Le 23 décembre 2019

JORF n°0286 du 10 décembre 2019

Texte n°40

Délibération n° 2019-139 du 18 juillet 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles

NOR: CNIL1935146X

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code du commerce, notamment ses articles L. 225-102-3 et R. 822-33 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu 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 (loi « Sapin 2 »), notamment ses articles 6, 8 et 17 ;

Vu la loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (loi « devoir de vigilance ») ;

Vu le décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat ;

Vu le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu les recommandations de l'Agence française anticorruption destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme ;

Après avoir entendu M. Alexandre LINDEN, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;

Adopte le référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles, qui sera publié au Journal officiel de la République française.

Annexe

ANNEXE

Vous pouvez consulter l'intégralité du texte avec ses images à partir de l'extrait du Journal officiel électronique authentifié accessible en bas de page

1. A qui s'adresse ce référentiel ?

Ce référentiel s'adresse aux organismes privés ou publics qui sont tenus ou qui décideraient de mettre en œuvre un dispositif de recueil et de gestion des alertes professionnelles nécessitant un traitement de données à caractère personnel. Il couvre dès lors deux types de dispositifs.

D'une part, le présent référentiel concerne les dispositifs d'alerte encadrés par des dispositions législatives ou réglementaires spécifiques, que l'organisme soit ou non assujetti juridiquement à ces dispositions. Il peut s'agir, notamment, des dispositifs prévus par les articles 8 et/ou 17 de la loi dite « loi Sapin 2 »(1), ou bien mis en œuvre en application de la « loi relative au devoir de vigilance »(2), quels que soient la taille des effectifs, la nature juridique ou encore le chiffre d'affaires des organismes concernés.

Dans cette première hypothèse, constitue une alerte professionnelle tout signalement effectué de bonne foi et qui révèle ou signale une infraction pénale, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, lorsque les faits en question ne sont pas couverts par le secret de la défense nationale, le secret médical ou le secret des relations entre un avocat et son client.

D'autre part, le présent référentiel a également vocation à régir les dispositifs d'alertes éthiques adoptés de sa propre initiative par un organisme en vue de prohiber des comportements jugés incompatibles avec sa charte éthique ou son règlement intérieur.

Dans cette seconde hypothèse, constitue une alerte professionnelle tout signalement effectué de bonne foi et qui révèle ou signale une violation de règles éthiques adoptées par un organisme ou un groupe, dès lors que les règles en question sont codifiées dans un document écrit (tel qu'un règlement intérieur, une charte éthique, etc.) qui respecte l'ensemble du cadre juridique existant (en particulier la législation du travail et l'ensemble des droits et libertés fondamentales des personnes concernées), et dont l'existence et le caractère opposable sont préalablement portés à la connaissance de l'ensemble des personnes concernées.

Les organismes mettant en place un dispositif d'alerte doivent s'assurer de sa conformité :

- aux dispositions du Règlement général sur la protection des données (RGPD) ainsi qu'à celles de la loi du 6 janvier 1978 dite « informatique et libertés » (LIL). En effet, lorsque ces dispositifs, comme c'est le cas en règle générale, nécessitent un traitement de données relatives à des personnes physiques identifiées ou identifiables (notamment celles de l'auteur et de la ou les personnes visées par l'alerte), ils sont soumis aux règles relatives à la protection des données personnelles ;

- à l'ensemble d'autres règles de droit applicables en vertu des législations spécifiques (loi dite « Sapin 2 », etc.) ou générales (droit du travail). Le responsable de traitement doit garantir le respect les droits et les libertés fondamentales ainsi que des intérêts légitimes des personnes concernées.

En l'absence d'encadrement précis par les textes législatifs et réglementaires en vigueur, les dispositifs créés à l'initiative des organismes sous la forme par exemple de chartes éthiques ou dans leurs règlements intérieurs doivent faire l'objet d'une attention particulière.

2. Portée du référentiel

Ce référentiel a pour objectif de fournir un outil d'aide à la mise en conformité des organismes publics et privés souhaitant se doter de dispositifs de traitement d'alertes professionnelles, à la réglementation relative à la protection des données privées.

Le respect de ce référentiel permet aux organismes de s'assurer de la conformité des traitements de données mis en œuvre dans le cadre des dispositifs d'alertes aux principes relatifs à la protection des données.

Les organismes qui s'écarteraient du référentiel au regard des conditions particulières tenant à leur situation doivent être en mesure de justifier l'existence d'un tel besoin, puis prendre toutes les mesures appropriées à même de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel.

Le référentiel n'a pas pour objet d'interpréter les règles de droit autres que celles relatives à la protection des données à caractère personnel. Il appartient aux acteurs concernés de s'assurer qu'ils respectent les autres réglementations qui peuvent par ailleurs trouver à s'appliquer.

Ce référentiel constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD).

La mise en place d'un dispositif d'alertes professionnelles doit en effet systématiquement donner lieu à la réalisation préalable d'une AIPD. En effet, ces dispositifs figurent dans la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise (cf. la 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).

Pour réaliser une étude d'impact, le responsable de traitement pourra se reporter aux outils méthodologiques proposés par la CNIL sur son site web. Il pourra également se

reporter au présent référentiel pour Les organismes pourront ainsi définir les mesures permettant d'assurer la proportionnalité et la nécessité de leurs traitements (points 3 à 7), de garantir les droits des personnes (points 8 et 9) et la maîtrise de leurs risques (point 10). A cette fin, l'organisme pourra se référer aux lignes directrices de la CNIL sur les analyses d'impact relatives à la protection des données (AIPD). Si l'organisme en a désigné un, le délégué à la protection des données (DPD/DPO) devra être consulté.

3. Objectif(s) poursuivi(s) par le traitement (Finalités)

Le traitement mis en œuvre doit répondre à un objectif précis et être justifié au regard des missions et des activités de l'organisme.

En ce qui concerne le dispositif d'alerte, le traitement de données est mis en œuvre afin de recueillir et traiter les alertes ou signalements visant à révéler un manquement à une règle spécifique.

Exemple 1.1 (alertes de l'article 8 de la Loi « Sapin 2 ») :

Un dispositif d'alerte mis en œuvre pour répondre aux exigences de l'article 8.III de la loi « Sapin 2 » vise à permettre aux « membres du personnel et aux collaborateurs extérieurs et occasionnels » d'un organisme, de signaler :

- un crime ou délit ;

- une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France ;

- une violation grave et manifeste d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un engagement international régulièrement ratifié ;

- une violation grave et manifeste de la loi ou du règlement ;

- une menace ou préjudice graves pour l'intérêt général, dont l'émetteur de l'alerte a eu personnellement connaissance.

Exemple 1.2 (lutte contre la corruption et le trafic d'influence) :

Un dispositif d'alerte mis en œuvre pour répondre aux exigences de l'article 17.II.2° de la loi « Sapin 2 », vise à permettre le recueil des signalements émanant des « employés » de l'organisme concerné et relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société et susceptibles de caractériser des faits de corruption ou de trafic d'influence.

Exemple 1.3 (devoir de vigilance) :

Un dispositif d'alerte prévu par l'article L. 225-102-4 du Code de commerce, issu de la Loi dite de « devoir de vigilance », aura pour finalité le recueil des signalements relatifs à l'existence ou à la réalisation des risques d'atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement, résultant des activités de la société et de celles des sociétés qu'elle contrôle au sens du II de l'article L. 233-16, directement ou indirectement, ainsi que des activités des sous-traitants ou fournisseurs avec lesquels est entretenue une relation

commerciale établie, lorsque ces activités sont rattachées à cette relation.

Exemple 2 (codes éthiques) :

Un dispositif d'alerte mis en place sur une base volontaire par l'organisme, en dehors d'une obligation légale spécifique, pourrait par exemple avoir pour finalité le recueil de tout signalement d'un risque existant ou réalisé d'un comportement ou d'une situation contraires à une charte éthique de l'organisme, quel que soit l'auteur de l'alerte ou son lien avec l'organisme.

Exemple 3 (dispositifs hybrides) :

Un dispositif visant à la fois les alertes « de droit commun » (article 8.III de la Loi « Sapin 2 »), celles répondant au devoir de vigilance (art. L. 225-102-4 du code du commerce) et celles résultant de l'application d'une charte ou d'un code éthique, devra explicitement viser l'ensemble des finalités correspondantes, en distinguant celles qui résultent d'une disposition obligatoire spécifique de celles qui sont adoptées volontairement par l'organisme.

Les informations recueillies pour l'une de ces finalités ne peuvent pas être réutilisées pour poursuivre un autre objectif qui serait incompatible avec la finalité première. Tout nouvel usage des données doit en effet respecter les principes de protection des données personnelles. Les traitements mis en œuvre ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des finalités ci-dessus énoncées.

4. Base(s) légale(s) du traitement

Chaque finalité du traitement doit reposer sur l'une des « bases légales » fixées par la réglementation. Les différents fondements autorisant un organisme à traiter des données personnelles dans le cadre d'un dispositif d'alerte sont listés ci-dessous.

Dans le cadre du présent traitement, la base légale peut être :

a) Le respect d'une obligation légale incombant à l'organisme, imposant la mise en œuvre d'un dispositif d'alerte ;

Afin de pouvoir invoquer ce fondement, le responsable du traitement s'assure de la réalisation des conditions suivantes :

- l'obligation de mettre en œuvre un dispositif d'alerte résulte d'une source interne du droit français (par exemple, la loi « Sapin » et son décret d'application), d'un engagement international signé et ratifié par la France (par exemple, une convention internationale), ou encore du droit dérivé des organisations internationales et européennes dont la France est partie ;

- l'organisme y est effectivement soumis au regard des critères retenus par la réglementation en question (par exemple, le dépassement des seuils de taille des effectifs, du chiffre d'affaires, la réalisation des opérations d'une certaine nature, etc.).

b) La réalisation de l'intérêt légitime poursuivi par l'organisme ou par le destinataire des données, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés

fondamentaux de la personne concernée.

Ce fondement juridique s'applique lorsque la mise en place d'un dispositif d'alerte ne résulte pas d'une obligation légale s'imposant au responsable du traitement.

Il incombe à chaque responsable du traitement de s'assurer du choix de l'une et/ou de l'autre de ces bases, en fonction des règles qui sont applicables à son entité.

Lorsqu'un dispositif répond à une obligation légale précise (par exemple, celles résultant des articles 8 et/ou 17 de la Loi « Sapin II », de la Loi « devoir de vigilance », etc.), tout en permettant le recueil d'alertes relatives à un engagement volontaire de l'organisme (par exemple, prévues par un code éthique interne, ou encore prévues par un texte législatif auquel l'organisme n'est pas juridiquement soumis), il appartient au responsable du traitement de distinguer les bases légales qui fondent chacune de ces finalités.

5. Données personnelles concernées

5.1. Principes de pertinence et de minimisation des données

5.1.1. Au stade de l'émission de l'alerte

De manière générale, le responsable de traitement doit veiller à ce que seules les données nécessaires à la poursuite des finalités du traitement soient effectivement collectées et traitées. Une attention particulière doit à cet égard être portée aux faits pouvant être signalés via les dispositifs d'alertes professionnelles mis en place, d'initiative, par des organismes qui ne sont pas assujettis à des obligations spécifiques en ce sens. En l'absence d'encadrement spécifique par les textes législatifs et réglementaires en vigueur, il incombe au responsable du traitement de s'assurer tout particulièrement du respect, dans cette hypothèse, des droits, libertés et intérêts légitimes de l'ensemble des personnes pouvant être concernées par une alerte.

Toutefois, dans le cas des dispositifs d'alerte professionnelle, seul le lanceur d'alerte est en capacité de déterminer la nature et le volume des informations, notamment à caractère personnel, communiquées à l'occasion du signalement.

Partant, le responsable du traitement doit rappeler aux auteurs de signalements que les informations communiquées dans le cadre d'un dispositif d'alerte, doivent rester factuelles et présenter un lien direct avec l'objet de l'alerte.

5.1.2. Au stade de l'instruction de l'alerte

Pour les besoins de ce référentiel, la phase d'instruction d'une alerte est entendue comme la période qui débute par la réception de l'alerte par l'organisme, et qui se termine par la prise de décision quant aux suites réservées à celle-ci.

Cette phase permet à l'organisme de mener une enquête sur les faits signalés. Pendant cette période, le dispositif d'alerte peut être utilisé en vue de documenter les diligences accomplies par l'organisme en ce sens (analyse juridique et technique des faits, collecte des preuves, échanges avec différentes parties prenantes, audition des témoins, réalisation d'actes d'expertise, etc.).

La phase d'instruction est caractérisée par le rôle du responsable de traitement dans la

détermination des éléments qui pourront être collectés ou conservés dans le dispositif.

Il lui appartient donc de s'assurer que seules les informations pertinentes et nécessaires au regard des finalités du traitement sont collectées et/ou conservées dans le dispositif d'alerte. Tel est généralement le cas des catégories suivantes :

- identité, fonctions et coordonnées de l'émetteur de l'alerte ;

- identité, fonctions et coordonnées des personnes faisant l'objet de l'alerte ;

- identité, fonctions et coordonnées des personnes intervenant dans le recueil ou dans le traitement de l'alerte ;

- faits signalés ;

- éléments recueillis dans le cadre de la vérification des faits signalés ;

- comptes rendus des opérations de vérification ;

- suites données à l'alerte.

5.2. Le traitement de données sensibles et de données d'infraction

Deux catégories de données appellent une vigilance renforcée.

D'une part, certaines données, en raison de leur caractère particulièrement sensible, notamment celles qui révèlent l'origine ethnique ou prétendument raciale, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, des données génétiques, des données biométriques, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne, bénéficient d'une protection particulière et ne peuvent être traitées que moyennant le respect de conditions spécifiques figurant à l'article 9 du RGPD et aux articles 6 et 44 de la LIL.

Dans le cadre du présent traitement, ces données peuvent notamment être traitées dès lors que le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice, conformément à l'article 9-2-f du RGPD.

D'autre part, les données collectées et traitées dans le cadre des dispositifs de recueil d'alertes professionnelles peuvent également comprendre des données relatives aux infractions, condamnations et mesures de sûreté concernant des personnes physiques. De telles données ne peuvent être collectées et traitées que dans des conditions strictement définies à l'article 10 du RGPD et à l'article 46 de la LIL.

Dans le cadre du présent traitement, la collecte de ces données peut être autorisée :

- par des dispositions spécifiques du droit national (par exemple, articles 8 ou 17 de la Loi « Sapin 2 », article L. 225-102-4.-I. du Code de commerce, etc.) ;

- ou pour permettre au responsable de traitement « 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 », conformément à l'article 46-3° de la LIL.

5.4. Traitement de l’identité de l’auteur d’une alerte

Un dispositif d’alerte peut imposer ou proposer que l’auteur de l’alerte s’identifie.

Si l’émetteur de l’alerte professionnelle doit s’identifier, son identité est traitée de façon confidentielle par l’organisation ou les personnes chargées de la gestion des alertes.

Il est toutefois recommandé que l’organisme n’incite pas les personnes ayant vocation à utiliser le dispositif à le faire de manière anonyme, étant entendu qu’une alerte anonyme est une alerte dont l’auteur n’est ni identifié ni identifiable.

Par exception, l’alerte d’une personne qui souhaite rester anonyme devrait être traitée sous les conditions suivantes :

- la gravité des faits mentionnés est établie et les éléments factuels sont suffisamment détaillés ;

- le traitement de cette alerte doit s’entourer de précautions particulières, telles qu’un examen préalable, par son premier destinataire, de l’opportunité de sa diffusion dans le cadre du dispositif.

Après s’être assuré de la nécessité et de la pertinence des données personnelles qu’il utilise, l’organisme doit par ailleurs s’assurer, tout au long de la durée de vie du traitement, de la qualité des données qu’il traite. Cela signifie en pratique que conformément à la règlementation, les données soient exactes et mises à jour.

6. Destinataires des informations

Les données personnelles doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions.

Les habilitations d’accès doivent être documentées par les organismes, et les accès aux différents traitements doivent faire l’objet de mesures de traçabilité. Voir point 9 relatif à la sécurité.

Le responsable de traitement qui souhaite avoir recours à un sous-traitant doit veiller à ne faire appel qu’à des organismes présentant des garanties suffisantes. Un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données doit être établi entre elles (article 28 du RGPD). Un guide du sous-traitant, édité par la CNIL, précise ces obligations et les clauses à intégrer dans les contrats.

6.1. Les personnes accédant aux données pour le compte de l’employeur

Seules les personnes habilitées au titre de leurs missions ou de leurs fonctions, doivent pouvoir accéder aux données à caractère personnel traitées, et ce dans la stricte limite de leurs attributions respectives et de l’accomplissement de ces missions et fonctions.

Il peut s’agir, par exemple :

- des personnes spécialement chargées de la gestion des alertes au sein de l’organisme ;

- du référent ou prestataire de service chargé de recueillir et traiter les alertes. Le référent ou prestataire de service éventuellement désigné pour gérer tout ou partie de ce dispositif s'engage notamment, par voie contractuelle, à ne pas utiliser les données à des fins autres que la gestion des alertes, à assurer leur confidentialité, à respecter la durée de conservation limitée des données et à procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation.

6.2. Les destinataires des données

Le RGPD définit les destinataires comme « tout organisme qui reçoit la communication des données ».

Dans le cadre de ce traitement, les données peuvent être communiquées au sein du groupe de sociétés auquel appartient l'organisme concerné si cette communication est nécessaire aux seuls besoins de la vérification ou du traitement de l'alerte.

Certaines dispositions légales ou réglementaires encadrent strictement la communication d'information. Ainsi, les éléments de nature à identifier l'émetteur de l'alerte ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'avec le consentement de la personne. De même, les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.

Pour assurer la continuité de la protection des données à caractère personnel, leur transfert en dehors de l'Union européenne est soumis à des règles particulières. Ainsi, conformément aux dispositions des articles 44 et suivants du RGPD, toute transmission de données hors de l'UE doit :

- être fondée sur une décision d'adéquation ;

- ou être encadrée par des règles internes d'entreprise (« BCR »), des clauses types de protection des données, un code de conduite ou un mécanisme de certification approuvé par la CNIL ;

- ou être encadrée par des clauses contractuelles ad hoc préalablement autorisées par la CNIL ;

- ou répondre à une des dérogations prévues à l'article 49 du RGPD.

Pour en savoir plus, consulter la rubrique « Transférer des données hors de l'UE » sur le site de la CNIL.

7. Durées de conservation

Conformément à l'article 5-1-e du RGPD, les données à caractère personnel ne doivent être conservées sous une forme permettant l'identification des personnes que le temps strictement nécessaire à la réalisation des finalités poursuivies. C'est donc au regard de la finalité que la durée de conservation sera déterminée.

La durée de conservation de données ou, lorsqu'elle est impossible, les critères utilisés

pour déterminer cette durée, font partie des informations qui doivent être communiquées aux personnes concernées.

Dans ces conditions, il incombe au responsable du traitement de déterminer cette durée en amont de la réalisation du traitement.

7.1. Les durées de conservation

Au regard des finalités pouvant justifier la mise en place d'un dispositif d'alerte, et sauf disposition légale ou réglementaire contraire :

- les données relatives à une alerte considérée par le responsable du traitement comme n'entrant pas dans le champ du dispositif, sont détruites sans délai du dispositif d'alertes professionnelles ou anonymisées conformément à l'avis 05/2014 relatif aux techniques d'anonymisation du Comité européen de la protection des données (CEPD).

- Lorsqu'aucune suite n'est donnée à une alerte rentrant dans le champ du dispositif, les données relatives à cette alerte sont détruites ou anonymisées par l'organisation chargée de la gestion des alertes, dans un délai de deux mois à compter de la clôture des opérations de vérification. Pour les besoins du présent référentiel, l'expression « suites » désigne toute décision prise par l'organisme pour tirer des conséquences de l'alerte. Il peut s'agit de l'adoption ou de la modification des règles internes (règlement interne, charte éthique, etc.) de l'organisme, d'une réorganisation des opérations ou des services de la société, du prononcé d'une sanction ou de la mise en œuvre d'une action en justice.

La Commission rappelle que les décisions relatives aux suites réservées aux alertes professionnelles doivent intervenir dans un délai raisonnable à compter de l'émission de celles-ci.

- Lorsqu'une procédure disciplinaire ou contentieuse est engagée à l'encontre d'une personne mise en cause ou de l'auteur d'une alerte abusive, les données relatives à l'alerte peuvent être conservées par l'organisation chargée de la gestion des alertes jusqu'au terme de la procédure ou de la prescription des recours à l'encontre de la décision.

A l'exception des cas où aucune suite n'est donnée à l'alerte, le responsable de traitement peut conserver les données collectées sous forme d'archives intermédiaires aux fins d'assurer la protection du lanceur de l'alerte ou de permettre la constations des infractions continues. Cette durée de conservation doit être strictement limitée aux finalités poursuivies, déterminée à l'avance et portée à la connaissance des personnes concernées.

Les données peuvent être conservées plus longtemps, en archivage intermédiaire, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales).

7.2. La conservation de données anonymisées

La réglementation relative à la protection des données à caractère personnel ne s'applique pas, notamment en ce qui concerne les durées de conservation, aux données anonymes, c'est-à-dire celles qui ne peuvent plus être mises en relation avec une ou des personnes physiques identifiées ou identifiables.

Partant, le responsable du traitement peut conserver sans limitation de durée les données anonymisées. Dans ce cas, l'organisme concerné doit garantir le caractère anonymisé des données de façon pérenne.

Pour en savoir plus, vous pouvez vous référer aux guides de la CNIL :

- « Sécurité : Archiver de manière sécurisée » ;

- « Limiter la conservation des données ».

Les données utilisées à des fins statistiques ne sont plus qualifiées de données à caractère personnel dès lors qu'elles auront ont été dûment anonymisées (Voir les lignes directrices du CEPD sur l'anonymisation).

Exemple :

Un organisme est soumis à l'obligation de mettre en place un dispositif d'alerte en application des dispositions de l'article 8 de la loi « Sapin 2 » (dispositif d'alerte général), mais également un dispositif d'alerte en application de l'article 17-II-2° de la même loi (dispositif visant à permettre le signalement de manquements ou situations contraires au code de conduite de l'organisme, dans le cadre de la lutte contre la corruption et le trafic d'influence).

Il est alors possible pour l'organisme de mettre en place un seul et unique outil de recueil de ces signalements. Toutefois, il peut exister des différences d'encadrement législatif et réglementaire des traitements. Ainsi, les modalités de mise en place des dispositifs d'alerte généraux sont encadrées, notamment en ce qui concerne les durées de conservation, par le décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte au sein des personnes morales de droit public ou de droit privé ou des administrations de l'Etat.

Or, ce décret n'est pas applicable en matière de lutte contre la corruption et le trafic d'influence. Les données recueillies via les dispositifs spécifiques d'alerte ne font donc pas l'objet d'un encadrement particulier et leur traitement doit être encadré en application de la réglementation.

La mise en place d'un outil unique de recueil des signalements implique de respecter les exigences législatives et réglementaires de chacun des dispositifs, et notamment de :

- différencier le traitement appliqué aux signalements portant sur des soupçons ou des faits de corruption de celui appliqué aux autres signalements ;

- d'appliquer des durées de conservation différentes selon que les données sont collectées dans le cadre de l'un ou l'autre des dispositifs d'alerte.

8. Information des personnes

Il incombe au responsable de traitement qui décide de mettre en place un dispositif d'alertes professionnelles, de s'assurer du respect des principes de transparence et de loyauté à l'égard des personnes dont les données peuvent être traitées.

Le respect de cette obligation suppose d'informer les personnes concernées individuellement et collectivement, selon les modalités décrites ci-après.

8.1. Identification des personnes concernées

Pour les besoins du présent référentiel, sont considérées comme « personnes potentiellement concernées » par un dispositif d'alertes professionnelles toutes les personnes qui peuvent potentiellement émettre un signalement via le dispositif ou être visées par une alerte, et notamment :

- Les effectifs propres de l'organisme concerné, quel que soit le statut juridique de collaboration (salariés, agents, intérimaires, stagiaires, salariés détachés par une entité tierce, bénévoles, etc.) ;

- Les collaborateurs, clients et fournisseurs extérieurs de l'organisme, lorsqu'il s'agit de personnes physiques ayant un lien contractuel direct avec l'organisme (consultants, agents, conseils, sous-traitants personnes physiques au statut d'autoentrepreneur, etc.) ;

- Les effectifs (salariés, associés, dirigeants, etc.) des personnes morales qui entretiennent un lien contractuel avec l'organisme concerné.

Sont considérées comme « personnes concernées » par un dispositif d'alertes professionnelles toutes les personnes dont les données à caractère personnel sont effectivement traitées dans le cadre du dispositif (par exemple, les auteurs des alertes, les personnes visées, les personnes entendues dans le cadre de l'enquête, etc.).

8.2. Contenu de l'information à délivrer

L'information communiquée aux personnes concernées doit se faire dans les conditions prévues par les articles 12, 13 et 14 du RGPD.

De manière générale, elle doit mentionner l'existence du traitement, ses caractéristiques (notamment les finalités poursuivies, les types de données susceptibles d'y figurer, les types de personnes susceptibles d'émettre l'alerte ou d'en faire l'objet, les principales étapes de la procédure déclenchée par l'alerte, les durées de conservation de données, etc.) ainsi que les droits dont disposent les personnes concernées.

Des modèles d'information sont disponibles sur le site de la CNIL et peuvent être consultés dans la rubrique « RGPD : exemples de mentions d'information ».

8.3. Les modalités de l'information

8.3.1. Consultations préalables à la mise en place du dispositif

Il appartient aux responsables de traitement de s'assurer, au regard de la réglementation qui leur est applicable, du respect de l'obligation d'informer et/ou de consulter les instances compétentes, lors de la mise en place des dispositifs d'alerte.

8.3.2. Information générale lors du déploiement du traitement

Afin de respecter pleinement les principes de loyauté et de transparence, le référentiel recommande que l'ensemble des personnes potentiellement concernées par le dispositif

en soient informées préalablement à son introduction dans l'organisme.

Cette information précise le fonctionnement du dispositif, notamment les étapes de la procédure de recueil des signalements, et en particulier les destinataires et les conditions auxquelles l'alerte peut leur être adressée.

Le responsable de traitement indique expressément que l'utilisation abusive du dispositif peut exposer son auteur à des sanctions ou des poursuites mais qu'à l'inverse, l'utilisation de bonne foi du dispositif n'exposera son auteur à aucune sanction disciplinaire, quand bien même les faits s'avéreraient par la suite inexacts ou ne donneraient lieu à aucune suite.

Le responsable de traitement rappelle que le dispositif d'alerte n'est qu'un moyen de signalement parmi d'autres (comme peut l'être la voie hiérarchique), et que le fait de ne pas y avoir recours ne peut entrainer aucune sanction à l'encontre des membres du personnel.

L'information individuelle des personnes (par exemple, via un envoi de courrier électronique sur la messagerie personnelle de la personne, remise d'un document individuel d'information sous forme papier, etc.) doit être privilégiée dans la mesure du possible.

8.3.3. Information spécifique du lanceur de l'alerte

Conformément à l'article 13 du RGPD, les personnes qui émettent un signalement via le dispositif, doivent recevoir les informations relatives au traitement dès le début du processus du recueil de l'alerte.

Elle peut notamment prendre forme d'un affichage d'une page ou d'un bloc de texte, préalablement à l'étape de la saisine des informations relatives à l'alerte. Le responsable de traitement peut subordonner l'accès à la réalisation d'une action (par exemple, le fait de cocher une case) indiquant que l'auteur de l'alerte a pris connaissance de ces informations.

Lorsqu'une alerte est émise, un accusé de réception de celle-ci doit être fourni au lanceur d'alerte pour permettre à celui-ci de bénéficier, le cas échéant, d'un régime de protection spécifique. Cet accusé de réception doit être horodaté. Il récapitule l'ensemble des informations et, le cas échéant, des pièces jointes communiquées dans le cadre du signalement. La remise de ce récépissé à l'auteur de l'alerte ne doit pas être subordonnée à la production d'informations identifiantes (adresse électronique ou postale, etc.) lorsque la personne souhaite conserver son anonymat.

Lorsqu'une décision sur les suites de l'alerte a été prise par le responsable du traitement, l'auteur de l'alerte en est informé.

8.3.4. Information spécifique de la personne visée par l'alerte

Conformément à l'article 14 du RGPD, le responsable de traitement doit informer la personne visée par une alerte (par exemple, en tant que témoin, victime ou auteur présumé des faits) dans un délai raisonnable, ne pouvant pas dépasser un mois, à la suite de l'émission d'une alerte.

Néanmoins, conformément à l'article 14-5-b du RGPD, cette information peut être différée lorsqu'elle est susceptible « de compromettre gravement la réalisation des objectifs dudit traitement ». Tel pourrait par exemple être le cas lorsque la divulgation de ces informations à la personne visée compromettrait gravement les nécessités de l'enquête, par exemple en présence d'un risque de destruction de preuves. L'information doit alors être délivrée aussitôt le risque écarté.

Cette information est réalisée selon des modalités permettant de s'assurer de sa bonne délivrance à la personne concernée. Elle ne contient pas d'informations relatives à l'identité de l'émetteur de l'alerte ni à celle des tiers.

Toutefois, lorsqu'une sanction disciplinaire ou une procédure contentieuse est engagée suite à l'alerte à l'égard de la personne visée, celle-ci peut obtenir la communication de ces éléments en vertu des règles de droit commun (droits de la défense notamment).

9. Droits des personnes

Les personnes concernées disposent des droits suivants, qu'ils exercent dans les conditions prévues par le RGPD (voir la rubrique qui s'intitule « respecter les droits des personnes » sur le site de la CNIL) :

- droit de s'opposer au traitementde leurs données, sous réserve des conditions d'exercice de ce droit en application des dispositions de l'article 21 du RGPD ;

- droit d'accès, de rectification et d'effacement des données qui les concernent ;

- droit à la limitation du traitement. Par exemple, lorsque la personne conteste l'exactitude de ses données, celle-ci peut demander à l'organisme le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires.

9.1. Droit d'accès

Toute personne dont les données à caractère personnel font ou ont fait l'objet d'un traitement dans le cadre d'une alerte professionnelle (lanceur de l'alerte, victimes présumées des faits, personnes visées par l'alerte, témoins et personnes entendues lors de l'enquête, etc.), a le droit d'y avoir accès conformément aux dispositions de l'art. 15 du RGPD.

L'exercice de ce droit ne doit pas permettre à la personne qui l'exerce d'accéder aux données à caractère personnel relatives à d'autres personnes physiques.

Cette limitation est propre aux règles relatives à la protection des données personnelles et ne fait pas obstacle à l'application, le cas échéant, des règles du droit processuel, des libertés fondamentales (et notamment du principe du contradictoire), etc.

9.2. Droit d'opposition

Conformément à l'article 21 du RGPD, le droit d'opposition ne peut pas être exercé pour les traitements nécessaires au respect d'une obligation légale à laquelle est soumis le responsable du traitement.

Il ne peut donc pas être exercé à l'égard des traitements mis en place par des sociétés

remplissant les conditions des articles 8 et/ou 17 de la Loi « Sapin II » ou encore celles de la partie I-4 de l'article L. 225-102-4 du code de commerce.

En revanche, lorsqu'un organisme ne remplit pas ces conditions, mais se dote d'un dispositif d'alertes sur une base purement volontaire, le droit d'opposition existe. Partant, les personnes concernées devront être informées de son existence et le responsable du traitement devra veiller à en assurer le respect.

Toutefois, l'exercice de ce droit n'est pas automatique : la personne qui l'exerce doit caractériser l'existence de « raisons tenant à sa situation particulière ».

Le responsable du traitement devra prendre en compte l'opposition, sauf à démontrer :

- qu'il existe des motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et intérêts de la personne concernée ou ;

- que le traitement est nécessaire pour la constatation, l'exercice ou la défense de droits en justice.

Or, les faits susceptibles de faire l'objet d'un signalement sont par leur nature même liés à la constatation, l'exercice et la défense des droits (notamment ceux des victimes ou responsables présumés des faits signalés, ou encore ceux de l'organisme, si sa responsabilité civile ou pénale peut être engagée, ou encore si l'alerte n'a pas été faite de bonne foi mais avait pour l'intention de nuire à la bonne marche de l'organisme, etc.).

Dans ces conditions, il appartient aux organismes concernés d'examiner chaque demande d'opposition en tenant compte de ces critères.

9.3. Droits de rectification et d'effacement

Le droit de rectification, prévu à l'article 16 du RGPD, doit s'apprécier au regard de la finalité du traitement.

Dans le cas des dispositifs d'alerte professionnelle, il ne doit notamment pas permettre la modification rétroactive des éléments contenus dans l'alerte ou collectées lors de son instruction. Son exercice, lorsqu'il est admis, ne doit pas aboutir à l'impossibilité de reconstitution de la chronologie des éventuelles modifications d'éléments importants de l'enquête.

Aussi ce droit ne peut-il être exercé que pour rectifier les données factuelles, dont l'exactitude matérielle peut être vérifiée par le responsable du traitement à l'appui d'éléments probants, et ce sans que soient effacées ou remplacées les données, même erronées, collectées initialement.

Le droit à l'effacement est exercé dans les conditions prévues par l'article 17 du RGPD.

10. Sécurité

L'organisme doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient

accès.

En particulier, dans le contexte spécifique du présent référentiel, soit l'organisme adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir :

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (login) unique à chaque utilisateur
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	Prévoir un système de journalisation
	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour

	Installer un « pare-feu » (firewall) logiciel
	Recueillir l’accord de l’utilisateur avant toute intervention sur son poste
Sécuriser l’informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des smartphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l’accès aux outils et interfaces d’administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données

Catégories	Mesures
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu’aucun mot de passe ou identifiant n’est transmis dans les URL
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les cookies non nécessaires au service
Sauvegarder et prévoir la continuité d’activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr

	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir une clause spécifique dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi
	S'assurer qu'il s'agit du bon destinataire
	Transmettre le secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues

	Conserver les secrets et les clés cryptographiques de manière sécurisée

Pour ce faire, le responsable de traitement pourra utilement se référer au guide de la sécurité des données personnelles.

(1) Article 8 ou Article 17-II-2° 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.

(2) Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.

La présidente,
M.-L. Denis