RÉFÉRENTIEL

RELATIF AUX TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL DESTINES A LA MISE EN ŒUVRE D'UN DISPOSITIF D'ALERTE

Version adoptée le 6 juillet 2023

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. A qui s'adresse ce référentiel ?

1. Ce référentiel s'adresse :

   - aux organismes privés ou publics qui sont tenus ou décideraient de mettre en œuvre un dispositif de recueil et de gestion internes des alertes professionnelles (DAP) impliquant un traitement de données à caractère personnel, quelle que soit leur taille et qu'ils soient ou non membres d'un groupe de sociétés national ou international ;
   - aux différentes entités tierces proposant des services liés à la réception, au traitement et à la conservation des alertes.

2. Les organismes mettant en place un DAP doivent s'assurer de sa conformité :

   - aux dispositions du Règlement général sur la protection des données (RGPD) et de la loi du 6 janvier 1978 « informatique et libertés » (LIL). En effet, lorsque ces dispositifs, comme c'est le cas en règle générale, impliquent la mise en œuvre d'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 ou générales (droit du travail). Le responsable de traitement doit garantir le respect des droits et des libertés fondamentales ainsi que des intérêts légitimes des personnes concernées.

2. Portée du référentiel

3. Ce référentiel a pour champ d'application **l'ensemble des traitements susceptibles d'être mis en place en vue d'assurer la réception et le traitement des alertes professionnelles.**

4. **Il s'applique en particulier aux traitements de signalements encadrés par des dispositions spécifiques du droit français, tels que :**

   - un dispositif d'alerte interne relevant de l'article 17.II.2° de la loi Sapin 2 modifiée et permettant le recueil des faits relatifs à « *l'existence de conduites ou de situations contraires au code de conduite de la société* » ;
   - un dispositif d'alerte interne relevant des articles 6 et suivants de la même loi et permettant (sous certaines conditions et limites) le recueil des faits tels qu' « *un crime ou délit, une menace ou un préjudice pour l'intérêt général, une violation, une violation supposée ou une tentative de dissimulation d'une violation : 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, du droit de l'Union européenne, de la loi ou du règlement* » ;

5. Le référentiel s'applique également aux dispositifs d'alertes mis en place sans contrainte règlementaire par des organismes, ou mis en œuvre pour se conformer à une obligation résultant du droit étranger, et dont le régime n'est pas expressément encadré par des règles juridiques françaises.

6. Afin de couvrir l'ensemble de ces dispositifs, le référentiel adopte une définition large de ce qui constitue une « alerte professionnelle » : **il s'applique ainsi aux traitements automatisés des données permettant de recevoir, traiter et conserver tout signalement effectué de bonne foi et qui révèle ou signale une violation de règles juridiques (qu'elles soient françaises, européennes, internationales ou étrangères) ou éthiques**.

7. Le référentiel a pour objectif de fournir aux organismes mettant en œuvre de tels traitements un outil d'aide à la mise en conformité à la réglementation relative à la protection des données à caractère personnel.

8. **Ce référentiel n'ayant pas de valeur contraignante,** les organismes peuvent s'en écarter. Il leur appartient néanmoins de justifier et de documenter ce besoin et les mesures mises en œuvre afin de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel. Les

traitements en question doivent être inscrits dans le registre prévu à l'article 30 du RGPD (voir modèle de registre).

9. Il appartient, en tout état de cause, aux acteurs concernés de s'assurer qu'ils respectent les autres réglementations qui peuvent par ailleurs trouver à s'appliquer (code de la fonction publique, code du commerce, code de l'action sociale et des familles ainsi que des dispositions éventuellement applicables des droits étrangers, sous réserve de leur compatibilité avec l'ordre public international, etc.).

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

11. Les organismes peuvent également se reporter aux outils méthodologiques proposés par la CNIL sur son site web en vue de faciliter la mise en conformité des traitements mis en œuvre. Ils seront ainsi à même de définir les mesures permettant d'assurer la nécessité et la proportionnalité de leurs traitements, de garantir les droits des personnes et la maîtrise de leurs risques. L'organisme pourra également s'appuyer sur les lignes directrices de la CNIL sur les AIPD. Si l'organisme en a désigné un, le délégué à la protection des données (DPD/DPO) devra être consulté.

3. Objectifs poursuivis par le traitement (finalités)

12. Le traitement des données d'alertes internes doit répondre à des objectifs précis et être justifié au regard des missions et des activités de l'organisme.

13. En ce qui concerne les DAP, le traitement de données est mis en œuvre afin de :

- recueillir et traiter les alertes ou signalements visant à signaler un manquement à une règle spécifique ;
- effectuer les vérifications, enquêtes et analyses nécessaires ;
- définir les suites à donner au signalement ;
- assurer la protection des personnes concernées ;
- exercer ou défendre des droits en justice.

Exemples :

Exemple 1.1 (alertes de l'article 6 de la loi « Sapin 2 » modifiée) :
Un DAP mis en œuvre pour répondre aux exigences de l'article 8.I.B de la loi « Sapin 2 » modifiée vise à permettre à l'ensemble des personnes énumérées à l'article 8.I.A de cette loi (membres du personnel, associés, actionnaires, collaborateurs extérieurs et occasionnels, cocontractants, sous-traitants, etc.), de signaler ou de divulguer « *un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation 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, du droit de l'Union européenne, de la loi ou du règlement* ».

Exemple 1.2 (lutte contre la corruption et le trafic d'influence, article 17.II.2° de la loi Sapin 2 modifiée) :
Un DAP anticorruption mis en œuvre pour répondre aux exigences de l'article 17.II.2° de la loi Sapin 2 modifiée, 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 DAP 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 DAP 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 contraire à une charte éthique de l'organisme, quel que soit l'auteur de l'alerte ou son lien avec l'organisme.

Exemple 3 (DAP uniques) :
Un DAP unique peut être mis en place pour répondre à plusieurs finalités distinctes, par exemple pour traiter à la fois les alertes « de droit commun » (article 6 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. Il devrait 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.

14. Les informations recueillies dans le cadre d'un DAP ne peuvent pas être réutilisées pour poursuivre un autre objectif qui serait incompatible avec les finalités mentionnées plus haut (v. le point 13).
A titre d'exemple, une réutilisation à des fins de la défense des droits de l'organisme dans le cadre d'un procès lié à l'alerte, constituerait *a priori* un objectif compatible. Il est à noter qu'en raison de l'encadrement strict des alertes professionnelles par le législateur, les hypothèses d'une réutilisation ultérieure des données d'une alerte sont en pratique très limitées. Par ailleurs, tout nouvel usage des données devra respecter l'ensemble des principes de protection des données personnelles.

15. Les traitements mis en œuvre ne doivent pas donner lieu à des mises en relation autres que celles nécessaires à l'accomplissement des finalités ci-dessus énoncées.

4. Bases légales du traitement

16. Chaque finalité du traitement doit reposer sur l'une des « bases légales » fixées par la réglementation. 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 DAP.**
    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 DAP résulte d'une source interne du droit français (par exemple, la loi « Sapin 2 »), d'un engagement international signé et ratifié par la France, ou encore du droit dérivé des organisations internationales et européennes dont la France fait 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 DAP ne résulte pas d'une obligation légale.

17. 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.

18. Lorsqu'un DAP 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 par un texte législatif auquel l'organisme n'est pas juridiquement soumis), il appartient au responsable du traitement de distinguer non seulement ces finalités elles-mêmes (v. le n°13), mais également les bases légales qui fondent chacune de celles-ci.

5. Données personnelles concernées

5.1 Principes de pertinence et de minimisation des données

5.1.1 Au stade du recueil de l'alerte

19. Pour les besoins de ce référentiel, la **phase de recueil d'une alerte est entendue comme la période couvrant la réception de l'alerte par l'organisme et l'envoi du récépissé à son auteur**.

20. 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 être portée aux faits pouvant être signalés via les DAP 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.

21. Les DAP présentent une particularité du fait que c'est le lanceur d'alerte qui choisit la nature et le volume des informations, notamment à caractère personnel, qu'il estime devoir communiquer. Le responsable de traitement est ensuite fondé à traiter ces données dans le cadre du signalement.

22. Néanmoins, il est recommandé au responsable du traitement de rappeler aux auteurs de signalements que les informations communiquées dans le cadre d'un DAP :

    - doivent rester factuelles et présenter un lien direct avec l'objet de l'alerte ;
    - ne doivent pas relever du secret de la défense nationale, du secret médical, du secret des délibérations judiciaires, du secret de l'enquête ou de l'instruction judiciaires ou du secret professionnel de l'avocat.

23. Lorsqu'un signalement émis de bonne foi s'avère être hors champ du DAP et sous réserve des dispositions spécifiques contraires, les organismes doivent garantir aux personnes concernées le même niveau de protection contre des représailles, ainsi que le même niveau de confidentialité de l'identité du lanceur d'alerte que ceux résultant des articles 6 et suivants de la loi Sapin 2 modifiée.

5.1.2 Au stade de l'instruction de l'alerte

24. 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 l'alerte et par l'information de son auteur**.

25. Cette phase permet à l'organisme de vérifier l'exactitude des faits signalés. Pendant cette période, le DAP 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 personnes susceptibles de fournir des informations pertinentes, réalisation d'actes d'expertise, prise de mesures conservatoires, etc.).

26. 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 DAP.

27. 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 DAP. Tel est généralement le cas des catégories suivantes :
    - alerte (les faits signalés) ;
    - identité, fonctions et coordonnées de :
        - l'émetteur de l'alerte ;
        - personnes faisant l'objet de l'alerte ;
        - personnes intervenant, consultées ou entendues dans le recueil ou dans le traitement de l'alerte ;
        - facilitateurs et personnes en lien avec l'émetteur de l'alerte ;
    - éléments recueillis dans le cadre de la vérification des faits signalés ;
    - comptes rendus des opérations de vérification ;

- suites données à l'alerte.

28. 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 les données soient exactes et mises à jour.

5.1.3 Après la prise de la décision sur les suites à réserver à l'alerte

29. Lorsque la décision sur les suites à donner à l'alerte est prise par l'organisme, seules les données nécessaires aux finalités suivantes peuvent être conservées :

- assurer la protection des différentes parties prenantes (auteurs des signalements, facilitateurs, personnes mentionnées ou visées dans l'alerte) contre le risque de représailles ;
- permettre de constater, exercer et défendre ses droits en justice ;
- réaliser des audits internes ou externes de ses processus de conformité.

30. L'organisme doit veiller à ce que les modalités de conservation de ces éléments écartent la probabilité d'un détournement des finalités de la conservation.

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

31. Deux catégories de données appellent une vigilance renforcée.

32. 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.

33. Dans le cadre du présent traitement, ces données peuvent notamment être traitées dans la mesure où la mise en place de DAP répond à un intérêt public important au sens de l'article 9.2.g) du RGPD ou encore est nécessaire, le cas échéant, à la constatation, à l'exercice ou à la défense d'un droit en justice au sens de l'article 9.2.f).

34. D'autre part, les données collectées et traitées dans le cadre des DAP 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 définies à l'article 10 du RGPD et à l'article 46 de la LIL.

35. Dans le cadre du présent traitement, la collecte des données sensibles et des données relatives aux infractions 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.

5.3 Traitement de l'identité de l'auteur d'une alerte

5.3.1 Signalements effectués de manière anonyme

36. La règlementation applicable aux alertes internes distingue entre « *les signalements effectués de manière anonyme* », et les signalements pour lesquels les auteurs ont fourni des informations susceptibles de les identifier.

37. **Pour les besoins de ce référentiel, sera considéré comme un « *signalement effectué de manière anonyme* » tout signalement dont l'auteur aura choisi de ne pas révéler son identité (nom,**

prénom, fonction, identifiants, adresse de courriel nominative, etc.), peu important qu'il puisse être possible de l'identifier au terme d'une enquête ou recherche complémentaire.

38. La plupart des dispositions régissant telle ou telle alerte spécifique (par exemple, le signalement d'une situation de conflits d'intérêts en application de l'article L. 135-3 du code général de la fonction publique (CGFP), le signalement des actes de violence, alertes anti-corruption de l'article 17 de la loi Sapin 2, etc.[1]) ne prévoient pas de règles particulières relatives au traitement des signalements effectués de manière anonyme. Il en va différemment dans le cas des alertes internes relevant du régime des articles 6 et suivants de la loi Sapin 2 modifiée. Dans ce dernier cas, les règles de procédure élaborées par les organismes doivent préciser « *les suites données aux signalements anonymes* ».

39. Les DAP mis en place par les organismes devraient permettre aux auteurs d'émettre leurs signalements de manière anonyme.

40. Le DAP devrait, dans ce cas, permettre une poursuite des échanges avec l'auteur de l'alerte tout en lui conservant le bénéfice de l'anonymat (il est par exemple envisageable de lui demander de fournir une adresse électronique qui ne permette pas son identification ou l'adresse d'une boîte postale).

41. Sauf obligation légale contraire ou consentement de l'auteur du signalement, **les organismes doivent s'abstenir de toute tentative de réidentification d'un lanceur d'alerte qui a souhaité émettre un signalement de manière anony**me.

42. Par application des principes de protection de vie privée par défaut et de minimisation des données par défaut, il est vivement recommandé aux entreprises de ne pas avoir recours à des procédés techniques rendant possible la réidentification des auteurs des signalements anonymes (dépôt des cookies et des pisteurs sur le terminal de l'utilisateur, collecte et recoupement des informations telles que les adresses IP, les paramètres de configuration du terminal, etc.).

5.3.2 Le traitement de l'identité du lanceur d'alerte

43. Si l'émetteur de l'alerte professionnelle choisit de s'identifier, ou si une disposition spécifique oblige l'organisme à identifier l'auteur d'un signalement anonyme, son identité est traitée de façon confidentielle par les personnes chargées de la gestion des alertes.

6. Accédants et destinataires des informations

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

45. 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 « 10. Sécurité » pour plus de détails.**

6.1. L'externalisation du traitement des alertes

46. Le recours à différentes formes de mutualisation ou d'externalisation des opérations liées au traitement du signalement est susceptible d'entrainer une qualification des entités concernées en tant que « responsable de traitement », « sous-traitant » ou « responsable conjoint de traitement », au sens du RGPD.

47. Il appartient à l'organisme qui décide de s'engager dans une telle démarche, de déterminer le statut respectif des parties prenantes précédemment à la mise en place du traitement en question. 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 (cf. le chapitre IV du RGPD « responsable du traitement et sous-traitant »).

[1] Pour une liste plus détaillée de dispositifs d'alerte relevant des régimes spécifiques, consulter rapport d'information n° N° 4325 déposé à l'Assemblée nationale par MM. les députés Rapahël GAUVAIN et Olivier MARLEIX, sur l'évaluation de l'impact 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 « loi Sapin 2 » (sp. p. 132, « 2. L'existence de nombreux statuts de protection »). Rapport disponible en ligne à l'adresse : https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b4325_rapport-information.pdf

48. 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, notamment lorsqu'il confie son canal de réception des signalements à un tiers agissant pour son compte.

49. Par ailleurs, **les différentes règles encadrant les différents dispositifs d'alertes spécifiques prévoient la possibilité, pour l'organisme mettant en place un DAP, de déléguer la totalité ou une partie des opérations de traitements des alertes, à des entités tierces**.

50. **Le présent référentiel n'a pas vocation à interpréter de telles dispositions,** et se borne à rappeler aux organismes mettant en place un DAP les règles en matière de protection des données à caractère personnel devant être respectées dès lors que le traitement des données afférent est effectué sous la responsabilité conjointe de deux ou plusieurs organismes, ou est confié à un ou plusieurs sous-traitants.

51. En toute hypothèse, il appartient à l'organisme souhaitant déléguer une partie des opérations liées à la réception ou traitement des signalements, de mener une **analyse de faisabilité juridique de cette délégation**.

Exemple des DAP internes relevant de l'article 6 de la loi Sapin 2 modifiée :

La transposition par la France de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des infractions au droit de l'Union a modifié les règles applicables à la possibilité, pour les organismes assujettis, de déléguer la fonction de traitement des alertes internes (article 8.I.B.4° de la loi Sapin 2 modifiée et l'article 7 de son nouveau décret d'application).

L'externalisation des canaux de réception des signalements apparaît largement ouverte à l'ensemble des organismes concernés par l'obligation de mettre en place un DAP : ils peuvent donc déléguer cette fonction à un tiers tel qu'un cabinet d'avocat, une plateforme spécialisée, ou un fournisseur de services de messagerie électronique. Les fonctions déléguées peuvent couvrir la réception de l'alerte (quelle qu'en soit la forme), mais aussi l'enregistrement d'un échange téléphonique ou audiovisuel en vue de sa transcription, sa consignation dans un procès-verbal, l'analyse initiale de la recevabilité de l'alerte et, enfin, l'émission du récépissé à destination de l'auteur du signalement.

La mise en commun des ressources aux fins d'évaluation de l'exactitude des faits invoqués dans le signalement, quant à elle, est en principe réservée aux seuls organismes employant moins de 250 personnes,[2] qu'ils soient, ou non, membres d'un groupe.

La nouvelle règlementation ne semble pas prévoir de possibilité de déléguer purement et simplement l'intégralité du traitement des alertes (leur réception, l'évaluation de leur recevabilité, la réalisation des investigations et des enquêtes complémentaires éventuelles, l'évaluation juridique et éthique des éléments collectés, la décision sur les suites à donner au signalement, la communication éventuelle avec les différentes personnes concernées par l'alerte, des personnes susceptibles de fournir des informations pertinentes, ainsi qu'avec des autorités externes) à une entité tierce.

Exemple des DAP spécifiques :

Les limites imposées à l'externalisation du traitement des alertes par les articles 6 et suivants de la loi Sapin 2 modifiée ne concernent que la gestion des « alertes internes » mentionnées par ce texte.

Les autres DAP (telles que les alertes anti-corruption de l'article 17 de la loi Sapin 2, par exemple) ne sont pas concernées par cette règlementation. Les organismes publics comme privés peuvent y avoir recours sans conditions particulières de taille des effectifs ou de nature des fonctions déléguées.

Exemple des DAP uniques :

Les organismes qui souhaitent mettre en place un DAP unique permettant de recevoir et traiter des alertes relevant des régimes différents, devraient respecter les conditions d'externalisation et/ou de mise en commun des ressources qui s'appliquent aux alertes internes de droit commun (v. ci-dessus).

[2] Par exception, l'article 8.I.B.4° de la loi Sapin 2 modifiée prévoit que « *Les communes et leurs établissements publics membres d'un centre de gestion de la fonction publique territoriale peuvent confier à celui-ci le recueil et le traitement des signalements internes dans les conditions prévues à l'article L. 452-43-1 du code général de la fonction publique, quel que soit le nombre de leurs agents.* »

6.2. Les personnes accédant aux données pour le compte de l'organisme

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

53. 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 DAP 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 ;
- de l'avocat/ du conseil chargé d'assister l'organisme ayant recueilli l'alerte ;
- d'une autre entité appartenant au même groupe, sous réserve des développements aux paragraphes 45 et suivants.

6.3. Les destinataires des données

54. Le RGPD définit les destinataires comme « *la personne physique ou morale, l'autorité publique, le service ou tout organisme qui reçoit la communication des données, qu'il s'agisse ou non d'un tiers* ».

55. Dans le cadre de ce traitement, il convient d'être particulièrement attentif à toute transmission des données en dehors de l'organisme ayant reçu l'alerte.

56. En effet, **certaines dispositions légales ou réglementaires encadrent strictement la communication d'information**[3]. Par exemple, la loi Sapin 2 modifiée précise que « *les éléments de nature à identifier le lanceur d'alerte ne peuvent être divulgués qu'avec le consentement de celui-ci* », la seule exception admise à cet égard étant la communication à l'autorité judiciaire, et ce uniquement « *dans le cas où les personnes chargées du recueil ou du traitement des signalements sont tenues de dénoncer les faits à celle-ci* » (cf. l'article 9.I, alinéa 2 de la loi Sapin 2 modifiée).

57. C'est pourquoi le décret n° n° 2022-1284 du 3 octobre 2022 prévoit que lorsqu'un signalement est susceptible d'intéresser non seulement l'organisme auquel il a été adressé, mais, par exemple, une autre société appartenant au même groupe, l'organisme en question ne peut pas transférer l'alerte, et ne peut que proposer à l'auteur du signalement de le faire directement.

58. Il en va de même pour les éléments de nature à identifier la personne mise en cause par un signalement et qui ne peuvent être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.

59. Les données peuvent notamment 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, sous réserve des développements des paragraphes 45 et suivants.

60. Pour assurer la continuité de la protection des données à caractère personnel, leur transfert en dehors de l'Union européenne (UE) 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 ;

[3] Article 9.I de la loi Sapin 2 modifiée ainsi que l'articles 6 du décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

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

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

7. Durées de conservation

62. 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.

63. Les informations relatives à la durée de conservation de données ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée, doivent être communiquées aux personnes concernées.

7.1 Les durées de conservation

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

- Les données relatives à une alerte peuvent être conservées en base active **jusqu'à la prise de la décision définitive sur les suites** à réserver à celle-ci. Cette décision doit intervenir dans un délai raisonnable à compter de la réception du signalement.

- Après la prise de la décision définitive sur les suites à réserver à l'alerte, les données pourront être conservées sous forme **d'archives intermédiaires**, « *le temps strictement proportionné à leur traitement et à la protection de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent, en tenant compte des délais d'éventuelles enquêtes complémentaires*[4] ».

- 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 intervenue.

65. 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), ou à des fins probatoires dans l'optique d'un contrôle ou d'un contentieux éventuel, ou encore à des fins de réalisation des audits de qualité des processus de traitement des signalements.

7.2 La conservation de données anonymisées

66. La réglementation relative à la protection des données à caractère personnel (le RGPD, la loi « informatique et libertés » modifiée, etc.) ne s'applique pas, notamment en ce qui concerne les durées de conservation, aux données anonymisées, c'est-à-dire celles qui ne peuvent plus être mises en relation avec une ou des personnes physiques identifiées ou identifiables (voir, pour plus de précisions, l'avis n° 05/2014 relatif aux techniques d'anonymisation du Groupe 29 (devenu Comité européen de la protection des données ou "CEPD").

67. De même, la loi Sapin 2 modifiée prévoit désormais pour les alertes internes que « *les données relatives aux signalements peuvent toutefois être conservées au-delà de [la durée nécessaire pour leur traitement et pour la protection des parties prenantes] à la condition que les personnes physiques concernées n'y soient ni identifiées ni identifiables* ».

68. Pour les besoins de ce référentiel, les expressions « *données [dans lesquelles] les personnes physiques concernées [ne sont] ni identifiées ni identifiables* » (au sens de la loi Sapin 2 modifiée) et « *données anonymisées* » (au sens de l'avis n° 95/2004 du G29, précité) sont considérées comme équivalentes.

[4] Article 9.III de la loi Sapin 2 modifiée.

69. 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.

70. 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.

Il est à noter que les termes « signalement / alerte anonyme » et « anonymat [de l'auteur du signalement] », utilisés dans la loi Sapin 2 modifiée, sont propres à ce texte et n'ont pas d'impact direct sur la qualification des données à caractère personnel traitées dans ce cadre. Il en résulte qu'un signalement anonyme au sens de la loi Sapin 2 modifiée peut ne pas être anonyme au sens de la réglementation en matière de la protection des données à caractère personnel (Voir les lignes directrices du CEPD sur l'anonymisation).

8. Information des personnes

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

72. 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.

73. Pour les besoins du présent référentiel, sont considérées comme « ***personnes potentiellement concernées*** » par un DAP toutes les personnes qui sont susceptibles d'émettre un signalement via le DAP ou d'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.

74. Sont considérées comme « ***personnes concernées*** » par un DAP toutes les personnes physiques dont les données à caractère personnel sont effectivement traitées dans le cadre du DAP (par exemple, les auteurs des alertes, les personnes visées, les facilitateurs personnes physiques, l'ensemble des personnes susceptibles de fournir des informations sur le signalement, qu'elles aient été nommées ou non par l'auteur du signalement, ainsi que les personnes protégées par ricochet conformément aux 2° et 3° de l'article 6-1 de la loi « Sapin 2 » modifiée).

8.2 Contenu de l'information à délivrer

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

76. 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 d'accès, de rectification et d'effacement dont**

disposent les personnes concernées, des règles applicables en cas de transfert hors UE et du **droit d'introduire une plainte auprès de l'autorité compétente**.

77. 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 DAP

78. 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 éventuelles instances compétentes, lors de la mise en place des DAP.

79. Il est également recommandé aux organismes de rendre régulièrement compte de l'utilisation des DAP aux instances représentatives de personnel.

8.3.2 Information générale lors du déploiement du traitement

80. Afin de respecter pleinement les principes de loyauté et de transparence, le référentiel recommande que l'ensemble des personnes potentiellement concernées par le DAP en soient informées préalablement à son introduction dans l'organisme.

81. Lorsque l'information individuelle, ou collective, des personnes potentiellement concernées se heurte à des difficultés pratiques (notamment pour des DAP dont l'utilisation est ouverte à des personnes extérieures à un organisme ou un groupe), il est recommandé aux responsables de traitement de rendre cette information facilement accessible (par exemple, via le site web de l'entité).

82. Cette information précise le fonctionnement du DAP, 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.

83. Le responsable de traitement indique expressément que l'utilisation abusive du DAP peut exposer son auteur à des sanctions ou des poursuites, mais qu'à l'inverse, l'utilisation de bonne foi du DAP 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.

84. Le responsable de traitement rappelle que le DAP 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 entraîner aucune sanction à l'encontre des membres du personnel.

85. L'information individuelle des personnes (par exemple, via un envoi de courrier électronique sur la messagerie personnelle de la personne, la 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

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

87. Dans le cas des signalements effectués en ligne, via un portail ou une application dédiée, cette information 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.

88. Lorsque le signalement est effectué d'une autre manière (par voie postale, par courrier électronique, par visioconférence, oralement, etc.), ces informations sont communiquées à l'intéressé dans les meilleurs délais et au plus tard au moment de l'envoi de l'accusé de réception de l'alerte.

89. Lorsqu'une alerte est émise, **un accusé de réception** de celle-ci doit être fourni au lanceur d'alerte, quel que soit le régime applicable au signalement,[5] pour permettre à celui-ci de bénéficier, le cas échéant, d'un régime de protection spécifique. Cet accusé de réception devrait être horodaté et récapituler 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 identifiante ou postale, etc.) lorsque la personne souhaite conserver son anonymat, mais seulement d'une information de contact lui permettant de délivrer l'accusé de réception.

90. Par ailleurs, la loi Sapin 2 modifiée ainsi que son décret d'application créent pour les auteurs des signalements le droit **d'être informés sur les mesures envisagées ou prises** pour évaluer l'exactitude des allégations et, le cas échéant, remédier à l'objet du signalement **ainsi que sur les motifs de ces dernières**[6]. Cette information doit être effectuée par écrit. Sa délivrance ne peut pas être subordonnée à la production d'informations identifiantes de l'auteur du signalement : seul un moyen de contacter le lanceur d'alerte est nécessaire.

8.3.4 Information spécifique de la personne visée par l'alerte

91. 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, sauf exception dûment justifiée, à la suite de l'émission d'une alerte.

92. Conformément à l'article 14-5-b) du RGPD, cette information peut effectivement 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.

93. 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.

9. Droits des personnes

94. Les personnes concernées disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD (voir la rubrique intitulée « respecter les droits des personnes » sur le site de la CNIL) :

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

95. 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,

---

[5] L'ensemble des organismes souhaitant bénéficier de la présomption de conformité résultant du respect de ce référentiel, sont concernées par cette exigence, y compris pour les DAP non soumis à l'article 4.II du décret n° 2022-1284 du 3 octobre 2022 *relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.*

[6] Article 4.III du décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte.

témoins et personnes entendues lors de l'enquête, facilitateurs, personnes protégées par ricochet, etc.), a le droit d'y avoir accès conformément aux dispositions de l'art. 15 du RGPD.

96. L'exercice de ce droit ne doit pas porter atteinte aux droits et libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Néanmoins, cette limitation ne peut pas avoir pour conséquence de priver la personne concernée d'accès à la totalité des informations visées à l'article 15.1 du RGPD (voir, pour plus de précisions, les lignes directrices du CEPD n° 01/2022 sur le droit d'accès[7]).

97. 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 et des libertés fondamentales (et notamment du principe du contradictoire).

9.2. Droit d'opposition

98. 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.

99. Il ne peut donc pas être exercé à l'égard des traitements mis en place par des sociétés remplissant les conditions des articles 8.B 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.

100. En revanche, lorsqu'un organisme se dote d'un DAP sur une base purement volontaire, le droit d'opposition peut être exercé. Les personnes concernées devront être informées de son existence et le responsable du traitement devra veiller à en assurer le respect. Il est toutefois à noter que lorsqu'il existe, l'exercice de ce droit n'est pas automatique : la personne qui s'en prévaut doit caractériser l'existence de « *raisons tenant à sa situation particulière* ».

101. S'agissant de personne dont les données sont mentionnées dans l'alerte ou apparaissent durant son instruction, le droit d'opposition peut être exercé, mais le responsable du traitement peut refuser d'y faire droit si :

    - il existe des motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et intérêts de la personne concernée ou ;
    - le traitement est nécessaire pour la constatation, l'exercice ou la défense de droits en justice.

102. 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).

103. Dans ces conditions, il appartient aux organismes concernés d'examiner chaque demande d'opposition, quelle que soit la qualité de la personne qui entend s'en prévaloir (l'auteur du signalement, la personne visée, les personnes ayant été contactées dans le cadre des vérifications, les personnes protégées par ricochet, etc.) en tenant compte de ces critères.

9.3. Droits de rectification et d'effacement

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

105. Dans le cas des DAP, 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.

---

[7] https://www.cnil.fr/fr/droit-dacces-guichet-unique-violation-de-donnees-le-cepd-publie-de-nouvelles-lignes-directrices

106. 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.

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

10. Sécurité

108. **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.

109. 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 attribué automatiquement ou par un administrateur
	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 et les responsabilités internes pour la gestion des incidents, dont la procédure de notification aux régulateurs des notifications de violation de données personnelles
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
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
	Sécuriser ses réseaux Wi-Fi, notamment en mettant en œuvre le protocole WPA3
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes

Catégories	Mesures
	habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou donnée personnelle 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
	Protéger les sauvegardes, notamment durant leur convoyage
	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 les développements informatiques	Prendre en compte la protection des données personnelles dès la conception
	Proposer des paramètres respectueux de la vie privée par défaut
	Éviter les zones de commentaires ou les encadrer strictement
	Utiliser des données fictives ou anonymisées pour le développement et les tests
Encadrer la maintenance et la fin de vie des matériels et des logiciels	Enregistrer les interventions de maintenance dans une main courante
	Encadrer les interventions de tiers par un responsable de l'organisme
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir des clauses spécifiques 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.)
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
Chiffrer, hacher ou signer	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues et sécurisées
	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.