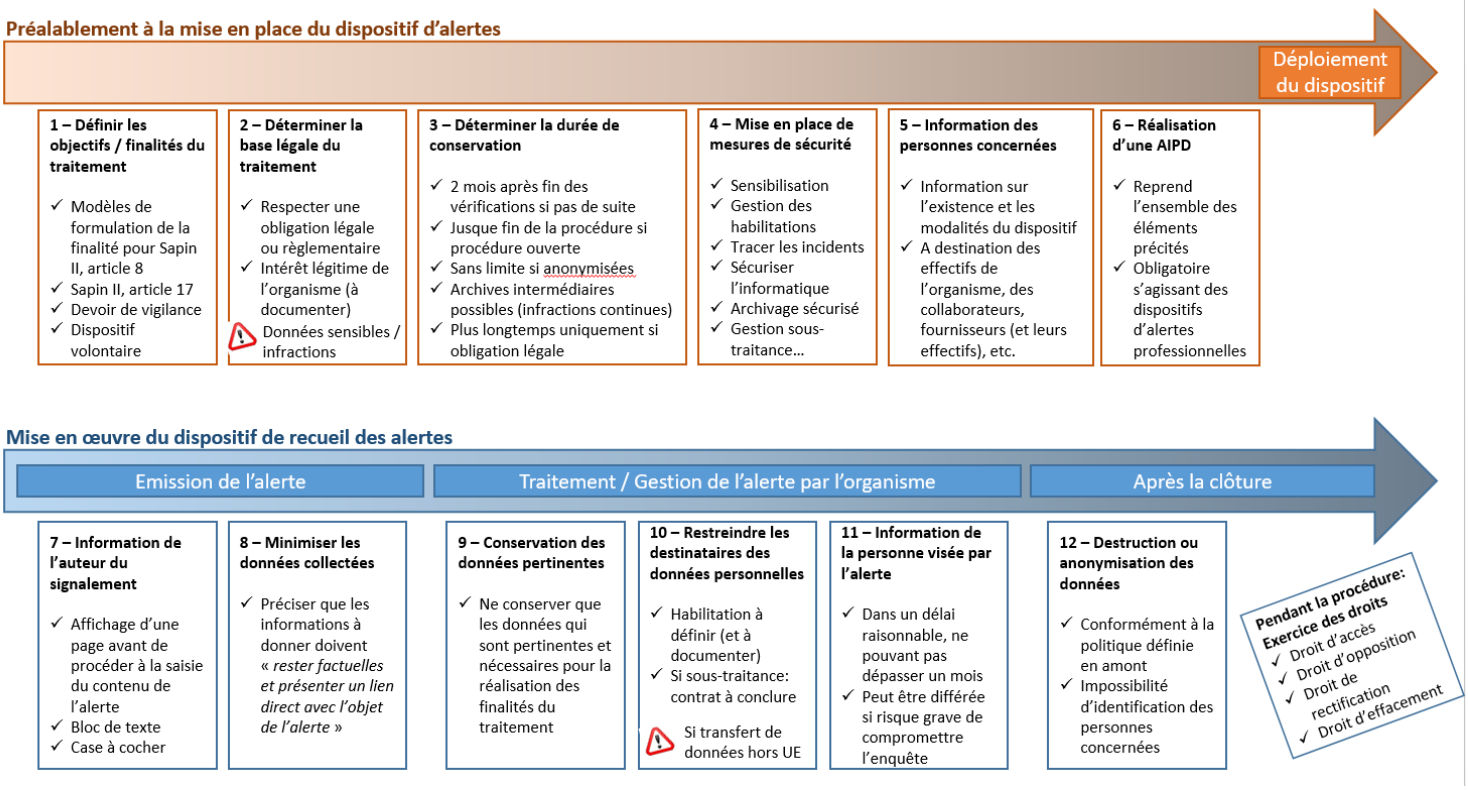
Mettre en place une procédure d'alertes conforme au RGPD dans l'entreprise ou l'ONG

Commentaire du référentiel de la CNIL relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles, JO 10 décembre 2019



Face à la multiplication des obligations en matière de signalement, à la charge tant des entreprises que des ONG et des personnes morales de droit public, se pose la question de la conciliation entre ces obligations et celles de conformité au Règlement Général de Protection des Données (RGPD), lequel est entré en vigueur le 25 mai 2018.

Les personnes morales de toute nature – de tout statut, de toute taille économique ou humaine[1] – sont en effet confrontées au processus de mise en conformité, indispensable non seulement au respect d'obligations légales et règlementaires mais également à la gestion des risques pénaux, civils voire commerciaux, par ces mêmes personnes morales.

Cette conciliation répond ainsi à un enjeu réputationnel mais également judiciaire et, ainsi que la CNIL vient le rappeler dans le référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles, publié dans sa version

[1] Si les seuils fixés par l'article 17 de la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite Sapin II, et par l'article L.225-102-4 du code de commerce créé par la loi n°2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre, dite loi vigilance, sont relativement élevés, l'article 8 de la loi Sapin II impose l'obligation de mettre en place un dispositif de recueil des signalements à l'ensemble des personnes morales de plus de 50 salariés. Elle offre par ailleurs une définition du lanceur d'alerte (article 6) susceptible d'étendre ce statut même dans les plus petits organismes.

définitive le 10 décembre 2019, ils sont également importants en termes de protection des données à caractère personnel au sein des personnes morales.

Mettre en place un dispositif d'alertes donc, mais tout en garantissant, aussi, la conformité aux dispositions légales et règlementaires spécifiques à un autre domaine de la compliance : celui de la protection des données.

*

Les étapes de la mise en place d'un dispositif de recueil des alertes conforme au RGPD

Adopté initialement par la délibération n°2019-139 du 18 juillet 2019, à la suite d'une consultation publique, le référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles, a vocation à s'appliquer tant aux organismes qui sont tenus de mettre en œuvre un dispositif de recueil et de gestion des alertes professionnelles, qu'à ceux qui décideraient, sans obligation légale, de le mettre en œuvre, notamment aux fins de prohiber les comportements jugés incompatibles avec leur charte éthique ou leur règlement intérieur.

Il devra ainsi être respecté par tout employeur qui aura à traiter des données à caractère personnel, notamment relatives à ses salariés, dans le cadre de tels dispositifs d'alerte[2], de façon à respecter tant les dispositions du RGPD que celles de la loi Informatique et Liberté[3].

Préalablement à la mise en place du dispositif d'alerte

Etape 1 - Définir les finalités du traitement. Toute opération effectuée ou appliquée à des données à caractère personnel, qu'il s'agisse de la collecte, l'enregistrement, la destruction, ou la simple *consultation* de ces données, s'entend comme un « traitement » de ces données au sens du RGPD[4]. Afin de respecter l'un de ses principes[5], le traitement doit nécessairement répondre à une finalité précise, justifiée au regard de l'activité du responsable de traitement.

A cet égard, la CNIL propose aux employeurs dans son référentiel des formulations des finalités propres à chaque type de dispositif d'alertes mis en œuvre. Celles-ci doivent être déterminées de façon exhaustive, dès lors que les informations recueillies pour une finalité donnée ne pourront pas être réutilisées à d'autres fins.

Etape 2 – Déterminer la base légale du traitement. Un traitement n'est licite que s'il repose sur l'une des bases légales définies par l'article 6 du RGPD. La CNIL précise, s'agissant des dispositifs de recueil des alertes que ceux-ci sont fondés, en principe, soit sur le respect d'une obligation légale incombant à l'organisme, soit, lorsque tel n'est pas le cas, sur l'intérêt légitime poursuivi par l'organisme ou le destinataire des données, sous réserve de ne pas méconnaitre les droits et libertés de la personne dont les données sont traitées (la « personne concernée »). Dans ce second cas, la balance des

[2] Précisions ici que par nature et au regard de leur objet, les dispositifs de recueil des signalements semblent nécessairement susceptibles d'avoir à traiter de telles données, celles-ci étant définies par l'article 4(1) du RGPD comme « toute information se rapportant à une personne physique identifiée ou identifiable », c'est-à-dire se rapportant à « une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

[3] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[4] V. article 4(2) du RGPD.

[5] V. article 5 du RGPD.

intérêts opérée entre l'intérêt légitime de l'organisme et les droits de la personne concernée devra être documentée, par exemple en rédigeant l'analyse opérée de la balance des intérêts.

A noter que dans le cas où l'organisme mettrait en œuvre un dispositif d'alertes mixte, ayant pour finalité de recueillir tant les alertes dans le cadre de la loi Sapin II par exemple, que les alertes relatives à un engagement volontaire de l'organisme, chacune de ces finalités devra être justifiée par une base légale spécifique.

Une attention particulière doit être apportée au traitement des données dites sensibles[6], lesquelles doivent voir leur traitement justifié sur le fondement de l'article 9 du RGPD. Dans le cas de la mise en place d'un dispositif de recueil des alertes, il pourra s'agir par exemple, de la nécessité du traitement pour la constatation, l'exercice ou la défense d'un droit en justice[7]. De même, les données relatives aux infractions, condamnations et mesures de sûreté ne peuvent être traitées que si ce traitement est justifié au regard des articles 10 RGPD et 46 de la Loi Informatique et Libertés, c'est-à-dire au titre d'une obligation légale, ou pour permettre à l'employeur de « *préparer, et le cas échéant, d'exercer et de suivre une action en justice en tant que victime, mise en cause, ou pour le compte de ceux-ci* ».

Etape 3 – Déterminer la durée de conservation des données. Les données à caractère personnel ne doivent être conservées par l'organisme que le temps strictement nécessaire à la réalisation des finalités poursuivies[8]. La CNIL précise à cet égard que :

- Si les données n'entrent pas dans le champ du dispositif, elles doivent être détruites ou anonymisées[9] ;
- Si aucune suite n'est donnée à l'alerte[10], les données à caractère personnel doivent être anonymisées ou détruites, dans un délai de deux mois à compter de la clôture des opérations de vérification ;
- Si une procédure disciplinaire ou contentieuse est engagée, elles peuvent être conservées jusqu'au terme de la procédure ou de la prescription des recours contre la décision ;
- En cas d'infraction continue, des archives intermédiaires peuvent être conservées pour assurer la protection du lanceur d'alerte : durée de conservation strictement limitée aux finalités poursuivies.

Les données peuvent être conservées plus longtemps seulement en cas d'obligation légale de le faire (obligations comptables, fiscales, sociales…).

Etape 4 – Mise en place de mesures de sécurité. Préalablement au déploiement du dispositif de recueil des alertes, enfin, l'organisme est tenu de prévoir et de prendre toutes les précautions utiles au regard des risques présentés par son traitement. La CNIL détaille ainsi les mesures de sécurité attendues de la part des employeurs, qu'il s'agisse de sensibiliser les utilisateurs, de gérer les habilitations, de tracer et gérer les incidents, de sécuriser les postes de travail et l'informatique, les sites web, de l'archivage, de la gestion de la sous-traitance, etc.

---

[6] Sont définies comme telles, par l'article 9(1) du RGPD, les « *données à caractère personnel qui révèle[nt] l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ».

[7] Article 9(2f) du RGPD.

[8] Article 5(1e) du RGPD.

[9] L'anonymisation implique l'impossibilité irréversible d'identifier à l'avenir la personne concernée. V. sur cette question l'avis 05/2014 relatif aux techniques d'anonymisation du Comité Européen de la Protection des Données (CEPD).

[10] La CNIL précise à cet égard et en tout état de cause que les suites réservées à l'alerte doivent intervenir « dans un délai raisonnable à compter de l'émission de celle-ci ».

Etape 5 – Information des personnes concernées du déploiement du dispositif d'alertes. L'organisme qui met en place le dispositif d'alertes professionnelles doit ensuite informer les personnes susceptibles d'être concernées dans le futur par une alerte, c'est-à-dire les effectifs de l'organisme, mais également à les collaborateurs, clients, fournisseurs extérieurs et les effectifs de ceux-ci, individuellement et collectivement, de l'existence et des modalités de ce dispositif d'alerte. Cette information doit inclure notamment des précisions quant aux finalités des traitements et la durée de conservation des données à caractère personnel, ainsi que relativement aux droits des personnes si leurs données sont collectées dans ce cadre[11].

Etape 6 - Réalisation d'une AIPD. A l'aune de l'ensemble des étapes précitées, et préalablement à l'établissement de tout dispositif de recueil de signalements, une analyse d'impact relative à la protection des données (AIPD) doit être réalisée. La CNIL a en effet déjà eu l'occasion de rappeler que la mise en place d'un tel dispositif d'alertes doit systématiquement donner lieu à la réalisation préalable d'une AIPD[12].

Mise en œuvre du dispositif d'alertes

Etape 7 – Information spécifique du lanceur d'alerte. Les personnes qui émettent un signalement doivent recevoir les informations relatives au traitement dès le début du processus de recueil de l'alerte, par exemple par l'affichage d'une page ou d'un bloc de texte préalablement à l'étape de saisie des informations relatives à l'alerte. La CNIL précise qu'il peut s'agir aussi d'une case à cocher confirmant que l'intéressé a pris connaissance de ces informations.

Etape 8 – Traiter les données en conformité avec les principes du RGPD, minimiser les données personnelles conservées. Au stade de l'émission de l'alerte, afin de respecter le principe de minimisation des données, l'organisme doit rappeler à l'auteur des signalements que les informations qu'il va communiquer doivent « *rester factuelles et présenter un lien direct avec l'objet de l'alerte* ». Un accusé réception incluant l'ensemble des informations transmise devra être envoyé à la personne ayant émis le signalement.
Au stade de l'instruction de l'alerte, l'organisme ne devra conserver que les données personnelles qui sont pertinentes et nécessaires pour la réalisation des finalités du traitement prédéterminées.

Etape 9 – Restreindre les destinataires des données personnelles. Les données à caractère personnel ne doivent être accessibles que pour les personnes habilitées à en connaitre. L'employeur doit donc documenter les habilitations (ex : personnes spécialement chargées de la gestion des alertes, référents ou prestataire de service chargé de les traiter).
En cas de sous-traitance de la gestion des alertes, un contrat doit être établi avec le sous-traitant afin que celui-ci respecte également les principes du RGPD[13]. Le sous-traitant devra notamment s'engager à ne pas utiliser les données à d'autres fins que la gestion des alertes.
Une attention particulière doit également être portée à toute transmission de données en dehors de l'Union européenne.

Etape 10 – Sous un mois maximum, informer la personne visée par l'alerte. La CNIL apporte une précision d'importance dans son référentiel, à savoir que c'est « *dans un délai raisonnable, ne pouvant pas dépasser un mois, à la suite de l'émission de l'alerte* » que la personne visée par cette

[11] L'information communiquée doit respecter les dispositions des articles 12, 13 et 14 du RGPD.
[12] Délibération n°2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.
[13] Article 28 du RGPD.

alerte doit être informée de cette alerte et de la collecte des données la concernant[14]. Cette information ne peut être différée que lorsqu'elle serait susceptible de « *compromettre gravement la réalisation des objectifs dudit traitement* »[15]. L'information doit alors être délivrée aussitôt le risque écarté.

Etape 11 – Exercice des droits. Les personnes dont les données sont effectivement collectées dans le cadre d'une alerte disposent de plusieurs droits :

- droit de s'opposer au traitement, lequel n'existe que lorsque le traitement n'est pas justifié par une obligation légale[16] (il existe contre le dispositif volontairement mis en œuvre par une entreprise, sous réserve que la personne justifie de « *raisons tenant à sa situation particulière* », mais pas contre le dispositif mis en œuvre au titre de Sapin II par exemple) ;
- droit d'accès, de rectification et d'effacement, sans que le droit d'accès ne puisse permettre à une personne d'accéder aux données à caractère personnel d'une autre personne ;
- droit à la limitation du traitement.

Etape 12 – Ne conserver les données que le temps strictement nécessaire. Conformément à ce qui a été précédemment indiqué concernant la fixation de la durée de conservation des données, il convient, à l'issu du traitement d'une alerte, de détruire ou d'anonymiser les données collectées.

*

Alimenté par la consultation publique ouverte en avril 2019, ce référentiel, définitivement adopté, étaye le premier projet publié en avril dernier par la CNIL[17] en apportant ainsi davantage de précisions, notamment concernant :

- Le rappel qui doit être adressé aux auteurs de signalement que les informations communiquées dans le cadre du dispositif doivent rester factuelles et présenter un lien direct avec l'objet de l'alerte,
- L'information à la personne visée par une alerte doit intervenir dans un délai raisonnable ne pouvant, selon la CNIL, dépasser un mois à la suite de l'émission de l'alerte – laquelle peut être différée en cas de risque de compromettre gravement l'enquête,
- La nécessité de différencier les modalités de traitement selon la base légale utilisée.

Pour les organismes ayant déjà mis en place leur dispositif d'alerte, une actualisation de leur AIPD et des modalités de leur dispositif en place sera probablement bienvenue au regard de cette version définitive.

Le référentiel sera bientôt complété par la publication d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre par les entreprises pour la gestion du personnel, pour lequel une consultation publique avait pareillement été ouverte en avril 2019.

Emmanuel Daoud, Avocat au barreau de Paris, associé du cabinet Vigo, membre du réseau international d'avocats GESICA.

---

[14] Cette information doit être donnée dans le cadre de l'article 14 du RGPD. La CNIL précise à cet égard que cette information ne doit en revanche pas contenir « *d'informations relatives à l'identité de l'émetteur de l'alerte ni à celle des tiers* ».

[15] Article 14(5b) du RGPD.

[16] Article 21 du RGPD.

[17] Projet de référentiel relatif aux traitements de données à caractère personnel mis en œuvre par des organismes privés ou publics aux fins de gestion du personnel, 11 avril 2019, accessible sur https://www.cnil.fr/sites/default/files/atoms/files/referentiel-alertes-pro.pdf.

Marine Doisy, Avocate au barreau de Paris, collaboratrice du cabinet Vigo, membre du réseau international d'avocats GESICA.