MINDBAZ

Procédure interne
Faille de sécurité

Table des matières

1. Approche générale

Cette procédure interne a pour objet de présenter à la **société MINDBAZ, société par actions simplifiée située 125 Avenue de la république, 59110 LA MADELEINE, enregistrée au Registre du commerce et des sociétés de LILLE METROPOLE sous le numéro 893278382 et représentée par son Président Monsieur Sébastien LEMIRE** les aspects stratégiques et juridiques relatifs à la problématique des failles informatiques de sécurité mettant en cause des données à caractère personnel sur le territoire français.

Le renforcement des obligations de sécurité des systèmes d'information s'inscrit dans le cadre du Règlement européen sur la protection des données adopté le 27 avril 2016 (« RGPD »). En effet, le RGPD instaure une obligation spécifique de sécurité des données à caractère personnel[1].

Ce renforcement des obligations implique de nouvelles obligations de sécurité entrainant la prise de mesures concrètes en cas d'attaque de sécurité au sein du système d'information de LA SOCIETE.

2. Définition

Dans le cadre de la présente procédure, les termes clefs visent la signification ci-après définie.

2.1 Faille de sécurité

Une faille de sécurité est une vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient[2].

2.2 Donnée à caractère personnel

Une donnée à caractère personnel est une donnée permettant d'identifier directement ou indirectement une personne physique.

L'article 4.1 Règlement 2016/679 du 27 avril 2016 définit ainsi la « donnée à caractère personnel », comme « 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 ».

2.3 Violation de données à caractère personnel

La notion de violation implique, quant à elle, une transgression d'une règle, d'une loi ou d'un accord.

---

[1] RGPD art. 37

[2] Stratégie de la France, Anssi, 2011, pp. 21-22.

La notion de violation de données à caractère personnel renvoie à la situation dans laquelle une faille de sécurité aurait des conséquences sur l'intégrité ou à la confidentialité de données à caractère personnel.

La violation de données à caractère personnel 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 à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données ».[3]

3. Les obligations de sécurité (Présentation générale)

Les failles de sécurité concernent la violation de l'une ou plusieurs exigences suivantes :

- la protection dès la conception ;
- la protection par défaut ;
- la sécurité stricto sensu ;
- la notification des violations de données personnelles ;
- la communication auprès des personnes physiques concernées par la violation.

3.1 Obligation de protection dès la conception

3.1.1 Principe

La première obligation imposée par le RGPD est relative à la protection des données à caractère personnel dès la conception du traitement ainsi que sur la protection des données par défaut. Cette protection comprend l'ensemble des obligations et notamment l'obligation de sécurité générale[4].

3.1.2 Mise en œuvre

Cette obligation comprend la prise en compte des exigences de sécurité :

- en phase de conception ;
- pendant l'exploitation et la maintenance ;
- pour les sauvegardes et les procédures d'archivage.

3.2 L'obligation de protection par défaut

3.2.1 Principe

Cette exigence impose une obligation de garantie que « seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité »[5].

3.2.2 Mise en œuvre

L'application suppose la mise en pratique de mesures organisationnelles et techniques.

---

[3] RGPD art. 4 (12)
[4] RGPD art. 25 al. 1
[5] RGPD art. 25 al. 2

3.3 Obligation de sécurité[6]

3.3.1 Sécurité du traitement et limitation d'accès

Cette obligation de sécurité érigée par l'article 32 du RGPD s'adresse non seulement au responsable de traitement, mais également aux sous-traitants.

Ces derniers doivent garantir un niveau de sécurité adapté au risque du traitement.

Tout comme le prévoit l'article 25 du RGPD sur la protection des données, le responsable de traitement et le sous-traitant seront dans l'obligation de limiter l'accès aux données à caractère personnel.

3.3.2 Mise en œuvre

Le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment, selon les besoins, de la façon suivante:

- pseudonymisation et cryptage des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitement des données à caractère personnel ;
- des moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
- une procédure d'évaluation du niveau de sécurité en tenant compte des risque que présente le traitement et notamment la destruction, perte, altération, divulgation non autorisée ou accès non autorisé accidentelle ou illicite ;
- une mise en place notamment d'une liste limitative des personnes autorisées à accéder au traitement ainsi qu'une mise en place technique du contrôle de ces accès.

Les mesures de sécurité sont mises en œuvre en tenant compte de :

- la nature ;
- la portée ;
- le contexte ;
- les finalités du traitement ;
- le risque pour les droits et libertés des personnes physiques.

Le RGPD suggère la mise en place de deux solutions :

- l'adoption d'un « code de conduite » (article 40 RGPD) ;
- ou l'adoption d'un « mécanisme de certification » (article 42 RGPD).

3.4 Obligation de notification[7]

Le RGPD introduit une obligation générale de notification des violations de données. En cas de violation de données, le responsable de traitement sera donc tenu de la notifier à la

[6] RGPD art. 32
[7] RGPD art. 33

CNIL, voire aux personnes concernées, si cette notification résulte en un risque élevé pour les droits et les libertés des personnes.

Cette obligation est extrêmement vaste et il peut être difficile de déterminer les cas pour lesquels une notification est requise.

En outre, les notifications de sécurité doivent comprendre les mentions listées dans le RGPD.

3.4.1 Obligation du responsable de traitement

Sauf dans les cas où la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, le responsable de traitement devra toujours la notifier à l'autorité de contrôle compétente, au plus tard dans les 72 heures après en avoir pris connaissance.

3.4.2 Mise en œuvre

L'article 33 du RGPD prévoit ainsi de :

- mettre en place des mesures permettant d'analyser les risques du traitement mis en place pour les droits et libertés des personnes physiques ;
- s'assurer de notifier les violations dans un délai de 72 heures auquel cas il devra fournir des explications sur ce retard à la CNIL ou autorité nationale compétente dans l'État concerné ;
- indiquer les faits concernant la violation, la nature de cette violation, ses effets ainsi que les mesures prises pour y remédier ;
- faire tous ses efforts afin de documenter au mieux toute violation pour permettre à l'autorité de contrôle de vérifier le respect des exigences imposées par le RGPD ;
- mettre en place des mesures d'urgence afin de pouvoir remédier à la violation ainsi que d'en atténuer ses conséquences.

3.4.3 Obligation du sous-traitant

L'article 33 du RGPD fait peser le même type d'obligation de notification sur le sous-traitant : il devra notifier au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

3.4.4 Mise en œuvre

Le RGPD étant muet quant à la mise en œuvre des obligations du sous-traitant, il est conseillé d'établir certains documents annexes au contrat le liant au responsable de traitement afin de lui permettre de satisfaire à sa propre obligation de notification aux autorités de contrôle :

- rédaction d'un plan d'assurance sécurité (PAS) afin de préciser les dispositions prises par le sous-traitant pour répondre aux exigences de sécurité du responsable de traitement ;
- rédaction d'une annexe dans laquelle serait décrite la procédure à adopter par le sous-traitant en cas de violation de sécurité des données à caractère personnel ;
- modification des clauses de sous-traitance pour prendre en compte les nouvelles obligations ;
- mise en place d'une procédure spécifique de gestion de violations de données dans un délai de 24 heures à partir de la violation. Cette procédure pourra prendre la forme d'une cellule de crise interne au sein de LA SOCIETE.

3.5 Obligation de communication[8]

3.5.1 Obligation de communication du responsable de traitement

Le RGPD impose au responsable de traitement, sauf dans les cas où la violation n'engendre pas un risque élevé pour les droits et libertés d'une personne physique, de communiquer directement à la personne concernée la violation.

Le règlement ne définit toutefois pas comment évaluer la notion de « risque élevé ».

Toutefois, cette communication ne sera pas nécessaire si :

- des mesures techniques et organisationnelles ont rendues les données incompréhensibles pour toute personne (ex. : chiffrement) ;
- des mesures ont été prises pour que le risque ne soit plus « susceptible de se matérialiser ».

De plus, le RGPD autorise une communication « publique » plutôt que directe si la communication exige des « efforts disproportionnés ».

3.5.2 Mise en œuvre

Le RGPD prévoit de :

- définir le « risque élevé » afin d'être cohérent sur les communications à effectuer aux personnes concernées ;
- qualifier le type de violation dont a été victime le responsable de traitement afin d'évaluer son incidence sur la personne concernée. La communication doit en effet contenir les fait de la violation, mais également ses conséquences probables et les mesures proposées afin d'y remédier ;
- évaluer les situations nécessitant une communication privée de celles devant faire l'objet d'une communication publique. Des plans de communication seront nécessaires afin d'analyser l'impact d'une telle communication publique.

3.5.3 Réponse à l'injonction de communication de l'autorité de contrôle

Si le responsable de traitement ne procède pas à la communication de la violation de données à la personne concernée, l'autorité de contrôle pourra, après avoir examiné le risque résultant de cette violation, enjoindre le responsable de traitement qu'il procède à cette communication.

3.5.4 Mise en œuvre

Le RGPD prévoit que :

- le responsable de traitement devra respecter le plan d'action prévu par le RGPD et mentionné ci-dessus ;
- il est conseillé d'anticiper tout contentieux avec l'autorité de contrôle en cas de désaccord sur la question de la communication.

[8] RGPD art.34

4. La démarche préconisée : mise en place d'une cellule de crise

Le RGPD impose donc aux entreprises comme LA SOCIETE de nouvelles obligations contraignantes.

En effet, les obligations résultats des articles 25 et 32 à savoir la protection des données ainsi que leur sécurisation nécessitent la mise en place urgente de mesures appropriées afin de se conformer aux exigences du règlement avant sa date d'entrée, à savoir le 25 mai 2018.

Les articles 33 et 34 concernant la notification et la communication des violations imposent, quant à eux, des délais puisque la notification doit être réalisée au plus tard dans les 72 heures après en avoir pris connaissance et la communication doit être effectuée dans les meilleurs délais.

LA SOCIETE est donc dans une situation d'urgence ce qui nécessite de mettre en place une procédure de gestion des failles de sécurité afin de satisfaire aux obligations du RGPD, éviter le risque de sanction de la CNIL qui peut s'élever jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent.

Qu'elles proviennent d'une erreur, d'une négligence ou de procédés illicites, les failles de sécurité représentent aujourd'hui l'une des préoccupations majeures des entreprises.

La sécurité n'est plus une option. Les enjeux de sécurité des systèmes d'information doivent donc se rapprocher des préoccupations économiques, stratégiques et d'images qui sont celles des décideurs[9].

Les violations de failles de sécurité proviennent de sources multiples, mais considérées comme prévisibles : hameçonnage, déni de services, logiciels malveillants, espionnages, demandes de rançons, piratage des systèmes de traitement automatisé de données, perte d'informations confidentielles et stratégiques, vol de données à caractère personnel, et lourds de conséquences sur le plan financier, juridique, économique et d'image.

L'organisme confronté à une atteinte à son système informatique ayant conduit à une violation des données personnelles devra communiquer cet incident en interne et auprès de toutes personnes susceptibles de la solliciter et réagir très rapidement pour éviter toute diffusion d'information erronée ou inexacte, toute atteinte à sa réputation, ou encore mauvaise appréciation de l'impact de l'évènement sur son activité.

La cellule de crise aura de nombreux objectifs dont celui de s'occuper des différentes issues techniques et juridiques à mettre en place, mais également celui de la stratégie de communication à adopter que ce soit vis-à-vis de la CNIL, de la personne concernée, mais aussi des médias.

Sa mise en œuvre est donc essentielle à LA SOCIETE afin de limiter les conséquences néfastes d'une telle faille de sécurité et de préserver sa responsabilité face à ses obligations.

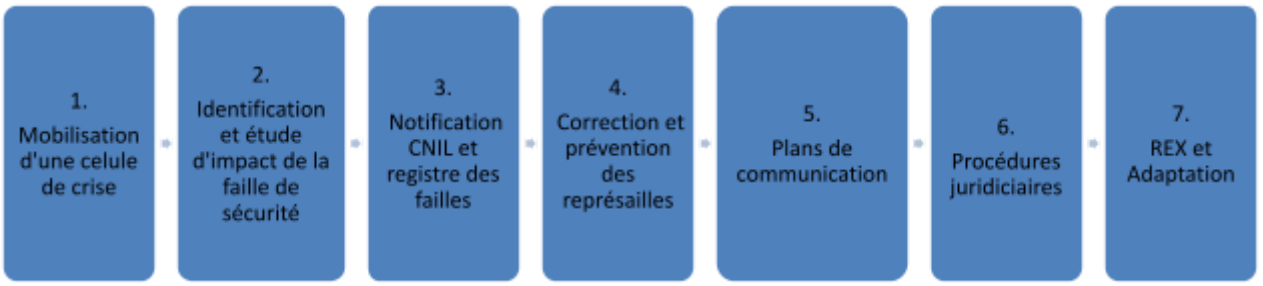
5. Mise en œuvre

Le présent chapitre a pour objet d'expliquer à LA SOCIETE les grands principes de gestion technique des failles de sécurité grâce à la mise en place d'une procédure dédiée.

---

[9] Guide d'hygiène information, ANSSI.

La procédure devra suivre par principe les séquences suivantes comme les grandes étapes de ses actions :



5.1 Prérequis – traçabilité des interventions

QUESTIONS	RÉPONSES
Qu'est-ce qu'une traçabilité des interventions ?	La traçabilité est utilisée afin de pouvoir identifier tout accès frauduleux aux données à caractère personnel ou toute utilisation abusive de ces données. LA SOCIÉTÉ se doit de mettre en place un dispositif permettant d'enregistrer les éléments garantissant la conservation des données. Suggestion de la CNIL : prévoir au minimum la journalisation des accès des utilisateurs incluant leur identifiant, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion. Le format de l'horodatage doit de préférence prendre comme référence le temps UTC10.[10]

5.2 Mobilisation d'une équipe de crise

5.2.1 Équipe de la cellule de crise

QUESTIONS	RÉPONSES
Qui mobiliser ?	Nombre restreint de personnes pour la gestion de crise : En interne, personnes clés dont : - personnes en charge de la sécurité des systèmes d'information (DSI,

[10] Guide CNIL la sécurité des données personnelles 2010.

QUESTIONS	RÉPONSES
	RSSI, administrateurs de la sécurité) ; - personnes en charge de la protection des données à caractère personnel (CIL, Data Privacy Officer, etc.) ; - gestionnaire des risques ; - directeur de la communication ; - directeur juridique ; - directeur général. En externe, personnes clés pourront être adjointes à la cellule crise : - Huissier (ou équivalent) : pour procéder à un procès-verbal de constat pour la copie du système d'information touchée par la violation de données et la faille de sécurité. - Expert (ou équivalent) : pour identifier la faille de sécurité et déterminer le mode opératoire de l'attaque, il est possible de faire appel à une société d'expertise informatique ayant toutes les compétences requises en investigations et les connaissances en matière d'attaques pour établir un rapport d'incident.
Quand mobiliser ?	Il est nécessaire de bien différencier un simple incident d'une véritable situation de crise. La cellule de crise ne sera mise en place que dans les cas où l'attaque du système d'information sera confirmée. Dans ce cas, des équipes seront mobilisées et seront en charge tant de l'investigation que de la défense du système pour éradiquer l'attaque.
Dans quel délai mobiliser l'équipe de crise ?	Immédiatement

5.2.2 Missions de la cellule de crise

Identification de la faille de sécurité et du mode opératoire de l'attaque informatique

QUESTIONS	RÉPONSES
Quel est l'objectif ?	L'objectif est de déterminer le mode opératoire de l'attaque en retraçant les actions effectuées par le pirate informatique (point d'entrée sur le système d'information, mouvements dans le système d'information, finalité de l'attaque, profil du pirate informatique). L'objectif est également de permettre de décrire la nature de la violation des données, les catégories et le nombre de personne concernée par la violation, les catégories et le nombre

QUESTIONS	RÉPONSES
	d'enregistrement de données à caractère personnel concerné. L'objectif est donc de documenter toute violation des données et permettre d'indiquer les faits et les effets de la violation des données.
Qui peut être chargé de cette mission ?	Gestion interne : cellule de crise et/ou société d'expertise informatique externe. Globalement toute personne disposant : - des compétences d'investigations : analyse système, analyse réseau, analyse de codes malveillants, etc. - des compétences sur les techniques d'attaque couramment utilisées pour anticiper les actions et réactions de l'attaquant ; - des connaissances générales sur le système d'information : architecture du système d'information, composants à disposition des équipes, socles systèmes, etc. ; - des connaissances sur les métiers impactés. La documentation doit être gérée par la cellule de crise.
Dans quel délai faut-il agir ?	Immédiatement Remarque : les investigations sur l'attaque mettent habituellement plusieurs jours, parfois plusieurs semaines dans le cas de systèmes de taille importante.

Correction de la faille de sécurité / arrêt de l'attaque informatique

QUESTIONS	RÉPONSES
Quel est l'objectif ?	Stopper l'attaque sur les périmètres du système d'information infectés et éradiquer la menace imminente pesant sur le système (suppression des logiciels malveillants, fermeture de ports ou de flux, désactivation de comptes, etc.). L'objectif est également de pouvoir décrire les mesures prises ou que l'on propose de prendre pour remédier à la violation des données, y compris les mesures pour en atténuer les éventuelles conséquences négatives. L'objectif est de pouvoir documenter les mesures prises pour remédier à la violation des données. Cette documentation est impérative car elle permet à la CNIL de vérifier le respect de l'article 33 du RGPD.
Qui peut être chargé de cette mission ?	Gestion interne : cellule de crise et /ou société d'expertise informatique externe. La documentation doit être gérée par la cellule de crise.

QUESTIONS	RÉPONSES
Quel type de mesures faut-il mettre en place ?	Mesures techniques et organisationnelles, telles que : - coupure de liens réseaux ou de l'accès Internet ; - déploiement de correctifs de sécurité ou de nouveaux logiciels ; - changement de mots de passe ; - installation de nouveaux équipements de protection ; - isolation de certaines entités métiers ; - déplacement d'utilisateurs sur des sites non touchés.
Dans quel délai faut-il agir ?	Immédiatement Remarque : la correction de la faille de sécurité/l'arrêt de l'attaque peut prendre quelques heures à quelques jours, suivant la taille du système touché. S'il n'est pas possible de fournir toutes les informations en même temps, celles-ci sont à conserver de manière échelonnée aux fins de communication à la CNIL.

Prévention des représailles et audit de sécurité

QUESTIONS	RÉPONSES
Quel est l'objectif ?	Éviter la résurgence de l'attaque. En cas de tentative de chantage, mise en place d'une surveillance permettant d'avoir connaissance en temps réel de toute citation sur l'attaque informatique subie (exemple : Google Alertes).
Qui peut être chargé de cette mission ?	Gestion interne : cellule de crise et/ou société d'expertise informatique externe.
Quelles actions mettre en œuvre ?	Quelques actions à mettre en œuvre : - surveillance des périmètres affectés et/ou reconstruits en interne ; - veille pour détecter de possibles réactions ; - vérification de potentielles vulnérabilités sur l'ensemble du système d'information.
Dans quel délai faut-il agir ?	Immédiatement après l'arrêt de l'attaque

5.2.3 Moyens de la cellule de crise

QUESTIONS	RÉPONSES
Quels sont les moyens devant être mis à la disposition de la cellule de crise ?	- systèmes de gestion de crise : messagerie, échange de fichiers ; - compte d'investigation ; - outil technique permettant de centraliser les traces issues des différents systèmes pour permettre leur interrogation ;

QUESTIONS	RÉPONSES
	- mécanisme d'alerte ; - des outils de travail sécurisés ; - des outillages d'investigation : scripts de collecte et d'analyse (de journaux d'évènements, de disques durs, de mémoire vive, etc.); - outils d'analyse de logiciels suspects ; - matériel d'investigation numérique ; - des moyens d'accès à l'intégralité du système d'information touché (mot de passe, compte d'administration, etc.) devant également être protégés ; - documentation type : rapport descriptif, lettre de notification à la CNIL, lettre d'information aux personnes concernées.

5.3 Identification et impact

L'objectif de cette phase est de réaliser un dossier de preuve technique en vue de la qualification juridique des faits et impact résultant de la violation des données.

5.3.1 Constitution d'un dossier de preuves techniques

QUESTIONS	RÉPONSES
Quel est l'objectif ?	Anticiper la déperdition des preuves et conférer une valeur juridique aux preuves techniques déjà à disposition. Le dossier de preuve pourra également être transmis en tant que de besoin à la CNIL.
Quels éléments peuvent constituer le dossier de preuves techniques ?	Le dossier de preuves techniques peut être composé des éléments suivants : - copie du système qui n'est ni en exploitation ni en analyse ; - rapport incident et logs de connexions au serveur ; - procès-verbal de constat d'huissier.
A qui faire appel pour constituer ce dossier de preuves techniques ?	Cellule de crise accompagnée éventuellement d'un huissier de justice pour la copie du système. Cellule de crise accompagnée de la société d'expertise informatique qualifiée PASSI pour l'établissement du rapport d'incident. Huissier de justice (territorialement compétent) pour l'établissement d'un procès-verbal de constat. Conseil juridique pour superviser la constitution du dossier de preuves techniques et assurer le lien avec l'huissier de justice (rédaction d'une note d'instruction permettant à l'huissier

	d'établir son procès-verbal de constat, notamment)
Dans quel délai faut-il agir ?	Immédiatement

5.3.2 Qualification juridique

QUESTIONS	RÉPONSES
Quel est l'objectif de la qualification juridique des faits ?	Préalable à la rédaction de la plainte simple et à l'action judiciaire
Qui contacter ?	Conseil juridique
Dans quel délai opérer un travail de qualification juridique des faits ?	Dès réception des premières investigations pour un dépôt de plainte rapide

5.3.3 Rapport d'impact de la violation

QUESTIONS	RÉPONSES
Pourquoi faut-il déterminer l'impact de la violation ?	Évaluation de la situation quant aux conséquences probables de la violation des données à caractère personnel. Évaluer si les mesures prises afin de remédier à la violation ont réduit ou supprimer ces conséquences. Il est également impératif de prévoir un rapport d'impact pour notification à la CNIL.
Quel est le contenu du rapport d'impact ?	- la description de la nature de la violation, y compris si possible les catégories et le nombre approximatif de personnes concernées par la violation ; - le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations peuvent être obtenues ; - la description des conséquences de la violation des données ; - les mesures à prendre ou proposées pour remédier à la violation de données, ou le cas échéant pour en atténuer les conséquences négatives. Le rapport d'impact devra également servir à vérifier si la violation des données est susceptible ou pas d'engendrer un risque pour les droits et libertés des personnes physiques. En effet : si ce risque n'existe pas, il n'y a pas d'obligation de notification à la CNIL.

5.4 Notification auprès de la CNIL de l'atteinte au système informatique ayant conduit à une violation des données à caractère personnel

QUESTIONS	RÉPONSES
La violation de données à caractère personnel doit-elle être notifiée à la CNIL ?	Oui quand la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques (obligation de l'article 33 RGPD), c'est-à-dire de leur causer des dommages physiques, matériels ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation, une perte de confidentialité de données à caractère personnel protégées par le secret professionnel ou tout autre dommage économique ou social important.
Dans quel délai faut-il notifier la violation de données à la CNIL ?	La notification doit être faite dans les meilleurs délais et au plus tard 72 heures à compter de la connaissance de la violation. Pour apprécier le délai raisonnable, le responsable de traitement doit tenir compte en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Si la notification à la CNIL n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. Par ailleurs, des informations peuvent être fournies de manière échelonnée sans autre retard indu. Pour le sous-traitant, il doit notifier, dans les mêmes conditions, au responsable de traitement la violation de données après en avoir pris connaissance.
Comment procéder à la notification auprès de la CNIL ?	Aucune condition de forme n'est prévue.
Que doit contenir la notification ?	La notification doit contenir : - la description de la nature de la violation, y compris si possible les catégories et le nombre approximatif de personnes concernées par la violation ; - le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations peuvent être obtenues ; - la description des conséquences de la violation des données ;

QUESTIONS	RÉPONSES
	- les mesures à prendre ou proposées pour remédier à la violation de données, ou le cas échéant pour en atténuer les conséquences négatives. Le RGPD demande également au responsable de traitement de fournir une documentation de la violation permettant d'indiquer les faits concernant la violation, ses effets et les mesures prises.
Qui contacter pour rédiger la notification ?	Conseil juridique
Qui adresse la notification à la CNIL ?	L'article 33 1° du RGDP prévoit que c'est le responsable du traitement qui doit notifier la violation à l'autorité compétente. L'article 33 2° du RGDP prévoit quant à lui que le sous-traitant doit notifier au responsable du traitement dans les meilleurs délais dans le cas où il où détecterait une faille de sécurité dans ses propres systèmes. En conséquence, si le responsable du traitement n'a pas été informé par le sous-traitant d'une faille de sécurité, c'est le sous-traitant qui devrait être reconnu responsable de l'absence de notification.

5.5 Tenue d'un inventaire de violation de données à caractère personnel

QUESTIONS	RÉPONSES
Un inventaire des violations de données à caractère personnel doit-il être établi ?	L'article 33, 5. impose au responsable du traitement de « documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article ».
Quelle forme doit avoir l'inventaire?	Aucune condition de forme n'est requise.
Que doit recenser l'inventaire ?	L'inventaire doit recenser : - le descriptif de la violation de données ; - ses effets ; - les mesures techniques et organisationnelles mises en œuvre pour y remédier. Il doit détailler les modalités de la violation de données, c'est-à-dire : - l'application concernée ; - les données concernées ; - la description de la faille ; - s'il y a lieu, le mode opératoire utilisé par l'attaquant.

5.6 Communication à la personne concernée

QUESTIONS	RÉPONSES
La violation de données à caractère personnel doit-elle être communiquée à la personne concernée ?	L'article 34 du RGPD introduit une obligation de communication de la violation de données à caractère personnel à la personne concernée. Par ailleurs, la CNIL peut imposer l'information des personnes concernées.
Qui est la personne concernée ?	La personne concernée est la personne physique pour laquelle la violation de données est susceptible d'engendrer un risque élevé pour ses droits et libertés.
Quelles informations doivent être communiquées ?	La communication à la personne concernée contient la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, b), c) et d) du règlement, à savoir : - le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations peuvent être obtenues ; - la description des conséquences de la violation des données ; - les mesures à prendre ou proposées pour remédier à la violation de données, ou le cas échéant pour en atténuer les conséquences négatives.
Dans quel délai la communication doit-elle être effectuée ?	La communication doit être adressée dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée.
Sous quelle forme la communication doit-elle être effectuée ?	Aucune condition de forme n'est prévue. Dès lors que cette mesure est faite pour atténuer un risque immédiat de dommage, la communication doit être réalisée en coopération avec l'autorité de contrôle, dans le respect de ses directives données par celle-ci ou par l'autre autorité compétente, telles que les autorités répressives.
Dans quels cas aucune communication ne doit être effectuée ?	Il existe des dérogations à la communication des violations de données personnelles aux personnes concernées lorsque : - le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y

QUESTIONS	RÉPONSES
	avoir accès, telles que le chiffrement ; - le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ; - elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

5.7 Correction et prévention des représailles : déclenchement du PCA (plan de continuité d'activité)

QUESTIONS	RÉPONSES
Qu'est-ce qu'un PCA ?	En cas d'attaque du système d'information de LA SOCIÉTÉ, cette dernière doit mettre en œuvre des mesures permettant le bon fonctionnement de ce système grâce à un PCA. Il est en effet indispensable à LA SOCIÉTÉ de pouvoir continuer son activité par le commerce électronique et par d'autres voies. La cellule de crise devra donc autoriser le déclenchement du PCA.
Quand déclencher le PCA ?	Dès que possible après avoir eu confirmation de l'imminence d'une violation des données à caractère personnel faisant état d'une faille de sécurité.

5.8 Plans de communication

5.8.1 Plan de communication interne

QUESTIONS	RÉPONSES
Qui sont les personnes concernées par le plan de communication interne ?	- salariés ; - actionnaires ; - syndicats.
Quel type de document peut être utile au plan de communication ?	Lettre d'information
Quand procéder à la communication sur l'attaque informatique ?	Si les circonstances l'exigent. Pas d'obligation de communiquer sur l'évènement.
Qui peut être en charge du plan de communication ?	Direction de la communication, en coordination avec la cellule de crise et le conseil juridique.

5.8.2 Plan de communication externe

QUESTIONS	RÉPONSES
Qui sont les personnes concernées par le plan de communication ?	- consommateurs et toutes personnes concernées par l'attaque informatique/faille de sécurité ; - clients ; - fournisseurs ; - partenaires ; - presse.
Quel type de document peut être utile au plan de communication ?	- lettre d'information - bandeau informatif sur le site internet - Information sur les réseaux sociaux (Facebook et Twitter) - communiqué de presse
Quand procéder à la communication sur l'attaque informatique ?	Si les circonstances l'exigent. Pas d'obligation de communiquer sur l'évènement.
Qui peut être en charge du plan de communication ?	Direction de la communication, en coordination avec la cellule de crise et le cabinet Bignon Lebray.

5.9 Gestion des assurances

QUESTIONS	RÉPONSES
Quel préalable à la déclaration de sinistre ?	Vérification de la police d'assurance.
Quand faire la déclaration de sinistre ?	Dès que possible après le dépôt de la plainte auprès du procureur de la République.

5.10 Procédures judiciaires

5.10.1 Plainte

QUESTIONS	RÉPONSES
Quel est le préalable au dépôt de la plainte ?	Signature de la plainte par le représentant légal de la société. A défaut de pouvoir signer la plainte, une délégation de pouvoir spéciale est nécessaire. Cette délégation de pouvoir doit être signée par le représentant légal de la société.
Auprès de qui déposer la plainte ?	Dépôt de plainte auprès du procureur de la République territorialement compétent (art. 43 du Code de procédure pénale), c'est-à-dire le procureur : - du lieu de l'infraction (exemple : lieu de situation des serveurs) ; - celui de la résidence de l'une des personnes soupçonnées d'avoir participé à l'infraction ; - celui du lieu d'arrestation d'une de ces personnes.
Qui se charge de déposer la plainte ?	Conseil juridique
Dans quel délai déposer la plainte ?	Dès que possible
Quels effets produit le dépôt de plainte ?	Le procureur de la République a 3 mois à compter du dépôt de la plainte pour apprécier

QUESTIONS	RÉPONSES
	l'opportunité de donner une suite judiciaire à l'affaire. Si dans ce délai, il informe la victime d'un classement sans suite ou s'il ne répond pas, la victime est alors recevable à se constituer partie civile devant le juge d'instruction, en application de l'article 85 alinéa 2 du Code de procédure pénale.

5.10.2 Enquête préliminaire

QUESTIONS	RÉPONSES
Quelles actions peuvent être mises en œuvre durant la phase de l'enquête préliminaire ?	Suivi de l'enquête et correspondance avec le procureur de la République et/ou les services de police ou de gendarmerie spécialisés ; transmission au procureur de la République et/ou aux services de police ou de gendarmerie spécialisés de toutes les informations utiles au soutien de la plainte ; préparation des auditions par les services de police ou de gendarmerie.
Qui se charge du suivi de l'enquête?	Le conseil juridique assure le suivi auprès du procureur de la République et des services enquêteurs : BEFTI : brigade d'enquêtes sur les fraudes aux technologies de l'information - service de la police judiciaire dévolu aux infractions informatiques sur la région parisienne. SDLC : sous-direction de lutte contre la cybercriminalité relève de la Direction centrale de la police judiciaire. Compétente pour les attaques à l'encontre d'un système d'information situé à l'extérieur du périmètre d'intervention de la BEFTI. OCLCTIC : office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Compétent sur tout le territoire.

5.10.3 Constitution de partie civile par voie d'intervention ou dépôt de plainte avec constitution de partie civile auprès du juge d'instruction

QUESTIONS	RÉPONSES
Quand se constituer partie civile par voie d'intervention ?	A l'issue de l'enquête préliminaire, si le procureur de la République a décidé de faire citer l'auteur des faits directement devant le tribunal correctionnel ou s'il a décidé l'ouverture d'une information judiciaire confiée à un juge d'instruction.
Quand déposer plainte avec constitution de partie civile ?	A l'issue du délai de 3 mois à compter du dépôt de la plainte simple : si le procureur de la République décide de classer la plainte ou s'il n'a pas répondu à la suite du dépôt de la plainte.
Préalable au dépôt de la plainte avec constitution de partie civile ?	Commande préalable du dossier d'enquête pour connaître les investigations menées par les services enquêteurs.

QUESTIONS	RÉPONSES
Documents nécessaires au dépôt de la plainte avec constitution de partie civile ?	déclaration d'adresse de la partie civile ; bilan et compte de résultats de la société (article 85, alinéa 3, du Code de procédure pénale).
Auprès de qui déposer la plainte avec constitution de partie civile ?	Dépôt de plainte avec constitution de partie civile auprès du Doyen des juges d'instruction territorialement compétent (art. 52 du Code de procédure pénale) à savoir notamment celui du lieu de l'infraction.
Qui se charge de déposer la plainte avec constitution de partie civile?	Conseil juridique
Dans quel délai déposer la plainte avec constitution de partie civile ?	Dès que possible

5.10.4 Procédure devant le tribunal correctionnel

QUESTIONS	RÉPONSES
Qui se charge de la procédure devant le tribunal correctionnel ?	Conseil juridique : rédaction des conclusions de partie civile, audiences de procédure, plaidoirie.

6. Évolution de la démarche

6.1 Retour d'expérience

Mise à jour des procédures internes

QUESTIONS	RÉPONSES
Quel est l'objectif ?	Tirer les enseignements de l'attaque subie pour déterminer les axes d'amélioration envisageables dans la sécurisation du système d'information et des procédures internes à mettre en place. La cellule de crise peut confier au DSI la charge d'établir un rapport annuel relatant les violations, les mesures prises pour y remédier, les actions de sensibilisation et de formation du personnel.
Dans quel délai faut-il agir ?	Après la gestion de la crise.

6.2 Adaptation

QUESTIONS	RÉPONSES
Quel est l'objectif ?	Adapter les méthodologies et/ou les outils selon les besoins exprimés par la situation.
Quelles mesures prendre ?	PCA / PRA : procédures devant être mises en œuvre par LA SOCIÉTÉ en cas d'urgence afin d'assurer la continuité ou la reprise de son activité. PSSI (Politique de sécurité du système d'information) : ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme.

QUESTIONS	RÉPONSES
	Charte SI : cette charte, base de la réglementation des moyens informatiques et de télécommunication, doit comprendre des développements spécifiques relatifs aux données à caractère personnel. Registres des failles : inventaire des violations de données à caractère personnel, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier. Autres politiques.
Dans quel délai faut-il agir ?	Après la gestion de la crise.

7. Cas particuliers

7.1 Origine interne de la violation

QUESTIONS	RÉPONSES
Quel est l'objectif ?	Une faille peut avoir pour origine l'action d'un ou plusieurs salariés.
Qui sont les personnes habilitées à effectuer un contrôle sur les matériels informatiques du salarié ?	La cellule de crise détermine les personnes habilitées au regard de la charte des systèmes d'information. Si la présence d'une personne externe à LA SOCIÉTÉ est nécessaire (huissier de justice, avocat, expert, etc.).
Le salarié concerné doit-il être présent ?	Eléments professionnels Par principe, non. Il est cependant préférable de réaliser le contrôle en présence de l'utilisateur. Eléments identifiés comme étant privés Si les dossiers, fichiers et/ou messages sont identifiés avec la mention « PRIVÉ », le contrôle s'effectuera en présence de l'utilisateur ou en son absence dans les cas suivant : valablement convoqué s'il existe un risque ou un évènement particulier pour LA SOCIÉTÉ [11]. Préférable de remettre ou transmettre une convocation à l'utilisateur que celui-ci soit présent ou absent le jour du contrôle. Il faut lui laisser un délai raisonnable entre la convocation et le moment où le contrôle est effectué.
D'autres personnes doivent-elles être présentes lors du contrôle ?	Il est recommandé de mener les opérations de contrôle en présence : d'une personne destinée à attester du déroulé de l'opération de contrôle (salarié, huissier de justice, etc. à l'exception du RSSI) ; d'une personne disposant des compétences techniques pour réaliser les opérations d'accès

[11] Cass. soc., 17-5-2005 pourvoi n° 03-40017 : « sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé. »

QUESTIONS	RÉPONSES
	et de copies avec l'utilisateur, ou d'utiliser des identifiants d'administrateur permettant de réaliser les copies sans accéder aux documents et informations.
Le recours à un huissier de justice est-il obligatoire ?	Facultatif mais le recours à un huissier de justice est recommandé pour limiter les contestations sur les conditions matérielles du contrôle et le contenu du compte-rendu de l'opération. Présence obligatoire d'un huissier de justice : si le contrôle est réalisé sur un matériel qui n'est pas la propriété de LA SOCIÉTÉ ; si le contrôle est réalisé dans un lieu qui n'appartient pas à LA SOCIÉTÉ ou dont elle ne dispose pas de la jouissance d'occupation ; s'il existe une possibilité ou un doute sur le fait que les agissements illicites aient été réalisés sous le couvert de correspondances privées ou intégrés dans les dossiers privés ; en présence d'un fichier, d'un message et/ou d'un répertoire identifié avec la mention « PRIVÉ ».
Une autorisation judiciaire est-elle nécessaire ?	La Cour de cassation n'exige pas l'autorisation du juge pour ouvrir un message ou un fichier privé « en cas de risque ou d'événement particulier, en présence du salarié concerné ou celui-ci dûment prévenu »[12]. Recommandation : demander au président du TGI de désigner un huissier de justice pour dresser un constat établissant le caractère illicite du message ou du fichier litigieux et mise sous scellés du disque dur de l'ordinateur du salarié concerné (article 145 du CPC) s'il existe un motif légitime de conserver ou d'établir, avant tout procès, la preuve des faits dont pourrait dépendre la solution d'un litige.[13] Sauf s'il existe des circonstances particulières justifiées par le risque de disparition des preuves, la procédure de référé, qui est une procédure contradictoire, doit être préférée à une ordonnance sur requête non contradictoire. LA SOCIÉTÉ devra prouver l'identité du salarié concerné (identifiant, mot de passe). En cas de contrefaçon : procéder par requête à fin de saisie contrefaçon.
Doit-on informer ou recouvrir aux autorités policières ou de gendarmerie ?	En cas de suspicion ou de découverte d'agissements illicites passibles de sanctions pénales, LA SOCIÉTÉ en informera les autorités policières ou de gendarmerie.

[12] Cass. soc., 17-5-2005, n° 03-40017 et Cass. soc., 17-6-2009, n° 08-40274

[13] Art. 145 du Code de procédure civile : « S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé. » ; Cass. soc. 23-5-2007 pourvoi n° 05-17818.

QUESTIONS	RÉPONSES
	Si la personne qui acquiert la connaissance d'un crime ou d'un délit à la qualité de fonctionnaire, elle est tenue d'en donner avis sans délai au Procureur de la République et de transmettre à ce dernier tous les renseignements, procès-verbaux et actes qui y sont relatifs en application de l'article 40 alinéa 2 du Code de procédure pénale.[14]
Quelles sont les modalités pratiques du contrôle ?	Accès à l'outil informatique et de communication électronique Copies Procès-verbal de contrôle
A qui communiquer les éléments découlant du contrôle ?	Personnes habilitées par la cellule de crise.
Quelles sont les précautions à prendre ?	Mise en place d'une gestion du risque d'atteinte à la vie privée et au secret des correspondances Aucun enregistrement vidéo et/ou sonore des opérations sans une autorisation préalable et écrite de l'utilisateur contrôlé. Attention, si un accès à des éléments privés intervient par erreur, il convient de : cesser immédiatement la procédure de contrôle ou d'analyse ; réaliser une copie intégrale du contenu du disque dur de l'ordinateur ainsi que le cas échéant des éléments mobiles associés (CD, clef USB, …) ; informer immédiatement la Direction générale qui prendra une décision quant à la suite de la procédure.
Les éléments doivent-ils être communiqués à la personne contrôlée ?	Absence de l'utilisateur concerné lors du contrôle : aucune copie des éléments du contrôle. Utilisateur est présent : un exemplaire du procès-verbal de contrôle lui est remis.
Les éléments doivent-ils être communiqués à une autorité extérieure ?	Une copie des éléments du contrôle pourra être communiquée à une autorité extérieure si : la demande est expresse et justifiée (commission rogatoire, ordonnance judiciaire, sommation de communiquer par huissier de justice…) ; sur présentation d'un titre (ordre de mission, jugement, ordonnance, commission rogatoire …).

7.2 Incidence internationale

QUESTIONS	RÉPONSES
Que faire en cas d'incidence internationale de la violation ?	Mobilisation des homologues étrangers dans la cellule de crise

[14] Art. 40 al. 2 du Code de procédure pénale : « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au Procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »

QUESTIONS	RÉPONSES
	Vérifications : droit applicable, juridiction compétente, autorité de contrôle compétente et à qui doit-être notifié la violation de la faille.