Projet de recommandation

Relative à la sécurité des traitements critiques

Version soumise à consultation publique
jusqu'au 8 octobre 2023

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Introduction

1. Le présent document constitue une recommandation relative aux modalités de sécurisation des traitements automatisés de données à caractère personnel présentant des risques d'une ampleur particulièrement importante. Les traitements visés, ci-après dénommés « traitements critiques », sont caractérisés par les deux critères cumulatifs suivants :
   - le traitement est à grande échelle au sens du RGPD ;
   - une violation de données à caractère personnel pourrait soit entraîner des conséquences très importantes pour les personnes concernées, soit entraîner des conséquences pour la sûreté de l'État ou pour la société dans son ensemble (en raison de la perte de confidentialité, d'intégrité ou de disponibilité des données ou du traitement).
2. Ces traitements sont tels qu'une violation de données peut impliquer une action des pouvoirs publics pour en maîtriser ou corriger les conséquences. Par exemple :
   - les bases de données clients et autres traitements qui réunissent une part importante de la population française du fait de services essentiels fournis par le responsable du traitement, tels que dans les secteurs de l'énergie, des transports, des banques et assurances ou la fourniture d'accès à Internet ;
   - les services publics dématérialisés à grande échelle, que ce soit au niveau national ou régional, tels que les services des impôts, de gestion de l'identité, d'attribution des aides sociales ou d'assurance maladie ;
   - les traitements de santé à grande échelle, aussi bien dans le cadre du soin, de la gestion des épidémies, de la recherche ou des mutuelles ;
   - les traitements mis en œuvre dans le cadre de la fourniture de services nécessaires ou non à la sécurité de la population mais qui, du fait de leur popularité, ont conduit à la constitution d'une base de données contenant des données sensibles au sens du RGPD ou à caractère hautement personnel (au sens des lignes directrices concernant l'analyse d'impact relative à la protection des données du G29) d'une part importante de la population française.

   Étant donné leur statut, les opérateurs d'importance vitale (OIV), au sens de l'article R. 1332-1 du code de la défense et les entités dites essentielles et importantes visées par la directive européenne 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (dite directive « SRI 2 ») peuvent être concernés pour leurs traitements impliquant des données à caractère personnel.
3. La réglementation applicable à tous les traitements de données à caractère personnel impose aux responsables de traitement de mettre en œuvre des mesures afin de garantir la sécurité (confidentialité, intégrité, disponibilité) des données traitées. Cette obligation de moyens impose d'adopter une approche par les risques pour ajuster les mesures de sécurité en fonction des risques pour les personnes concernées.
4. Ainsi, les traitements ne correspondant pas à la définition d'un traitement critique introduite au paragraphe 1 et relevant du RGPD ou de la loi « informatique et libertés » doivent, en tout état de cause, mettre en œuvre les mesures permettant d'assurer un niveau de sécurité satisfaisant au regard de l'obligation de sécurité posée aux articles 5.1.f et 32 du RGPD et 99 et 121 de la loi « informatique et libertés ».
5. La CNIL rappelle que, pour tout traitement de données à caractère personnel, il est nécessaire de mettre en place les mesures de sécurité élémentaires. Le guide de la sécurité des données à caractère personnel publié par la CNIL ainsi que le guide d'hygiène informatique de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI), dans leur dernière version publiée, rappellent ces précautions qui devraient être mises en œuvre de façon systématique.
6. Par ailleurs, tous les responsables de traitement, en particulier ceux traitant des données sensibles au sens de l'article 9 du RGPD ou des données de personnes vulnérables telles que définies dans les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » adoptée le 4 avril 2017 par le groupe de travail « de l'Article 29 » sur la protection des données, peuvent s'inspirer des recommandations détaillées ci-après pour réduire les risques qui pèsent sur leurs traitements.
7. Les traitements critiques sont susceptibles d'être particulièrement ciblés par des attaquants qui disposent de fortes capacités ou de fortes motivations. De ce fait, la détermination et le suivi des mesures de sécurité nécessaires doivent faire l'objet d'un soin renforcé. En particulier, les risques auxquels ils sont soumis se doivent d'être correctement identifiés et traités.
8. Lorsque le traitement critique est soumis à des exigences sectorielles propres, l'application de la présente recommandation doit se faire sans préjudice de ces exigences sectorielles. En particulier, les traitements mis en œuvre dans le cadre d'activités en lien avec un statut d'OIV ou d'entité essentielle ou importante sont soumis à

des obligations de sécurité supplémentaires et spécifiques, respectivement détaillées par l'article R. 1332-1 du code de la défense et la directive « SRI 2 », dont certaines portent également sur des traitements de données à caractère personnel.

2. Gestion de la protection des données à caractère personnel

9. La CNIL recommande qu'une gouvernance de la protection des données à caractère personnel soit mise en place et maintenue, incluant dans son périmètre les traitements critiques de l'organisme. La protection des données à caractère personnel des traitements critiques devrait être un enjeu porté par la direction générale de l'organisme. À ce titre, cette dernière devrait s'assurer que des moyens suffisants sont mobilisés pour sécuriser les traitements critiques mis en œuvre et être régulièrement informée du niveau de sécurité de ces traitements par son responsable de la sécurité des systèmes d'information (RSSI) et par son délégué à la protection des données (DPD), par exemple par le biais de rapports réguliers (au moins annuels) compilant les éléments décrits dans les paragraphes suivants.
10. La CNIL recommande que l'organisme se fixe des objectifs de sécurité et de protection des données à caractère personnel, à même de le guider dans sa gouvernance de la protection des données. Ces objectifs devraient être clairs, vérifiables, mesurables et cohérents avec les risques que font peser le traitement de données à caractère personnel sur les personnes concernées (en raison, par exemple, des finalités ou de la nature des données). Une politique de sécurité et de protection de la vie privée devrait traduire ces objectifs en règles de fonctionnement pour l'organisme.
11. Afin de mesurer la réalisation de ces objectifs, la CNIL recommande que des indicateurs soient créés pour vérifier la sécurité du traitement dès sa mise en œuvre. Des procédures devraient être prévues afin de suivre de manière suffisamment régulière l'évolution de ces indicateurs, les menaces déjouées, les failles identifiées et le maintien en condition opérationnelle des systèmes d'information assurant leur sécurité (mises à jour, audits, etc.). À cet égard, la CNIL recommande la création d'un comité de suivi de la sécurité des systèmes d'information et de la protection des données, ou bien la mise en place d'une mission dédiée au sein d'un comité existant de suivi des systèmes d'information.
12. De plus, la CNIL estime que la sécurité des traitements critiques devrait faire l'objet d'une démarche d'amélioration continue, afin de permettre une progression constante de leur niveau de sécurité et de celui des infrastructures qui les portent. À cet effet, elle recommande qu'un bilan de sécurité du traitement soit réalisé de façon annuelle afin de tirer les leçons des éventuels incidents de sécurité dont le traitement aurait fait l'objet, ainsi que d'identifier et de mettre en œuvre, sous la forme d'un plan d'action, les axes de progression susceptibles d'accroître le niveau de sécurité du traitement. Cette démarche d'amélioration continue de la sécurité des traitements critiques peut être incluse dans une démarche plus générale de l'organisme concernant l'ensemble de sa sécurité informatique. Dans ce cas, le bilan et le plan d'action des traitements critiques peuvent faire l'objet d'une partie dédiée au sein du bilan et du plan d'action globaux des systèmes d'information.
13. Enfin, elle recommande que, pour chaque traitement critique, une personne soit spécifiquement désignée comme référente en matière de protection des données et de sécurité pour le traitement concerné. Ce référent devrait être une personne dont le rôle, déjà établi, la positionne au cœur du traitement. Ce rôle peut dépendre de la phase de vie du traitement, passant par exemple du chef de projet pendant la phase de conception à un agent opérationnel après la mise en production. Cette position doit lui apporter une connaissance approfondie du traitement, qui lui permette d'être l'interlocuteur principal, en cas de besoin, des équipes du DPD et du RSSI. Le référent pourra également être sollicité en cas d'échanges entre la CNIL et le responsable du traitement, notamment dans des situations pour lesquelles une certaine réactivité est nécessaire, par exemple lors d'une potentielle violation de données ou lors d'une situation d'urgence nécessitant une modification du dispositif, afin d'apporter son expertise et de fluidifier les échanges. Le rôle de référent ne se substitue pas à celui du DPD mais procure une connaissance approfondie du traitement, du fait de son implication dans la conception et/ou la mise en œuvre du traitement. L'organisme devrait anticiper toute indisponibilité ou départ de la personne désignée comme référent d'un traitement critique, afin d'assurer la continuité de la fonction.
14. Pour mettre en place un système de gestion de la protection des données à caractère personnel, le responsable du traitement peut s'appuyer sur des normes reconnues et éprouvées définissant de tels systèmes, telle que la norme ISO/IEC 27 701.

3. Gestion des risques

15. Si, comme pour tous les traitements, la gestion des risques constitue la pierre angulaire de l'obligation de sécurité, la CNIL considère que les traitements critiques devraient faire l'objet d'une démarche de gestion des risques particulièrement méticuleuse et suivie au plus haut niveau de direction de l'organisme.
16. Ainsi, les traitements critiques devraient systématiquement faire l'objet, avant la mise en œuvre des traitements, d'une analyse d'impact relative à la protection des données, telle que définie par le RGPD. Cette analyse devra être mise à jour régulièrement et fréquemment, afin de prendre en compte l'évolution des risques pesant sur le traitement. La CNIL recommande, en conséquence, que la nécessité de mettre à jour les analyses d'impact soit évaluée au moins une fois tous les deux ans, ainsi qu'à chaque changement substantiel du traitement, de son contexte ou de la menace.
17. Les traitements critiques étant soumis à des menaces particulièrement importantes, la CNIL estime qu'un soin tout particulier devra être porté à l'identification des sources de risques et à la détermination de leurs capacités. Ainsi, les scénarios de risques s'appuyant sur les éléments suivants devraient être pris en compte :
    - les attaques étatiques ou émanant d'organisations criminelles organisées, qui sont en capacité d'avoir recours à des attaques très élaborées, telles que les attaques visant les chaînes d'approvisionnement (« *supply chain attacks* »), susceptibles de s'inscrire dans un temps long ;
    - plus largement, la compromission de prestataires tiers, chargés du développement informatique, de la mise en œuvre, de l'hébergement ou bien des opérations de maintenance ou de support du traitement critique ;
    - l'exploitation de vulnérabilités inconnues de composants logiciels ou matériels (dites failles « *zero-day* ») ;
    - la compromission de personnes habilitées à accéder au traitement, en particulier celles disposant de privilèges élevés.
18. Pour réaliser une analyse de risques sur ses traitements critiques en concordance avec les points précédents, le responsable du traitement peut s'appuyer sur la méthode EBIOS Risk Manager (EBIOS RM) de l'ANSSI.
19. La CNIL recommande également que les traitements critiques fassent l'objet d'une homologation de sécurité (voir notamment le guide de l'ANSSI sur le sujet) avant leur mise en œuvre. Cette homologation de sécurité consiste, pour le responsable du traitement, à faire valider par la personne sous l'autorité de laquelle le traitement est mis en œuvre (par exemple, le directeur général dans une entreprise ou la personne délégataire du pouvoir de décision) le niveau de sécurité du traitement, les risques résiduels identifiés et le plan d'action visant à maintenir et à améliorer le niveau de sécurité du traitement dans le temps. Le processus d'homologation doit comprendre un audit complet du traitement critique avant que la décision d'homologation soit prononcée.

4. Nécessité de cultiver une maturité élevée en sécurité et protection des données à caractère personnel

20. La CNIL considère que les organismes qui mettent en œuvre des traitements critiques doivent, d'une manière générale, disposer d'un niveau de maturité élevé en matière de sécurité des systèmes d'information ainsi qu'en gestion de projets informatiques.
21. Ainsi, il apparaît incontournable que ces organismes soient dotés d'un RSSI et d'équipes chargées d'inclure les problématiques de sécurité dans les phases amont des projets de modification ou de création de systèmes d'information, puis de maintenir leur sécurité des systèmes dans le temps.
22. La CNIL recommande qu'une attention particulière soit portée à la sensibilisation à la sécurité informatique et à la protection des données à caractère personnel du personnel de l'organisme. Entre autres, les notions de données à caractère personnel et d'impact sur les personnes concernées devraient être abordées. Indispensable dès l'arrivée d'un collaborateur, la sensibilisation devrait ensuite être continue et adaptée aux nouvelles menaces. Les connaissances essentielles au maintien en condition de sécurité des systèmes informatiques (par exemple, concernant le risque d'hameçonnage ou la sensibilité des données à caractère personnel) devraient être évaluées, afin de confirmer leur bonne prise en compte par le personnel. Une culture de la sécurité de l'information et de la protection des données à caractère personnel devrait être entretenue au sein de l'organisme. Cette sensibilisation devrait également être étendue aux prestataires extérieurs intervenant sur le traitement critique.
23. Un exercice relatif à la sécurité informatique devrait être conduit régulièrement auprès du personnel de l'organisme, au moins une fois tous les deux ans. Chaque exercice devrait faire l'objet d'un bilan auprès des agents concernés pour mettre l'accent sur l'utilité des mesures de sécurité et revoir, le cas échéant, les mesures

et procédures prévues. Ces exercices peuvent être d'ampleur variable : du simple test (fausse campagne d'hameçonnage, clé USB laissée sur une table, etc.) à l'exercice de crise impliquant l'ensemble de l'organisme.

24. De plus, les personnels en charge de la conception d'un système informatique, de sa mise en œuvre, de son maintien en conditions opérationnelles et de sécurité et de sa fin de vie devraient bénéficier d'une formation continue à la sécurité informatique et à la protection des données à caractère personnel. La bonne assimilation des compétences indispensables devrait être régulièrement évaluée.
25. La sécurité des traitements critiques devrait être prise en compte dès leur conception et par défaut, selon les principes énoncés par les lignes directrices 4/2019 du Comité européen de la protection des données (CEPD) adoptées le 20 octobre 2020. Il est rappelé que le respect du principe de minimisation des données imposé par le RGPD participe à la réduction, par conception, des risques pesant sur les personnes concernées. La minimisation des données participe également à la simplification des mesures de protection à mettre en place et à la réduction des coûts liés.
26. Afin de respecter ces principes, la CNIL recommande que des exigences de sécurité et de protection des données à caractère personnel pour ces traitements soient déterminées en amont des premières phases de conception. Ces exigences devraient être cohérentes avec la nature des données à caractère personnel traitées ainsi qu'avec la nature, la portée, le contexte et les finalités du traitement critique en question. La sécurité et la protection des données à caractère personnel devraient être considérées au même niveau que les besoins fonctionnels du traitement (et non comme une simple exigence de conformité accessoire) et devraient être testées et validées au même titre que toute autre fonctionnalité.
27. La CNIL recommande également que le RSSI et le DPD, ou leurs équipes, soient systématiquement intégrés à la phase de conception des traitements critiques et lors d'une mise à jour fonctionnelle majeure. Le référent du traitement critique, de par son rôle dans le cycle de vie du traitement, devrait être impliqué naturellement dans ces étapes.
28. Elle recommande de privilégier les outils et briques informatiques développés par des tiers et dont les codes sources peuvent être mis à disposition à fin d'audit et/ou de correction des failles. L'usage de composants en source ouverte soutenus par une communauté solide est susceptible d'augmenter le niveau de sécurité des systèmes et de réduire les coûts de développement. La CNIL appelle cependant l'attention des responsables de traitements sur la nécessaire vigilance allant de pair avec l'usage de tels outils et briques informatiques. Il convient de s'assurer que :
    - ils ne contiennent pas de traceurs ou tout autre élément non maitrisé pouvant avoir un impact sur la protection des données à caractère personnel (par exemple, paramétrage intrusif par défaut, en violation du principe de protection des données par défaut) ;
    - ils soient correctement répertoriés en interne, c'est-à-dire de manière exhaustive et à jour ;
    - leur maintien en condition opérationnelle et de sécurité soit garanti ;
    - une veille informationnelle soit maintenue à leur sujet (notamment auprès des concepteurs de ces outils, d'experts ou encore des bulletins publics mis à disposition par des centres d'alerte spécialisés) afin que le RSSI prenne connaissance au plus tôt d'une éventuelle faille de sécurité liée à ces outils ou à leurs dépendances.
29. Certaines situations exceptionnelles peuvent nécessiter la mise en place de traitements de données à caractère personnel inédits, pour répondre à une urgence incompatible avec le temps nécessaire à la mise en œuvre des bonnes pratiques décrites dans cette recommandation. Pour pallier d'éventuelles vulnérabilités introduites par la mise en œuvre rapide du traitement, la CNIL recommande que de tels traitements ne soient mis en œuvre qu'à condition que leur usage soit limité raisonnablement dans le temps et qu'un plan d'action à même de répondre à l'ensemble des points de cette recommandation et des bonnes pratiques en termes de sécurité, soit défini et suivi. Tant que le plan d'action n'a pas permis de répondre aux risques sécuritaires induits par la situation d'urgence, une surveillance systématique et renforcée des opérations devrait être mise en place afin de détecter et de répondre à tout incident de sécurité.

5. Mise en place d'une démarche de défense en profondeur

30. Compte tenu des risques particuliers pesant sur les traitements critiques, la CNIL recommande aux responsables du traitement concernés de mettre en place une démarche globale de sécurité suivant le concept de défense en profondeur appliqué à la sécurité informatique, tel que présenté par l'ANSSI.
31. Ainsi, la sécurité des données et de leur traitement pour réduire un risque donné ne devrait pas être assurée par une mesure unique mais par un ensemble cohérent de mesures capables de parer à la défaillance d'une mesure unitaire. À titre d'exemple, si les données d'un traitement critique sont communiquées par le responsable à d'autres organismes, il conviendra de véhiculer les données via un canal de transmission chiffré et mutuellement authentifié, mais également de sur-chiffrer les données à la source afin de garantir la confidentialité en cas de compromission de l'envoi.
32. Dans le cadre de cette démarche de défense en profondeur, les responsables de traitements devraient s'inspirer de la logique « zéro confiance » (ou « *zero trust* »), en tant que modèle d'architecture limitant la confiance implicite accordée au sein du système de défense périmétrique, tel que présenté par l'ANSSI. Ce renforcement de la sécurité passe principalement par des mesures de cloisonnement, d'imputabilité et de maîtrise des accès plus granulaires et à tous les niveaux du traitement et des systèmes qui le supportent.
33. En outre, une analyse de la sécurité périmétrique (équipements réseau, etc.) de l'infrastructure technique sur laquelle repose un traitement critique devrait être réalisée, notamment si d'autres traitements, non critiques, reposent sur cette même infrastructure.
34. Les sauvegardes des traitements critiques devraient faire l'objet d'un cloisonnement renforcé, qui ne permette d'y accéder qu'à partir de postes d'administration durcis. Des tests de restauration des sauvegardes devraient être effectués régulièrement pour s'assurer qu'elles puissent répondre à leur fonction en cas de besoin. La mise en œuvre d'une sauvegarde hors ligne régulière et au moins une fois par an est indispensable. Les sauvegardes devraient être chiffrées.
35. Le responsable du traitement devrait également s'assurer que les plans de continuité et de reprise d'activité de l'organisme répondent aux besoins de sécurité des données à caractère personnel traitées. Entre autres, la confidentialité des données doit continuer d'être assurée malgré le fonctionnement dégradé du système, selon l'impact pour les personnes concernées en cas de violation.
36. Conformément aux bonnes pratiques en matière de sécurité, l'organisme met en place une veille active des nouvelles vulnérabilités concernant tous les composants de ses systèmes, menée par le RSSI et ses équipes. Cette veille devrait s'accompagner de la définition de processus et de mécanismes d'application des correctifs de sécurité adaptés à différentes situations de risque, selon leur gravité et leur vraisemblance. Si un correctif de sécurité est disponible, il devrait être appliqué dès que possible. Pour se prémunir des compromissions rapides après la divulgation publique d'une nouvelle vulnérabilité, le processus devrait prévoir d'appliquer en priorité et dans des courts délais les correctifs nécessaires aux services exposés sur Internet.
37. En complément de la veille active, les équipes de sécurité peuvent s'appuyer sur des outils de détection automatique de vulnérabilités. En procédant à des analyses (« *scans* ») continues ou hebdomadaires de son réseau et des systèmes supportant ses traitements critiques, l'organisme complète sa capacité à détecter leur présence dans son système d'information. Il doit être particulièrement attentif au périmètre couvert par l'outil choisi, et à la fréquence de mise à jour de la base de connaissance. Le même processus d'application des correctifs de sécurité que celui consécutif à la veille devrait s'appliquer.
38. En plus de cette démarche continue de détection et de correction des vulnérabilités, la CNIL recommande que les traitements critiques fassent l'objet d'audits de sécurité avant leur mise en service, puis régulièrement tout au long de leur cycle de vie. Chaque audit doit faire l'objet d'un plan d'action visant à corriger les failles identifiées dans des délais convenus. En complément de l'audit d'homologation, des audits plus poussés devraient être mis en œuvre régulièrement en ciblant différents points de contrôle : code source, architecture du système, configuration des équipements, gouvernance, tests d'intrusion, tests impliquant des données aléatoires (ou « *fuzzing* »), etc. Dans le cas où le responsable de traitement met en place un processus de prime à la faille détectée (« *bug bounty* »), il est indispensable d'encadrer une telle pratique au préalable, afin d'en assurer la légalité et de garantir la sécurité du traitement et la protection des données à caractère personnel.

6. Nécessité de se préparer activement à d'éventuels incidents de sécurité ou violation de données

39. La CNIL recommande que les traitements critiques fassent l'objet de mesures de traçabilité particulièrement poussées, mises en place dès l'intégration du traitement de données au système d'information et couvrant tous les équipements impliqués dans le traitement de données à caractère personnel. En particulier, la recommandation de la CNIL du 14 octobre 2021 sur le sujet devrait être appliquée.
40. Ces mesures de traçabilité devraient s'accompagner de mesures d'analyse automatique des journaux afin de faciliter la détection des éventuels incidents de sécurité et violations de données. Le responsable du traitement devrait, par exemple au moyen d'une procédure dédiée, préciser les critères conduisant à qualifier un incident de sécurité en tant que violation de données à caractère personnel.
41. La CNIL considère que les systèmes assurant la traçabilité des traitements critiques devraient être distincts du reste du traitement, et gérés par des équipes différentes, afin de garantir leur bon fonctionnement et leur intégrité en cas d'atteinte au reste du traitement. Une attention particulière devrait être apportée aux personnes habilitées à accéder aux données de traçabilité.
42. Les organisations mettant en œuvre des traitements critiques devraient être dotées, en interne ou de manière externalisée, d'un centre opérationnel de sécurité (COS ou SOC, pour « *security operations center* ») disposant d'outils dédiés à l'analyse des journaux et à la détection d'incidents, et notamment d'un système de gestion des informations et des événements de sécurité. En fonction des risques pesant sur le traitement critique, le responsable devrait envisager que l'équipe de détection d'incident soit opérationnelle à tout instant.
43. Lorsque les personnes concernées par les données utilisées par un traitement critique ont accès à une portion de ce traitement, il peut être pertinent de les considérer comme des acteurs de la sécurité du traitement. Il devrait ainsi être envisagé de donner accès aux personnes concernées à tout ou partie des données de traçabilité liées à leurs données à caractère personnel (par exemple, rappeler à la connexion la dernière date d'accès). Si la personne relève un accès anormal à ses données, un moyen de signalement ou d'action approprié devrait lui être proposé (par exemple, mettre fin à toutes les sessions de connexion actives).
44. Compte tenu du risque important lié à une violation de données des traitements critiques, la CNIL recommande que les procédures de gestion des violations soient anticipées en amont du traitement et formalisées dans une politique de réponse aux violations de données. Les procédures envisagées devraient avoir pour objectif principal de limiter, dans les plus brefs délais, les conséquences de la violation de données pour les personnes concernées. La politique de gestion des violations devrait prévoir les mesures nécessaires au respect des obligations, issues des articles 33 et 34 du RGPD et 102 de la loi « informatique et libertés », de documentation de la violation, de notification auprès de la CNIL et, le cas échéant, d'information des personnes concernées par la violation.
45. En plus de prévoir un protocole de réponse technique et organisationnelle générique, applicable à tout type de violation, la politique de gestion de ces dernières devrait définir des protocoles spécifiques à chacun des risques de violation de données les plus probables compte tenu des spécificités du traitement et des risques les plus couramment observés dans le contexte du traitement. En particulier, cette politique devrait prévoir les procédures de réponse aux risques liés à la cybercriminalité les plus fréquemment observés par la CNIL et par l'ANSSI (par exemple, dans les rapports annuels ou dans le Panorama de la cybermenace publié par le CERT-FR).
46. Les organismes mettant en œuvre des traitements critiques devraient également se doter d'une capacité de réponse rapide aux incidents, qui peut être assurée par un CSIRT (pour « *computer security incident response team* ») interne ou externe.
47. La politique de gestion des violations devrait définir la procédure à suivre par les éventuels sous-traitants auxquels a recours le responsable du traitement. Les processus de communication en cas de violation détectée par les sous-traitants devraient être clairement définis. Le responsable du traitement devrait s'assurer que les sous-traitants ont connaissance de cette procédure et ont mis en œuvre les moyens nécessaires à son application. Des exercices peuvent être programmés pour vérifier l'efficacité de ces procédures.

7. Maîtriser les relations avec les tiers

48. Comme pour tout traitement de données à caractère personnel, les interactions avec des tiers (sous-traitants, co-responsables du traitement, partenaires) sont autant de vecteurs d'attaque potentiels, pouvant constituer des vulnérabilités importantes. En conséquence, la CNIL recommande qu'un soin très important soit apporté à la gestion des relations avec les différentes parties prenant part aux traitements critiques.
49. Pour les sous-traitants, la CNIL rappelle qu'un encadrement contractuel conforme aux articles 28 du RGPD et 122 de la loi « informatique et libertés » doit être prévu. Elle considère que des exigences de sécurité devraient être formalisées et détaillées, par exemple sous la forme de niveau de service attendu (ou SLA, pour « *service-level agreement* »), à la hauteur des exigences que le responsable du traitement a identifiées pour le traitement (voir paragraphe 24). De plus, des mesures doivent être mises en œuvre afin de garantir une parfaite maîtrise de la sécurité du traitement sur le long terme par le responsable du traitement. À cet égard, la CNIL recommande qu'en fonction de la criticité de la prestation rendue par le sous-traitant, le responsable du traitement déploie des efforts proportionnés pour s'assurer du respect des obligations du contrat. Notamment, le responsable du traitement devrait auditer régulièrement les sous-traitants les plus critiques.
50. La CNIL rappelle qu'en vertu du point 2 de l'article 28 du RGPD, les sous-traitants doivent obtenir l'accord préalable du responsable du traitement pour tout ajout ou changement ultérieur d'un sous-traitant. Elle recommande que, dans les cas de traitements critiques, cet accord soit toujours explicite. À défaut d'accord, l'engagement contractuel devrait prévoir que le sous-traitant doit maintenir la prestation sous sa forme initiale pendant un délai suffisant à l'organisation d'une migration vers un autre service, ledit délai devant être de l'ordre de deux ans pour un système critique.
51. La CNIL recommande également que les sous-traitants se voient imposer la nécessité d'informer le responsable de traitement en cas de rachat ou de tout autre changement de contexte qui pourrait impacter les conditions matérielles ou contractuelles du service fourni.
52. En ce qui concerne les personnels des sous-traitants, la CNIL rappelle qu'ils devront être spécifiquement habilités à accéder au traitement critique et que le périmètre de leur habilitation devra être précisément défini. En fonction des opérations qui leurs seront confiées, un encadrement approprié devrait être mis en place pour que le responsable du traitement s'assure de conserver la maîtrise sur son traitement.
53. L'ANSSI a publié plusieurs référentiels pour encadrer les prestataires rendant plusieurs types de services en lien avec la sécurité. La CNIL recommande aux responsables de traitements critiques de se tourner vers les prestataires qualifiés selon ces référentiels ou de s'inspirer du contenu de ces référentiels pour sélectionner et encadrer les prestations fournies par d'autres acteurs.