit à la violation de données ;
- le type de violation ;
- les incidences de la violation sur les personnes concernées ;
- les éléments techniques sur le traitement et la résolution de l'incident ayant conduit à la violation.

Ce rapport va servir à l'équipe de gestion lors d'une revue post-incident.
La revue post incident consiste à reprendre les mesures mises en place lors de la survenance de la violation afin d'en évaluer l'efficacité et d'améliorer les processus de sécurité internes.
Il est important d'analyser avec recul ce qui a bien fonctionné et moins bien fonctionné dans le traitement de l'incident ayant conduit à la violation de données afin de prendre, le cas échéant, de nouvelles mesures ou de corriger celles déjà existantes.

Le rapport de synthèse doit documenter les conclusions de l'équipe de gestion ceci afin de présenter toutes les informations à la direction pour commencer à améliorer les protocoles de sécurité et pouvoir budgétiser les process à mettre en place.
Il convient également pour le Groupe de sensibiliser ses salariés à la sécurité informatique de manière accrue afin de limiter la survenance d'incidents de sécurité et ainsi endiguer le risque de violation de données personnelles.

6. Annexes

Annexe 1. Glossaire

TERMES	DÉFINITIONS
Donnée personnelle	Désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); 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.
Registre des traitements	Le registre de traitement permet de recenser les traitements de données du Groupe. Le registre est une obligation prévue par l'article 30 du RGPD. Il participe à la documentation de la conformité du Groupe. Document de recensement et d'analyse, il doit être mis régulièrement à jour, refléter la réalité des traitements de données personnelles du Groupe et lui permettre d'identifier précisément : - les parties prenantes (responsable de traitement, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données ; - les catégories de données traitées ; - les finalités des traitements (à quoi servent les données) ; - les personnes concernées ; - les destinataires des données ; - la durée de conservation des données personnelles ; - la sécurisation des données personnelles ; - les mesures de suppression et d'archivage des données personnelles.
Analyse d'impact	L'Analyse d'impact est un outil important pour la responsabilisation du Groupe. Elle permet au Groupe de construire des traitements de données respectueux de la vie privée, mais aussi à démontrer sa conformité au Règlement général sur la protection des données (RGPD). Elle est obligatoire pour les traitements susceptibles d'engendrer des risques élevés. L'Analyse d'impact se décompose en trois parties : - Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels ; - L'évaluation juridique de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) fixés par la loi et doivent être respectés, quels que soient les risques ; - L'étude technique des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données concernées.
Règlement Européen sur la protection des données personnelles (RGPD)	Désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des

	données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) : Plus d'informations ici : https://www.cnil.fr/fr/reglement-europeen-protection-donnees
Intégrité des données personnelles	L'intégrité des données est l'exactitude, l'exhaustivité et la cohérence globales de ces données durant tout leur cycle de vie.
Confidentialité des données personnelles	La confidentialité des données est la protection de ces données contre l'interception et la lecture par des personnes non autorisées.
Disponibilité des données personnelles	La disponibilité des données est l'accessibilité de ces données et l'opérationnalité des services durant tout le cycle de vie des données.
CNIL (Commission Nationale de l'Informatique et des Libertés)	La Commission Nationale de l'Informatique et des Libertés est une autorité administrative indépendante chargée de la protection des données personnelles en France. En tant que régulateur, elle veille au respect du règlement général sur la protection des données (RGPD) et de la loi Informatique et Libertés modifiée : - elle conseille et accompagne les responsables de projets numériques ; - elle accompagne les Délégués à la Protection des Données Personnelles (DPO) désignés par les sociétés, les associations et les services publics ; - elle analyse les conséquences des innovations technologiques sur la vie privée et les libertés, et émet des recommandations ; - elle autorise les traitements de données présentant une sensibilité particulière ; - elle a un pouvoir de contrôle et de sanction administrative ; - elle travaille en étroite collaboration avec ses homologues européens et internationaux. Plus d'informations ici : https://www.cnil.fr/

Mesures de protection techniques et organisationnelles appropriées	Les « mesures techniques » sont les mesures de protection prises par le Groupe pour sécuriser les données. Il peut s'agir par exemple : - du chiffrement des données confidentielles ; - de la gestion des droits d'accès ; - de la mise en œuvre d'outils de lutte contre les intrusions extérieures dans le réseau (firewall, anti-virus) - d'une politique de mots de passe (complexité, changement régulier) - d'une protection des communications de fichiers contenant des données personnelles via des flux sécurisés (TSL/SSL, https) Les « mesures organisationnelles " renvoient aux mesures de confidentialité et de protection de la vie privée mises en place par le Groupe. Par exemple : - Une cartographie des traitements réalisés par le Groupe et la tenue à jour du registre des traitements ; - La revue intégrale des contrats sous l'angle du RGPD (sous-traitants, partenaires, salariés, clients); - La sensibilisation/formation des équipes métiers et IT au RGPD et à la sécurité informatique ; - Une politique de minimisation des données (ne collecter que les données strictement nécessaires à la réalisation du traitement) - De l'analyse de risque (analyses d'impact) ; - La mise en place d'une procédure de gestion des droits des personnes sur leurs données personnelles.
PCA / PRA	Un Plan de continuité d'activité (PCA) est une procédure en place au sein du Groupe qui vise à mettre en œuvre l'ensemble des processus, des moyens humains, matériels et technologiques pour permettre au Groupe de continuer sans interruption son activité, même en cas de sinistre majeur. Un Plan de Reprise d'activité (PRA) est une procédure en place au sein du Groupe qui vise à mettre en œuvre l'ensemble des processus, des moyens humains, matériels et technologiques pour permettre au Groupe de reprendre son activité suite à un sinistre informatique majeur. La notion de « sinistre majeur » est très variable d'une société à une autre.
Registre des violations des données personnelles	L'article 33.5 du RGPD impose au Groupe de constituer et de tenir à jour un registre dédié et répertoriant toutes les violations de données personnelles qui ont lieu au sein du Groupe y compris celles qui ne sont pas automatiquement sujettes à une notification externe (CNIL et personnes concernées)
Responsable de traitement	Désigne 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. Si le Groupe confie le Traitement à un tiers agissant en tant que Sous-Traitant (toute personne traitant des données à caractère personnel pour le compte du Responsable de Traitement est considérée comme un Sous-Traitant), le Groupe sera toujours considéré comme étant le Responsable de Traitement. Le Groupe peut aussi avoir la qualité de Responsable de Traitement lorsqu'elle procède au traitement d'un fichier de données personnelles qui lui a été transmis, exploite ce fichier ou encore extrait des données personnelles de ce fichier.

Sous-traitant	Désigne 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.
Personnes concernées	Désigne les personnes auprès desquelles sont recueillies les données à caractère personnel. Ex : prospects, clients, fournisseurs, employés, travailleur temporaire, sous-traitants, auditeurs, visiteurs, passagers, etc.
Délégué à la Protection des Données Personnelles	La mission principale du Délégué à la Protection des Données Personnelles est d'assister le responsable du traitement ainsi que le sous-traitant dans leur démarche de conformité au RGPD. Le Responsable du Traitement (et le Sous-Traitant le cas échéant) désigne(nt) obligatoirement un Délégué à la Protection des Données Personnelles lorsque : - le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ; - les activités de base du Responsable du Traitement ou du Sous-Traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; où - les activités de base du Responsable du Traitement (ou du Sous-Traitant) consistent en un Traitement à grande échelle de catégories particulières de données sensibles et de données à caractère personnel relatives à des condamnations pénales et à des infractions pénales. Un groupe de sociétés peut désigner un seul Délégué à la Protection des Données Personnelles à condition qu'un Délégué à la Protection des Données Personnelles soit facilement joignable à partir de chaque lieu d'établissement.