BOAD

BANQUE OUEST AFRICAINE
DE DÉVELOPPEMENT

LA PROCEDURE DE GESTION ET DE NOTIFICATION DES VIOLATIONS DES DONNEES A CARACTERE PERSONNEL

SOMMAIRE

1. PRESENTATION GENERALE DE LA PROCEDURE 3
1.1. Rappel de la réglementation applicable en matière de notification des violations des données 3
1.2. Objectifs de la procédure 4
1.3. Vocabulaire 4
2. PREPARATION EN AMONT 5
3. CONSEQUENCES DE LA VIOLATION DES DONNEES PERSONNELLES 6
4. NOTIFICATION DE LA VIOLATION DES DONNEES PERSONNELLES 7
4.1. ETAPE 1 : Le moment de la notification 7
4.1.1. ETAPE 1.A) : Reconnaître l'existence de la Violation d'une Donnée Personnelle 7
4.1.2. ETAPE 1.B) : Evaluation de la Violation de la Donnée Personnelle 8
4.1.3. ETAPE 1.C) : Quand notifier 10
4.1.4. ETAPE 1.D) : La notification aux personnes concernées 10
4.2. ETAPE 2 : Contenu de la notification 11
4.2.1. ETAPE 2.A) : Le contenu a minima de la notification au Département Conformité et Règlementation 11
4.2.2. ETAPE 2.B) : Le contenu de la notification à la personne concernée 11
4.3. ETAPE 3 : L'action de l'Autorité de Contrôle – en cas de notification à cette dernière 12
4.4. ETAPE 4 : La documentation 12

1. PRESENTATION GENERALE DE LA PROCEDURE

1.1. Rappel de la réglementation applicable en matière de notification des violations des données

Le Règlement général pour la protection des données, dit RGPD, applicable depuis le 25 mai 2018[1] introduit une obligation pour tout responsable de Traitement de notifier à l'Autorité de Contrôle compétente tout éventuelle Violation des Données Personnelles et, dans certains cas, de notifier également ces violations aux personnes concernées.

Le Règlement européen n°2018/1725 du 23 octobre 2018 relatif à la protection des données personnelles par les institutions, organes et organisme de l'Union Européenne introduit l'obligation pour toute institution, organisme ou organes de l'Union Européenne agissant comme responsable de traitement, de notifier au Contrôleur Européen de la protection des données personnelles de toute violation de données.

En effet, l'objectif de la règlementation applicable en matière de protection des données personnelles est non seulement de renforcer les Droits des Personnes sur les Traitements mais aussi, d'éviter toute violation des Données Personnelles (accès non autorisé, fuite etc.) et donc, de prévenir tout dommage à l'encontre aussi bien du responsable de traitement que des personnes concernées. Ainsi, le RGPD oblige les responsables de Traitement à garantir un niveau de sécurité approprié des Données Personnelles, y compris la protection contre le traitement non autorisé ou illicite et contre la Perte, la Destruction ou les Dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)[2].

La notification doit donc faire partie intégrante de ce processus de traitement des violations déployé.

La BOAD intervient pour les Traitements mis en œuvre en tant que Responsable de Traitement, au sens de la Réglementation, (i) pour les Données Personnelles de ses Collaborateurs et (ii) pour les Données Personnelles de ses Clients Bénéficiaires, Prestataires, Fournisseurs et Sous-traitants, qui peuvent être des citoyens européens ou étrangers.

A ce titre elle doit :

- Déployer des mesures permettant de prévenir les violations des Données Personnelles ; et
- Déployer des mesures lui permettant de réagir rapidement en cas d'incident.

Il convient de noter que le fait de ne pas signaler une violation à une personne ou à une autorité de contrôle peut signifier qu'une sanction éventuelle est applicable au responsable du traitement[3].

Attention

Seuls les cas des Violation de **Données Personnelles** doivent être notifiés, le cas échéant, à l'Autorité de Contrôle compétente ou au Contrôleur Européen de la protection des données.

---

[1] Règlement (UE) n°2016-679 du Parlement Européen et du Conseil du 27 avril 2016, entré en application le 25 mai 2018

[2] Article 5 (f) du RGPD

[3] Article 83 RGPD.

Dans le cas de la BOAD et compte tenu de son statut particulier, le Département Conformité et Règlementation de la BOAD sera le point focal des Notifications en cas de Violation de données Personnelles. En effet, une fois que le DPO aura notifié au Département Conformité et Règlementation de l'existence d'une Violation de Données Personnelles, cette dernière devra identifier (i) la pertinence de la notification et (ii) à qui notifier, à savoir au Contrôleur Européen ou à l'Autorité de contrôle compétente.

1.2. Objectifs de la procédure

L'objectif de cette procédure est de :

- Définir à quoi correspondent les Violations des Données Personnelles ;
- Définir quels sont les événements des Violations des Données Personnelles qui doivent être notifiés ;
- Décrire les étapes à suivre pour notifier une violation des Données Personnelles ; et
- Présenter la documentation à maintenir à jour pour justifier de la prise en compte des notifications de Violations.

1.3. Vocabulaire

Les termes utilisés avec une majuscule ont la signification suivante.

Autorité de contrôle : l'autorité publique indépendante qui est instituée en vertu de l'article 51 du RGPD.

Contrôleur Européen de la protection des données: organe de l'Union Européenne en charge du contrôle de l'application des dispositions du Règlement n°2018/1725 sur la protection des données personnelles traitées par les institutions, organes et organismes de l'Union Européenne.

Dégâts des Données Personnelles: toute situation dans laquelle les données ont été modifiées, corrompues ou ne sont plus complètes.

Destruction des Données Personnelles: toute situation dans laquelle les données n'existent plus ou n'existent plus sous une forme qui est utile au responsable de traitement.

Données Personnelles: toute information se rapportant à une Personne concernée tel que son nom, prénom, numéro d'identification, données de localisation, identifiant en ligne, ou toute donnée relative à un ou plusieurs éléments spécifiques propres à l'identité physique de cette Personne tel que son identité physique, physiologique, génétique, psychique économique, culturelle ou sociale.

Personne concernée : toute Personne physique dont la BOAD traite les Données Personnelles tels que les clients bénéficiaires, porteurs de projets, collaborateurs, et les personnes physiques points de contact des fournisseurs, des prestataires, et/ou des collectivités.

Perte des Données Personnelles: toute situation dans laquelle les données existent encore mais où le responsable du traitement en a perdu le contrôle ou l'accès ou qu'il ne les a plus en possession.

Responsable de Traitement : personne morale ou organisme déterminant les finalités et les moyens du traitement, en l'occurrence, la BOAD.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou à des ensembles de Données Personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Traitement non autorisé ou illicite des Données Personnelles : toute divulgation des Données Personnelles à des destinataires qui ne sont pas autorisés à recevoir (ou à accéder à) ces données, ou toute autre forme de traitement qui viole le RGPD.

Violation des Données Personnelles : toute violation de la sécurité qui entraine, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

2. PREPARATION EN AMONT

2.1. Elaboration d'un IRP

La création d'un *Incident Response Plan* (IRP, ou plan de réponse aux incidents), et la sensibilisation des collaborateurs à leur rôle dans l'IRP, sera nécessaire pour assurer le respect des obligations dans le cas d'une Violation.

Le Système de Management de la Sécurité de l'Information (SMSI) de la BOAD comporte une Procédure de gestion des incidents (référence POS_06). Lorsqu'une Violation de Données Personnelles prend sa source dans un incident informatique, la présente procédure de gestion des violations de Données Personnelles est déclenchée si, lors de l'étape de qualification de tout incident, les intervenants du SMSI identifient qu'il s'agit d'une potentielle Violation de Données Personnelles et en informent le DPO.

2.2. Implémentation des outils de détection des incidents

Le responsable du traitement doit mettre en place des moyens organisationnels (ex : sensibilisation des collaborateurs à la détection de situations qui pourraient constituer des violations) et techniques (ex : outils de centralisation et de corrélation des logs ou service de « *threat intelligence* ») pour détecter et répondre à une Violation de données.

2.3. Désignation d'une autorité de contrôle chef de file le cas échéant

Le RGPD dispose que « *l'Autorité de Contrôle chef de file est le seul interlocuteur du responsable du Traitement ou du sous-traitant pour le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant.* »[4]

Au cours de la rédaction du plan de réponse aux incidents (IRP), le responsable de Traitement doit décider quelle Autorité de Contrôle sera l'autorité chef de file qui devra être notifiée. Cela permettra au responsable des données de notifier rapidement l'autorité de contrôle si besoin et donc remplir ses obligations en ligne avec l'article 33 (délai de 72h).

[4] Article 56 (6) du RGPD.

Le responsable de Traitement peut aussi notifier une autre autorité de contrôle, par exemple, s'il y a des personnes concernées dans un autre Etat Membre. S'il choisit de notifier seulement l'autorité de contrôle chef de file, le groupe de travail des autorités de contrôles de l'UE (WP29) conseille d'indiquer si la Violation va probablement affecter des établissements et/ou des personnes concernées dans des autres Etats Membres.

En l'occurrence, la notification de Violation de Données Personnelles se fera en interne de la BOAD, par le DPO à l'attention du Département Conformité et Règlementation, qui appréciera l'Autorité de Contrôle à laquelle notifier la Violation de Données Personnelles.

3. CONSEQUENCES DE LA VIOLATION DES DONNEES PERSONNELLES

Une Violation peut potentiellement avoir une série d'effets négatifs importants sur les personnes, qui peuvent se traduire par des dommages physiques, matériels ou immatériels.

Exemples : Dommages physiques, matériels ou préjudice moral pour les personnes physiques concernées[5] :

- × Perte de contrôle des Données Personnelles des personnes physiques concernées
- × Limitation des droits des personnes physiques concernées
- × Discrimination
- × Vol ou usurpation d'identité
- × Perte financière
- × Reversement non autorisé de la procédure de pseudonymisation
- × Atteinte à la réputation
- × Perte de confidentialité des données
- × Dommage économique ou social important

La règlementation applicable à la protection des données personnelles exige du responsable du Traitement qu'il notifie une violation à l'Autorité de Contrôle compétente ou au Contrôleur Européen, sauf s'il est peu probable que la Violation entraîne un risque de survenue d'effets négatifs. Inversement, lorsque la Violation implique des catégories particulières de données comme par exemple l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, il est conseillé de considérer un dommage comme probable[6]. Lorsque le risque de survenue de ces effets négatifs est élevé, la règlementation applicable exige du responsable du traitement qu'il communique la Violation aux personnes concernées.

L'importance d'être capable d'identifier une violation, d'évaluer le risque pour les personnes, puis de notifier si nécessaire, est soulignée dans le considérant 87 du RGPD :

« Il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature

[5] Considérant 85 du RGPD
[6] Considérants 75 et 85 du RGPD

et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement ».

4. NOTIFICATION DE LA VIOLATION DES DONNEES PERSONNELLES

Les Violations peuvent être classées comme suit[7] :

- La « Violation de confidentialité », lorsqu'il y a une divulgation ou un accès non autorisé ou accidentel à des Données Personnelles ;

- La « Violation de la disponibilité », en cas de perte accidentelle ou non autorisée de l'accès à des Données Personnelles ou de leur destruction ;

- La « Violation de l'intégrité », en cas d'altération accidentelle ou non autorisée des Données Personnelles.

Selon les circonstances, une violation peut concerner à la fois la confidentialité, la disponibilité et l'intégrité des Données Personnelles.

Les notifications des Violation des Données Personnelles suivent deux règles essentielles :

(i) Le moment de la notification
(ii) Le contenu de la notification

Parallèlement, des dispositions complémentaires sont nécessaires lorsque les Données Personnelles sont transférées à l'étranger.

Compte tenu du statut particulier de la BOAD, la notification se fera en interne, par le DPO, à l'attention du Département Conformité et Règlementation, qui appréciera la communication de la notification à l'Autorité de Contrôle compétente.

4.1. ETAPE 1 : Le moment de la notification

4.1.1. ETAPE 1.A) : Reconnaitre l'existence de la Violation d'une Donnée Personnelle

Un responsable de traitement peut être considéré comme conscient de la violation dès qu'il arrive à un niveau raisonnable de sûreté qu'un incident de sécurité s'est produit et que cet incident a compromis des Données Personnelles.

Dans certains cas, ce sera relativement clair dès le début qu'une Violation a eu lieu, alors que dans d'autres cas il faudra du temps pour vérifier si les données réellement sont compromises.

Une action rapide est requise pour :

- ✓ Investiguer l'incident et déterminer si les Données Personnelles ont été violées
- ✓ Si c'est le cas, prendre les mesures correctives
- ✓ Notifier le Contrôleur Européenne ou l'Autorité de Contrôle compétente au choix du Département Conformité et Règlementation de la BOAD

[7] WP29, avis 03/2014 sur la notification des violations

Après avoir été informé d'une Violation potentielle ou lorsqu'il a lui-même détecté un incident de sécurité, le responsable du Traitement peut entreprendre une brève période d'enquête afin d'établir si une Violation a effectivement eu lieu ou non. Le responsable du Traitement a l'obligation de donner suite à toute alerte initiale et d'établir si une Violation s'est effectivement produite ou non.

Le responsable du Traitement doit donc mettre en place des processus internes pour pouvoir détecter et traiter une Violation. Le responsable du Traitement doit également avoir mis en place des accords avec les sous-traitants auxquels il fait appel, qui ont eux-mêmes l'obligation d'informer le responsable du traitement en cas de Violation. Sur ce point, le RGPD ne donne pas une limite de temps explicite pendant laquelle le sous-traitant doit informer le responsable des données d'une violation, sauf qu'il doit le faire « dans les meilleurs délais ».

Concernant la notification du sous-traitant

- ✓ Une notification immédiate si possible, avec tout information supplémentaire fournie dès qu'elle devient disponible
- ✓ Un sous-traitant peut notifier l'autorité de contrôle pour le compte du responsable de Traitement, si cela fait partie des accords contractuels entre les deux

Pendant la période d'enquête, le responsable du Traitement peut être considéré comme étant inconscient de l'existence effective de la Violation[8]. Cette brève période permet de mener une enquête, de rassembler des preuves et d'évaluer le risque avant que le responsable du traitement ne soit obligé d'envoyer une notification. Toutefois, une fois que la BOAD a établi avec un degré raisonnable de certitude qu'une violation s'est produite il doit en informer son Département Conformité et Règlementation qui déterminera s'il convient de notifier le Contrôleur Européen ou l'Autorité de Contrôle compétente, étant précisé qu'il conviendra d'effectuer cette notification sans retard excessif et **au plus tard dans les 72 heures**.

4.1.2. ETAPE 1.B) : Evaluation de la Violation de la Donnée Personnelle

Etant donné les dommages éventuels évalués en cas de Violation et compte tenu des circonstances de la Violation, une évaluation ponctuelle sera nécessaire pour que le DPO communique au Département Conformité et Règlementation de la BOAD les éléments permettant de déterminer :

- Si les circonstances exigent une notification
- Quelles actions doivent être réalisées pour répondre à la Violation
- Auprès de qui doit être effectuée la Notification à savoir au choix (i) auprès du Contrôleur Européen ou (ii) auprès de l'Autorité compétente

Lors de l'évaluation il est conseillé de prendre en compte les critères suivants :

- ✓ Le type de Violation
- ✓ La nature, sensibilité et volume des Données Personnelles
- ✓ La facilité d'identification pour les individus
- ✓ La sévérité des conséquences potentielles pour les individus, et la permanence de ces conséquences (si les effets ont une longue durée, l'impact est considéré comme plus élevé)

[8] WP29, *Guidelines on Personal data breach notification under Regulation 2016/679*, 3 Octobre 2017

- ✓ Les particularités de l'individu (si la personne concernée est un enfant ou autre personne potentiellement vulnérable, par exemple, l'impact est considéré comme plus élevé)
- ✓ Le nombre d'individus affectés
- ✓ Les particularités du responsable des données et ses activités
- ✓ Autres éléments qui pourraient modifier la sévérité et la probabilité de l'impact sur les droits et libertés des individus

Les tableaux présentés ci-dessous peuvent être un guide pour effectuer l'évaluation d'une éventuelle Violation de Donnée Personnelle.

1- Evaluation de Violation au regard de la possibilité d'identifier la personne concernée

Les Données Personnelles ayant fait l'objet d'une Violation permettent-elle d'identifier les Personnes ?	Conséquences	Niveau de Violation
Il semble quasiment impossible d'identifier les personnes à l'aide des données les concernant (ex. identifier quelqu'un au sein de la population française en ne connaissant que son prénom)	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, simple contrariété…)	Négligeable
Il semble difficile d'identifier les personnes à l'aide des données les concernant, bien que cela soit possible dans certains cas (ex. identifier quelqu'un au sein de la population française en connaissant son nom et son prénom)	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourraient surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, affection physique ou psychologique mineure…)	Limité
Il semble relativement facile d'identifier les personnes à l'aide des données les concernant (ex. identifier quelqu'un au sein de la population française en connaissant son nom, son prénom et sa date de naissance)	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles pourraient surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, affection physique ou psychologique grave…)	Important
Il semble extrêmement facile d'identifier les personnes à l'aide des données les concernant (ex. identifier quelqu'un au sein de la population française en connaissant son nom, son prénom, sa date de naissance et son adresse postale)	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée ou permanente, décès…)	Maximal

2- Evaluation de la Violation par type de violation

Description de la Violation	Conséquences
Les données ont été ou pourraient être diffusées plus que nécessaire et ont été ou pourraient avoir échappé à la maîtrise des personnes concernées (ex. : diffusion non désirée d'une photo sur Internet, perte de contrôle d'informations publiées dans un réseau social…)	Perte de confidentialité
Les données ont été ou pourraient être corrélées avec d'autres informations relatives aux personnes concernées (ex. : corrélation d'adresses de résidence et de données de géolocalisation en temps réel…)	
Les données ont été ou pourraient être exploitées à d'autres fins que celles prévues et/ou de manière injuste (ex. : fins commerciales, usurpation d'identité, utilisation à l'encontre des personnes concernées…)	

Les données ont été ou pourraient être modifiées en des données invalides, qui ne seront pas utilisées de manière correcte, le traitement pouvant engendrer des erreurs, des dysfonctionnements, ou ne plus fournir le service attendu (ex. : altération du bon déroulement de démarches importantes…)	Perte d'intégrité
Les données ont été ou pourraient être modifiées en d'autres données valides, de telle sorte que les traitements ont été ou pourraient être détournés (ex. : exploitation pour usurper des identités en changeant la relation entre l'identité des personnes et les données biométriques d'autres personnes…)	
Les données ont été ou pourraient être manquantes à des traitements qui ne peuvent plus du tout fournir le service attendu (ex. : ralentissement ou blocage de processus administratifs ou commerciaux, impossibilité de fournir des soins du fait de la disparition de dossiers médicaux, impossibilité pour des personnes concernées d'exercer leurs droits…)	Perte de disponibilité
Les données ont été ou pourraient être manquantes à des traitements et générer des erreurs, des dysfonctionnements, ou fournir un service différent de celui attendu (ex. : certaines allergies ne sont plus signalées dans un dossier médical, certaines informations figurant dans des déclarations de revenus ont disparu, ce qui empêche le calcul du montant des impôts…)	

4.1.3. ETAPE 1.C) : Quand notifier

Après étude des éléments communiqués par le DPO, et si le Département Conformité et Règlementation l'estime pertinent, **la notification devra être effectuée, lorsque c'est possible, au plus tard 72 heures après en avoir pris connaissance.**

Si le DPO n'a pas toutes les informations au moment de la notification, elles peuvent être fournies au Département Conformité et Règlementation de manière échelonnée de manière à ce que cette dernière puisse déterminer la pertinence de la Notification. Si la notification ne peut avoir lieu dans ce délai de 72 heures, le retard doit impérativement être justifié.

En cas de doute, il est conseillé de notifier la Violation. Aucune sanction ne sera imposée pour la notification d'un incident qui ne constituerait finalement pas une Violation d'une Donnée Personnelle.

Exception : La notification n'est pas nécessaire si, conformément au principe de responsabilité, le responsable du Traitement et en l'occurrence le du Département Conformité et Règlementation de la BOAD, est capable de démontrer qu'il est peu probable que la Violation en question engendre un risque pour les droits et libertés des personnes physiques.

Cependant, ce risque doit continuer à être surveillé et réévalué au fil du temps. Une au Contrôleur Européen ou à l'Autorité de Contrôle compétente ainsi qu'une communication aux personnes concernées peuvent devenir nécessaires en cas de changement de la situation.

4.1.4. ETAPE 1.D) : La communication aux personnes concernées

Le responsable du Traitement devrait communiquer une Violation de Données Personnelles à la personne concernée dans les meilleurs délais lorsque cette violation est susceptible d'engendrer un **risque élevé** pour les droits et libertés de la personne physique afin qu'elle puisse prendre les précautions qui s'imposent.

Cette communication devrait décrire la nature de la violation des Données Personnelles et formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels. Cette communication doit avoir lieu aussi rapidement qu'il est

raisonnablement possible et en coopération étroite avec le Contrôleur Européen ou l'Autorité de Contrôle compétente le cas échéant. Dans certains cas, la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la Violation des Données Personnelles ou la survenance de violations similaires peut justifier un délai plus long pour la communication[9].

Note
Dans tous les cas, notifiez la Violation des Données Personnelles au Département Conformité et Règlementation. Elle vous indiquera alors s'il est nécessaire d'informer les personnes.

4.2. ETAPE 2 : Contenu de la notification

4.2.1. ETAPE 2.A) : Le contenu a minima de la notification

Il est précisé que la notification, qu'elle soit effectuée auprès du Contrôleur Européen ou de l'Autorité de Contrôle compétente, doit, *a minima*[10] :

1. Décrire la nature de la Violation de Données Personnelles 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 Personnelles concernés ;

2. Communiquer le nom et les coordonnées du Délégué à la Protection des Données (DPO) ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

3. Décrire les conséquences probables de la Violation des Données Personnelles ;

4. Décrire les mesures prises ou que le responsable du Traitement propose de prendre pour remédier à la Violation de Données Personnelles, y compris, le cas échéant, les mesures pour en atténuer les effets.

4.2.2. ETAPE 2.B) : Le contenu de la communication à la personne concernée

Les violations doivent être communiquées aux personnes concernées de façon directe et transparente[11].

Le texte du RGPD précise par ailleurs diverses exceptions[12] concernant la communication à la personne concernée :

i. Dans le cas où les données sont suffisamment protégées : « *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 avoir accès, telles que le chiffrement* »

[9] Considérant 86 du RGPD
[10] Article 33 (3) du RGPD
[11] Article 34 (2) du RGPD
[12] Article 34 (3) du RGPD

ii. Dans le cas où les risques ont été retenus par des mesures ultérieures déployées par le responsable de traitement : « *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* » ;

iii. Dans le cas où des efforts disproportionnés sont requis pour informer la Personne : « *exigerait des efforts disproportionnés 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* ».

4.3. ETAPE 3 : L'action de l'Autorité de Contrôle ou du Contrôleur Européen – en cas de notification par le Département Conformité et Règlementation

Si le Département Conformité et Règlementation a choisi de notifier le Contrôleur Européen ou l'Autorité de Contrôle compétente, ces derniers instruire la notification. La procédure relative à la Violation notifiée pourra être clôturée si le Contrôleur Européen ou l'Autorité de Contrôle compétente constate que :

- ✓ La Violation ne porte pas atteinte aux Données Personnelles ou à la vie privée des Personnes
- ✓ Vous avez correctement informé les personnes concernées
- ✓ Vous avez mis en place, préalablement à la Violation, des mesures techniques de protection appropriées*
- ✓ Le Contrôleur Européen ou l'Autorité de Contrôle compétente pourra vous imposer d'informer les personnes concernées si elle constate que :
  - Vous ne les avez pas correctement informées
  - Les mesures techniques de protection que vous avez mises en place préalablement à la violation ne sont pas appropriées

L'Autorité de Contrôle compétente notifiée disposera d'un **délai de 2 mois** pour vérifier le caractère approprié ou non de ces mesures techniques. En l'absence de retour de l'Autorité de Contrôle dans ce délai, vous devrez considérer que les mesures ne sont pas appropriées et vous devrez immédiatement informer les personnes de la Violation.

4.4. ETAPE 4 : La documentation

Cette documentation doit être effectuée dans tous les cas, même si la Violation n'est pas notifiée au Contrôleur Européen ou à l'Autorité de Contrôle compétente. Le RGPD exige en effet que responsable de Traitement documente toute Violation de Données Personnelles, en indiquant les faits concernant la Violation de telles données, ses effets ainsi que les mesures prises pour y remédier.

La documentation ainsi constituée permet au Contrôleur Européen ou à l'Autorité de Contrôle compétente de vérifier le respect par le responsable de Traitement des mesures à prendre en cas de Violation des Données Personnelles[13].

Cette documentation doit inclure :

[13] Article 33 (5) du RGPD.

- ✓ Les faits concernant la Violation des Données Personnelles
- ✓ Ses effets
- ✓ Les mesures prises pour y remédier

Recommandations du groupe de travail des autorités de contrôle Européennes (WP29) :

Documenter en complément :

- ✓ La justification des décisions prises lors de la Violation surtout, le cas échéant, de la décision de ne pas notifier,
- ✓ Lors d'un délai dans la notification au Contrôleur Européen ou à l'Autorité de Contrôle compétente, les raisons pour le délai, ou en l'espèce pour la BOAD, la justification de l'absence de notification au Contrôleur Européen ou à l'Autorité de Contrôle compétente compte tenu des règles spécifiques applicables à la BOAD
- ✓ Les preuves des communications aux personnes concernées lors d'une Violation,
- ✓ La procédure de notification dans le cas de Violation, inclut comment limiter, gérer, se remettre de l'incident, et l'évaluation de risque,
- ✓ Les preuves que les employés ont été informés de ces procédures et sont en mesure de réagir à une Violation

---

Par ailleurs, les responsables de traitement peuvent établir un registre interne des Violations réelles et potentielles, même lorsqu'ils ne sont pas obligés de notifier.