SÉCURITÉ NUMÉRIQUE DES COLLECTIVITÉS TERRITORIALES

L'essentiel de la réglementation

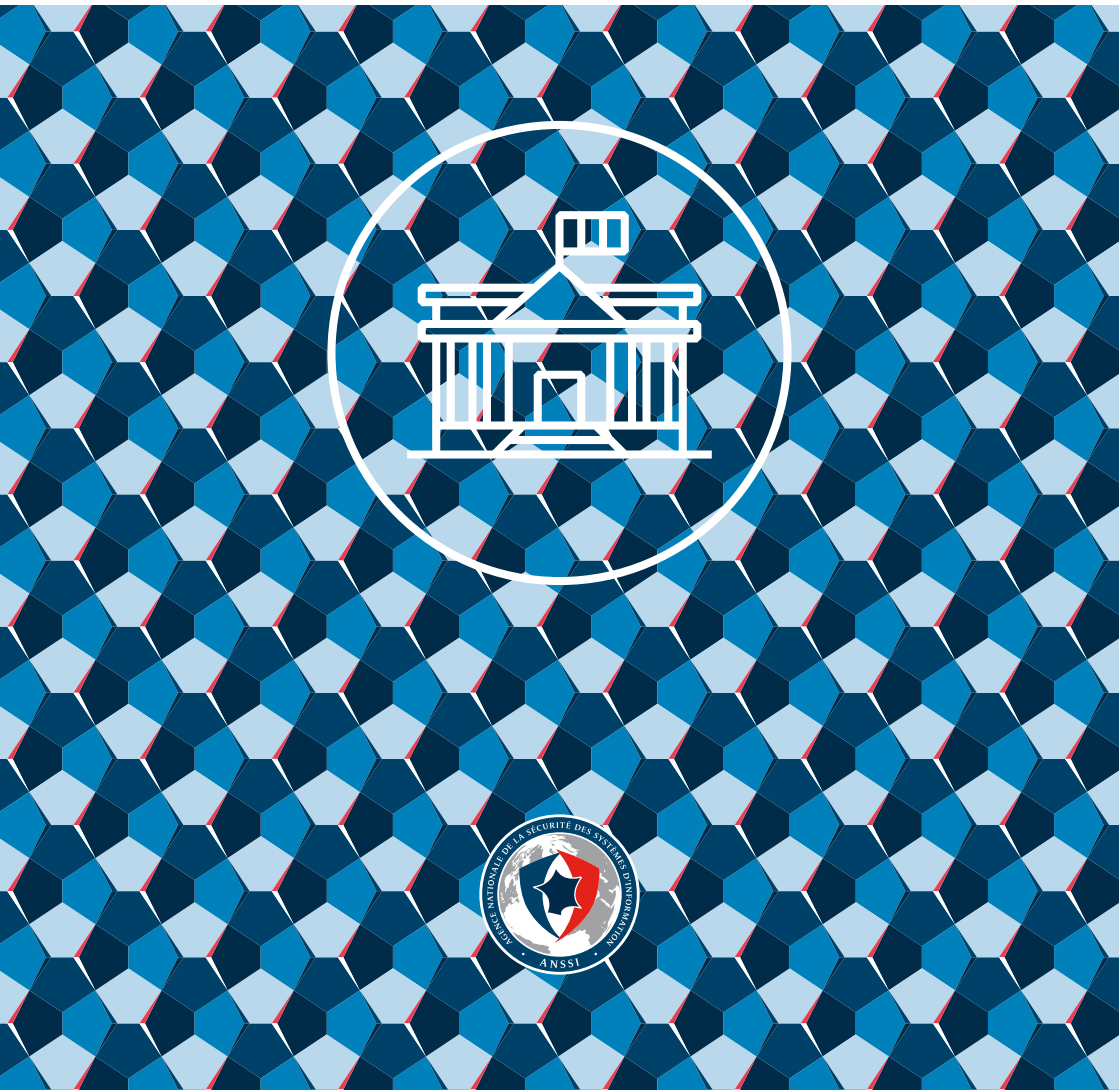


TABLE DES MATIÈRES

N.B.: les termes définis dans le glossaire sont suivis d'une étoile (*) lorsqu'ils apparaissent pour la première fois dans le texte.

PRÉAMBULE

Les collectivités territoriales (CT) sont engagées dans une transformation numérique profonde, autant pour répondre à des obligations règlementaires qu'à un souci de rendre un meilleur service aux citoyens. Cette dépendance de plus en plus forte aux systèmes d'information (SI), couplée à l'hétérogénéité de la taille des communes, crée une fragilité, soulignée dans la Revue stratégique de cyberdéfense (RSC) de 2018. Au même titre que les SI de l'État, des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE), la protection des SI des collectivités territoriales fait partie des champs prioritaires définis par la RSC pour consolider le modèle national de cyberdéfense.

Au-delà de l'application de mesures, qu'elles soient d'hygiène ou techniques, de gouvernance, organisationnelles et humaines, la dimension règlementaire et juridique est essentielle pour assurer une meilleure prise en compte des risques numériques.

Pour répondre au défi de la sécurité du numérique des collectivités territoriales, la France, soit directement par son droit national, soit via les règlements et directives pris au niveau de l'Union Européenne, s'est dotée d'un cadre règlementaire. Ce dernier participe à la protection de ces systèmes d'information et a pour objectifs :

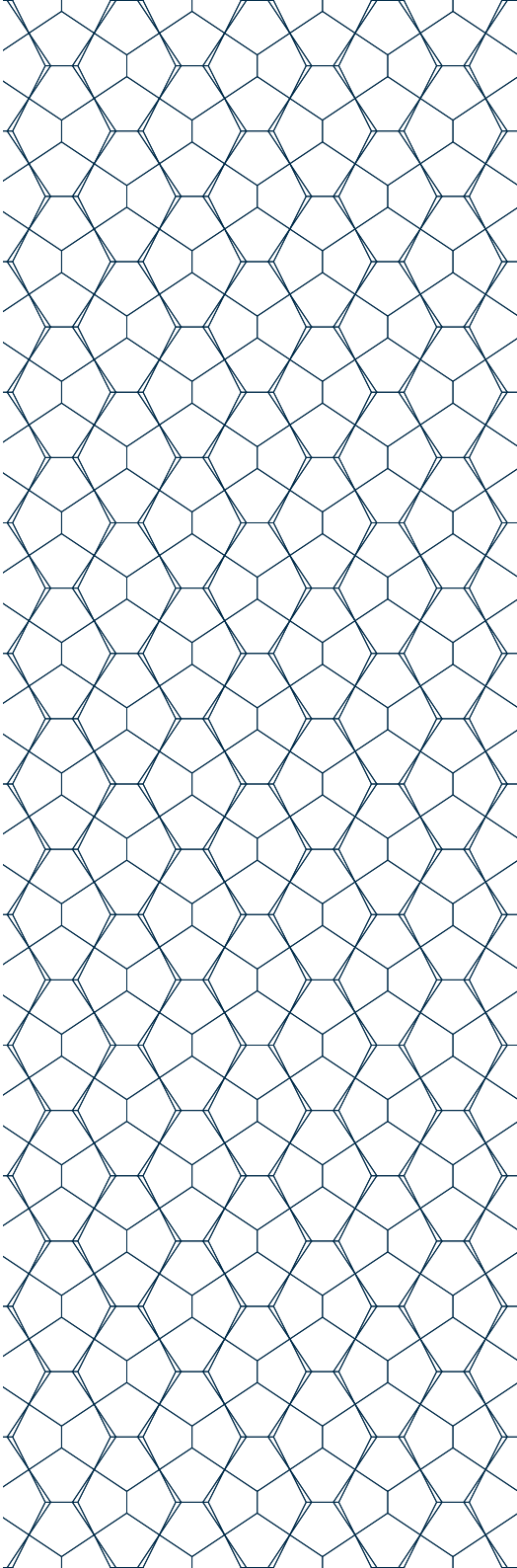
- le renforcement de la confiance des usagers dans l'utilisation des services numériques ;
- le renforcement de la sécurité des données à caractère personnel ;
- la transformation numérique des administrations l'État ;
- le renforcement de la sécurité des acteurs critiques pour l'État.
- Ces réglementations s'architecturent autour de trois principes fondamentaux :
- la **gouvernance** qui vise à impliquer l'ensemble des acteurs (décideurs,

agents, etc.) des collectivités territoriales dans la sécurité par la définition et le suivi d'une politique de sécurité des systèmes d'information (PSSI) ;

- la **gestion des risques** qui doit amener les collectivités territoriales à s'interroger sur les menaces auxquelles elles sont exposées et les mesures à mettre en œuvre pour s'en protéger tout en tenant compte d'un certain nombre de contraintes (financière, humaine, sociale, etc.) ;
- l'**amélioration continue** qui permet à la collectivité d'évaluer régulièrement son niveau de sécurité afin d'identifier les domaines dans lesquels elle doit progresser.

Pour les non-spécialistes et, singulièrement, pour les élus déjà en proie avec une multitude de règles et de textes à appliquer, le cadre règlementaire national participant à la protection des systèmes d'information des collectivités territoriales méritait un guide. Ce document se veut donc synthétique, pratique et abordable en particulier par les élus et les cadres territoriaux chargés d'en garantir l'application et la conformité.

PARTIE I : CADRE RÈGLEMENTAIRE



CHAPITRE I

Renforcer la confiance des usagers dans les services numériques

I/ Le cadre national du référentiel général de sécurité (RGS)

EN BREF :

En tant qu'autorités administratives, les collectivités territoriales ont l'obligation de respecter le référentiel général de sécurité (RGS). Ce texte règlementaire s'inscrit dans la politique publique de dématérialisation des démarches administratives et de confiance en l'économie numérique instauré par l'État. Il définit les exigences de sécurité (analyse de risque, homologation, etc.) pour tous les systèmes d'information (appelés téléservices*) mis à disposition des usagers et autorités administratives en vue de réaliser diverses démarches ou formalités administratives (déclaration d'imposition, règlement d'une contravention, plateforme de dématérialisation des marchés publics, etc.).

Le RGS définit également un processus de qualification des prestataires de services de confiance (délivrance de certificats électroniques, service d'horodatage électronique, etc.) sur lesquels les collectivités territoriales peuvent s'appuyer dans la mise en œuvre de leurs téléservices.

A QU'EST-CE QUE LE RGS ?

Le RGS est l'outil règlementaire permettant de sécuriser les échanges entre les autorités administratives et entre elles et leurs usagers. Le RGS a pour objectif le renforcement de la confiance des usagers dans les téléservices mis à disposition par les autorités administratives. Il s'impose ainsi à l'administration et peut être adapté aux enjeux et besoins de chacun.

Le RGS est pris en application du décret n° 2010-112 du 2 février 2010, lui-même pris en application de l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives.

B À QUI S'ADRESSE-T-IL ?

Le RGS s'impose spécifiquement aux téléservices mis en œuvre par les autorités administratives dans leurs relations avec les usagers et dans leurs relations entre elles. Les collectivités territoriales font partie des autorités administratives visées par l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 et sont, par conséquent, soumises aux obligations qui découlent de ce texte.

Sont des téléservices les systèmes d'information qui permettent :

- l'inscription des enfants à l'école ou à la cantine par Internet ;
- le paiement des factures d'eau par Internet ;
- la plateforme de dématérialisation des marchés publics ;
- une demande de prestation sociale par Internet ;
- les transferts de données vers une préfecture (par exemple contrôle de légalité) par Internet ;
- etc.

Indirectement, le RGS s'adresse à l'ensemble des prestataires de services et des éditeurs de produits de sécurité proposant des services et des produits qualifiés au sens du RGS.

De façon générale, pour tout autre organisme du secteur public ou privé souhaitant organiser la gestion de la sécurisation de ses systèmes d'information et de ses échanges électroniques, le RGS se présente comme un guide de bonnes pratiques conformes à l'état de l'art.

C QUE CONTIENT-IL ?

Le RGS se compose d'un corpus documentaire s'adressant aussi bien aux autorités administratives qu'aux prestataires de services de confiance tels que la délivrance de certificats électroniques, l'horodatage électronique ou encore l'audit de sécurité des systèmes d'information.

Les documents intéressant plus particulièrement les collectivités territoriales sont :

- le corps du RGS qui décrit la démarche que doivent suivre les collectivités territoriales lors de l'ouverture d'un téléservice. Cette démarche, détaillée dans la Fiche n°4 : Ouvrir un téléservice dans le respect des règles de sécurité du présent guide, impose :
  - la réalisation d'une analyse de risque ;
  - la définition des objectifs de sécurité ;
  - le choix et la mise en œuvre des mesures de protection et de défense du SI ;
  - l'homologation de sécurité du système d'information ;
  - le suivi opérationnel de sécurité du SI.
- dans le cas où l'analyse de risques fait apparaître la nécessité de recourir à des mécanismes cryptographiques (chiffrement, authentification, etc.), l'annexe B1 portant sur les recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques et l'annexe B3 portant sur les recommandations concernant les mécanismes d'authentification.

POUR PLUS D'INFORMATION :

Prestataires de services de confiance qualifiés (PSCE, PSHE, PASSI) : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/

Liste des produits qualifiés : www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/

Liste des produits certifiés :

- **CSPN** : www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/
- **CC** : www.ssi.gouv.fr/administration/produits-certifies/cc/produits-certifies-cc/

Fiche n°1 : Aide à la mise en œuvre des réglementations – *page 56*

Fiche n°2 : Se préparer et réagir en cas d'incident de sécurité – *page 62*

Fiche n°3 : L'usage de la signature électronique – *page 73*

Fiche n°4 : Ouvrir un téléservice dans le respect des règles de sécurité – *page 80*

Fiche n°6 : Recourir à l'externalisation pour la gestion du système d'information – page 93

Autorité compétente : Agence nationale de la sécurité des systèmes d'information (ANSSI)

mél. : rgs@ssi.gouv.fr

II/ L'apport européen du règlement nº910/2014 dit « eIDAS »

EN BREF :

Le règlement eIDAS est un texte européen qui s'applique aux organismes du secteur public interagissant par voie électronique avec le public [1]. Il a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur et établit un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques au sein de l'Union européenne.

Le règlement eIDAS développe deux axes consacrés respectivement à l'identification électronique et aux services de confiance (signature électronique, envoi recommandé électronique, etc.). Il traite également, dans une moindre mesure, des documents électroniques en leur accordant un effet juridique.

A QU'EST-CE QUE LE RÈGLEMENT EIDAS ?

Le règlement nº 910/2014 du 23 juillet 2014 [2], dit « règlement eIDAS » est un texte européen entré en vigueur le 17 septembre 2014 et

1 Ce qui distingue le règlement eIDAS du RGS qui, lui, se limite aux seules autorités administratives et qui couvre non seulement les téléservices à destination du public mais également les téléservices mis en œuvre entre autorités administratives.
2 Ce règlement abroge la directive européenne 1999/93/CE sur la signature électronique.

directement applicable en France. Il concerne l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Ce règlement a pour objectifs :

- d'accroître la confiance dans les transactions électroniques au sein du marché intérieur ;
- d'établir un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques ;
- d'accorder un effet juridique à l'utilisation des services de confiance qualifiés.

Le règlement est applicable :

- depuis le 1er juillet 2016 pour la qualification des prestataires de confiance ;
- depuis le 29 septembre 2018 pour la reconnaissance obligatoire des moyens d'identification électronique par les États membres.

B À QUI S'ADRESSE-T-IL ?

Les collectivités territoriales mettant en œuvre une identification électronique, une signature électronique ou un cachet électronique dans le cadre de service en ligne qu'elles mettent à disposition du public, sont directement concernées par ce règlement.

En effet, les collectivités territoriales exigeant une identification électronique de niveau de garantie substantiel ou élevé (*cf.* ci-dessous pour la présentation des différents niveaux de garantie) seront tenues d'accepter l'ensemble des moyens d'identification électronique de niveau égal ou supérieur, notifiés par un État membre de l'Union européenne.

De manière similaire, les collectivités territoriales exigeant une signature électronique ou un cachet électronique de niveau de garantie avancé [3] ou qualifié seront tenues d'accepter l'ensemble des signatures

3 Ce niveau de garantie couvre également les signatures électroniques ou les cachets électroniques avancés reposant sur un certificat qualifié.

ou cachets électroniques de niveau égal ou supérieur, notifiés par un État membre de l'Union européenne.

Les collectivités territoriales ne peuvent donc pas refuser des signatures ou cachets électroniques d'un niveau supérieur au niveau qualifié au sens du règlement mais pour autant n'étant pas conforme au RGS. Cependant, les signatures ou cachets électroniques mis en œuvre par les collectivités territoriales dans le cadre d'échanges avec les usagers ou autorités administratives doivent être conformes au RGS.

PAR EXEMPLE :

Le recours à la signature électronique des documents échangés dans le cadre de la dématérialisation des marchés publics, oblige à accepter l'ensemble des signatures électroniques ayant un niveau de garantie avancé ou qualifié et notifiées par la France ou d'autres États membres. Cela permet, par exemple, à une entreprise allemande de postuler à un marché ouvert par une collectivité territoriale avec les solutions de signature électronique notifiées par l'Allemagne et ayant le niveau de garantie avancé ou qualifié.

Le règlement prévoit en outre des exigences s'appliquant aux collectivités territoriales ou tout autre organisme se positionnant en fournisseur des services qualifiés reconnus au sens eIDAS.

En revanche, **le règlement ne s'applique pas** à la fourniture de services de confiance utilisés exclusivement dans des **systèmes fermés n'ayant pas d'impact direct sur des tiers (ex.: l'infrastructure de gestion de clé de l'administration [IGC/A], etc.), résultant du droit national ou**

d'accords au sein d'un ensemble défini de participants. Par exemple, une autorité administrative mettant en œuvre une infrastructure de gestion de clés pour couvrir ses besoins internes n'est pas soumise aux exigences du règlement eIDAS applicables aux services de confiance.

C QUE CONTIENT-IL ?

Deux sujets principaux sont concernés par le règlement eIDAS : l'identification électronique et les services de confiance.

1 – L'identification électronique

Le règlement instaure un mécanisme de reconnaissance mutuelle des moyens d'identification électronique des États membres pour l'accès aux services publics en ligne. Pour que cette reconnaissance soit effective, le moyen d'identification doit :

- avoir été préalablement notifié à la Commission européenne ;
- correspondre à un niveau de garantie substantiel ou élevé ;
- et avoir un niveau de garantie au moins égal à celui requis par l'organisation du secteur public concerné pour l'accès à un service en ligne.

Le règlement n° 910/2014 du 23 juillet 2014 introduit à cette fin trois niveaux de garantie pour les moyens d'identification électronique, caractérisés par la réponse qu'ils permettent d'apporter au risque de fraude ou d'altération de l'identité. Les trois niveaux de garantie prévus sont les suivants :

- **faible** : l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité. Ce niveau correspond typiquement au couple identifiant/mot de passe ;
- **substantiel** : l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité. À ce niveau, un second facteur d'authentification est nécessaire ;
- **élevé** : l'objectif est d'empêcher l'utilisation abusive ou l'altération de

l'identité. Par rapport au niveau substantiel, le moyen utilisé doit, en plus, être en mesure de résister à un potentiel d'attaque élevé.

Le règlement eIDAS est complété par le règlement d'exécution 2015/1502 du 8 septembre 2015 **fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique**.

2 – Les services de confiance

Le règlement eIDAS instaure un cadre juridique dans le cadre de l'utilisation des services de confiance qualifiés. Les services prévus par le règlement sont :

- la délivrance de certificats qualifiés de signatures électroniques, de cachets électroniques et d'authentification de site Internet ;
- la validation et la conservation de signatures électroniques qualifiées et de cachets électroniques qualifiés ;
- l'horodatage électronique qualifié ;
- l'envoi recommandé électronique qualifié.

Parmi les documents accompagnant le règlement eIDAS, le règlement d'exécution n° 2015/1506 du 8 septembre 2015 **établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organisations du secteur public**.

POUR PLUS D'INFORMATION :

Liste de confiance [LIST_CONF] : www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/liste-nationale-de-confiance/

Fiche n°1 : Aide à la mise en œuvre des réglementations – *page 56*
Fiche n°2 : Se préparer et réagir en cas d'incident de sécurité – *page 62*
Fiche n°3 : L'usage de la signature électronique – *page 73*
Fiche n°5 : Ouvrir un service numérique au public dans le contexte eIDAS – *page 88*
Fiche n°6 : Recourir à l'externalisation pour la gestion du système d'information – page 93

Autorité compétente : Agence nationale de la sécurité des systèmes d'information (ANSSI)
mél. : supervision-eIDAS@ssi.gouv.fr

III / L'articulation entre RGS et eIDAS

N.B. : le tableau ci-dessous a vocation à présenter au lecteur les différences entre les deux textes.

eIDAS	RGS
Périmètre organisationnel	
Le règlement eIDAS s'applique aux échanges entre l'administration et le public (citoyens, entreprises)	Le RGS s'applique aux échanges entre les autorités administratives et le public ainsi qu'aux échanges entre autorités administratives elles-mêmes
Périmètre fonctionnel	
Le règlement eIDAS couvre le service d'envoi recommandé électronique, service non couvert par le RGS	> Le RGS couvre le service de délivrance de certificat* d'authentification de personne qui n'est pas couvert par eIDAS > Le RGS couvre le service de délivrance de certificat d'authentification de machines qui n'est pas couvert par eIDAS > Le RGS couvre le service de délivrance de certificat de confidentialité qui n'est pas couvert par eIDAS
Usage	
Le règlement n'induit pas d'obligation pour les administrations de recourir à des moyens d'identification électronique notifiés ou à des services de confiance qualifiés au titre du règlement eIDAS	Si l'appréciation des risques implique le recours à une des fonctions de sécurité prévue dans le RGS, la mise en œuvre technique de cette fonction de sécurité doit s'appuyer sur des produits ou services conformes au RGS. **Cependant cette obligation de recours à des produits conformes ne peut être exigée pour les tiers (citoyens, entreprises)**

Tableau 1 : Articulation RGS / eIDAS

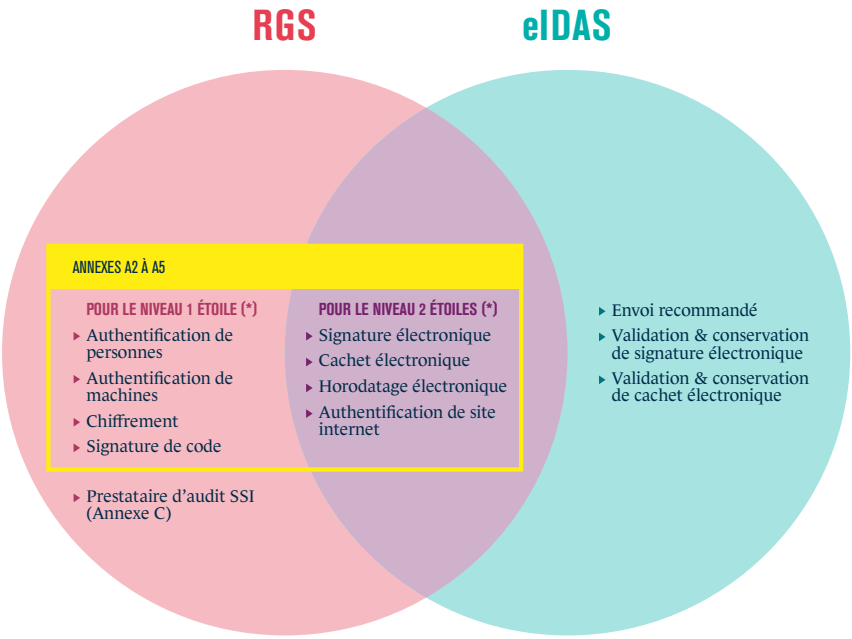


Figure 1 : Articulation eIDAS / RGS

CHAPITRE II

Renforcer la sécurité des données à caractère personnel

L'entrée en application du règlement général sur la protection des données (RGPD) au 25 mai 2018 **ne fait pas disparaître** la loi informatique et libertés (LIL). Cette dernière, afin de se mettre en conformité avec le RGPD et d'encadrer les traitements qui ne sont pas concernés, a fait l'objet d'évolutions successives.

Depuis le 25 mai 2018, le RGPD est le texte de référence comprenant les principales règles à mettre en œuvre en matière de protection des données personnelles. En synthèse la LIL est depuis lors un texte qui complète le RGPD sur des points où une marge de manœuvre est laissée aux États membres par le texte (cas des marges d'interprétation) ou qui encadre certains traitements de données personnelles qui ne relèvent pas du RGPD.

Si certains passages du RGPD sont reproduits dans la LIL, ces reprises ne sont pas exhaustives ou se limitent à de simples renvois. Il convient donc, s'agissant des collectivités territoriales, de toujours se référer au RGPD en premier lieu et, si nécessaire, de consulter la LIL afin d'identifier une éventuelle marge d'interprétation adoptée par la France.

I/ Le cadre européen du règlement général sur la protection des données (RGPD)

EN BREF :

Le RGPD est un texte européen qui s'applique aux collectivités territoriales car ces dernières sont responsables de traitements de données à caractère personnel.

Des exigences en matière de sécurité s'imposent, notamment :

- la nomination d'un *Data Protection Officer* (DPO) ;
- l'inventaire des traitements de données à caractère personnel mis en œuvre par l'organisation ;
- l'analyse d'impact relative à la protection des données nécessaire lorsque les traitements sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques ;
- l'obligation de sécurité dans la mise en œuvre de mesures de sécurité appropriées aux risques liés au traitement.

Certains éléments de cette section sont tirés du site Internet de la Commission nationale de l'informatique et des libertés (CNIL) [4].

4 www.cnil.fr/fr/comprendre-le-reglement-europeen

A QU'EST-CE QUE LE RGPD ?

1 – Cadre légal

Le règlement européen sur la protection des données à caractère personnel ou « RGPD » est le nom couramment donné au règlement (UE) nº 2016/679 du 27 avril 2016. Il concerne la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive nº 95/46/CE.

Le RGPD est **entré en vigueur le 26 mai 2016** et en **application depuis le 25 mai 2018**.

2 – Quel est l'objectif du RGPD ?

L'objectif du RGPD est de renforcer la protection et la libre circulation des données à caractère personnel au sein de l'UE *via* :

- le renforcement des droits des personnes (droit de rectification, droit à l'effacement, droit à la limitation du traitement, etc.) ;
- la responsabilisation des acteurs du traitement des données, qui se traduit notamment par une **obligation de sécurité des données à caractère personnel et l'encadrement de la sous-traitance** ;
- l'européanisation de la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront en particulier adopter des décisions communes ainsi que des sanctions renforcées lorsque les traitements de données seront transnationaux.

3 – Qu'est-ce qu'une donnée à caractère personnel ?

Selon l'article 4 du RGPD, une donnée à caractère personnel est « toute information se rapportant à une personne physique identifiée ou identifiable […] notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique,

culturelle ou sociale » [5].

Parmi les données à caractère personnel, certaines données dites « sensibles » font l'objet de mesures de protection particulières. L'article 9 du règlement prévoit ainsi que, sauf sous certaines conditions (§2), sont interdits « le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique […] ».

4 – Qu'est-ce que la protection des données à caractère personnel ?

La protection des données à caractère personnel repose sur plusieurs piliers, en particulier : la transparence et la licéité, les droits des personnes physiques concernées, la limitation des finalités, la minimisation des données, la pertinence et la durée de conservation. De plus, les données doivent être « traitées de façon à garantir […] la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) » [6].

B À QUI S'ADRESSE-T-IL ?

Les collectivités territoriales sont directement soumises au RGPD dans la mesure où les deux conditions d'application suivantes sont remplies :

- elles mettent en œuvre des traitements de données à caractère personnel

5 Par exemple, les données de l'agent (nom, prénom, numéro de téléphone professionnel, adresse de messagerie électronique professionnelle, etc.)
6 RGPD, Article 5, alinéa f).

(qu'ils soient sur support papier ou numérique) automatisés ou non (article 2 du RGPD, critère du champ d'application matériel) ;
- elles sont établies sur le territoire de l'Union européenne (article 3 du RGPD, critère du champ d'application territorial).

C QUE CONTIENT-IL ?

En matière de sécurité des données, l'article 25, alinéa 2 prévoit que « le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, […] les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée ».

Un article dédié – **l'article 32** – intitulé « sécurité du traitement » prévoit l'obligation pour les responsables de traitement ou les sous-traitants de « **garantir un niveau de sécurité adapté au risque** » pour les droits et libertés des personnes physiques via la mise en œuvre de « mesures techniques et organisationnelles appropriées » telles que :

- la **pseudonymisation*** ou le **chiffrement** des données à caractère personnel ;
- des moyens de garantir la disponibilité, la confidentialité, l'intégrité et la résilience des systèmes et services de traitement ;
- des moyens de garantir le rétablissement de la disponibilité des données à caractère personnel ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures.

L'article 33, dans le cadre d'une **violation de données à caractère personnel**, prévoit notamment la **notification** aux autorités de contrôle. Cette notification devra, le cas échéant, être étendue aux personnes concernées en application de l'article 34. Ces articles prévoient, notamment, de faire état dans la notification de la description des mesures proposées ou

mises en œuvre pour remédier à la violation de données ou, à tout le moins, en atténuer les conséquences.

L'article 35 présente **l'analyse d'impact relative à la protection des données**. Cette dernière doit être entreprise préalablement à la mise en œuvre du traitement lorsque celui-ci, s'appuyant notamment sur les nouvelles technologies, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. **Cette démarche est proche et complémentaire d'une démarche d'analyse de risque telle que celle décrite dans le RGS**.

L'article 37 prévoit l'obligation pour tout organisme public responsable de traitement, *de facto* les collectivités territoriales, de désigner un *data protection officer* (DPO)). Ce dernier remplace le correspondant informatique et libertés (CIL). Il participe notamment à la sécurité des données à caractère personnel dans les conseils et dans l'expertise qu'il amène au sein de l'organisation, notamment à l'occasion de la réalisation de l'analyse d'impact relative à la protection de ces données. Il est également en charge de contrôler, pour l'organisation pour laquelle il agit, l'application du règlement, notamment par les audits et la sensibilisation / formation du personnel à la protection des données.

L'article 40 introduit la possibilité d'adopter des codes de conduite. Ce dispositif doit permettre aux associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants de préciser les modalités d'application du règlement, pouvant notamment porter sur les mesures visant à assurer la sécurité des traitements.

Enfin, les articles 42 et 43 prévoient la mise en œuvre par chaque État membre des mécanismes de certification et de labellisation d'outils, de prestation et de compétence en lien avec la protection des données aux fins de démontrer que les opérateurs de traitements effectués respectent le règlement.

POUR PLUS D'INFORMATION :

« Kit sécurité des données » - ANSSI : www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/

Fiche n°1 : Aide à la mise en œuvre des réglementations – *page 56*
Fiche n°2 : Se préparer et réagir en cas d'incident de sécurité – *page 62*
Fiche n°6 : Recourir à l'externalisation pour la gestion du système d'information – *page 93*

Autorité compétente : Commission nationale de l'informatique et des libertés (CNIL)

Principes clés de la protection des données personnelles : www.cnil.fr/fr/collectivites-territoriales/les-principes-cles-de-la-protection-des-donnees
Impact du RGPD pour les collectivités territoriales : www.cnil.fr/fr/RGPD-quel-impact-pour-les-collectivites-territoriales
Guide de la sécurité des données personnelles : www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
La sécurité des données des administrés : www.cnil.fr/fr/la-securite-des-donnees-des-administres
Guide de sensibilisation au RGPD pour les collectivités territoriales : www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf
Cours en ligne (MOOC) RGPD : atelier-rgpd.cnil.fr/

II/ L'hébergement de Données de Santé (HDS)

EN BREF :

Les données de santé à caractère personnel sont des données sensibles. À ce titre, il convient de restreindre leur accès aux seules personnes autorisées et de garantir à tout moment leur disponibilité et leur intégrité. Le code de la santé publique prévoit en outre que les personnes hébergeant des données de santé à caractère personnel pour le compte de tiers (personnes physiques ou morales) doivent être titulaires d'un certificat de conformité délivré par un organisme accrédité.

Cette certification porte des exigences de sécurité et de respect de la vie privée que les hébergeurs doivent respecter afin de bénéficier du fameux sésame.

A QU'EST-CE QUE L'HDS ?

1 – À l'origine

En plus des dispositions du RGPD concernant la protection des données à caractère personnel (y compris les données sensibles à l'instar des données de santé), la loi n° 2016-41 du 26 janvier 2016 de modernisation du système de santé français prévoyait que « toute personne qui héberge des données de santé à caractère personnel […], pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites

données ou pour le compte du patient lui-même, doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime ».

Cette disposition législative introduisait le recours à un hébergeur agréé. Cet agrément était délivré par le ministère de la Santé, selon les modalités prévues dans le décret nº 2006-6 du 4 janvier 2006, pour une période de trois ans. La décision était rendue après étude du dossier d'auto-évaluation transmis par le candidat, l'ASIP-Santé [7] et la CNIL. Ce dossier se composait de différentes pièces traitant :

- des aspects administratifs et financiers du candidat ;
- des modèles de contrat prévus pour le service d'hébergement ;
- de la présentation fonctionnelle et technique du service d'hébergement ;
- de l'analyse de risques réalisée sur le service d'hébergement ;
- des dispositifs de sécurité mis en œuvre sur la gouvernance, le contrôle d'accès, la gestion des ressources humaines, l'exploitation, la continuité de service, etc.

Au terme des trois ans de validité de l'agrément, une demande de renouvellement devait être effectuée par le candidat dans laquelle étaient présentées les modifications intervenues dans le dossier lors de la délivrance de l'agrément (évolution des clauses contractuelles, du service, du système d'information, etc.).

2 – Les évolutions apportées par l'ordonnance n° 2017-27 du 13 janvier 2017

L'ordonnance nº 2017-27 du 13 janvier 2017 modifie les modalités d'obtention du titre d'hébergeur de données de santé. En effet les modalités **basculent d'un modèle d'agrément tel que décrit précédemment à un modèle de certification**. Elle est précisée par le décret nº 2018-137 du 26

7 Agence des Systèmes d'Information Partagés de Santé

février 2018 qui précise le champ des activités d'hébergement de données de santé à caractère personnel ainsi que les conditions d'obtention du certificat de conformité et les clauses minimales que doit comporter le contrat d'hébergement. Accompagnant ce changement, l'arrêté du 11 juin 2018 paru au Journal officiel du 29 juin 2018 entérine les référentiels de certification et d'accréditation relatif à l'hébergement de données de santé.

Cette publication permet dans un premier temps aux organismes de certification de se lancer dans le processus d'accréditation auprès du Comité français d'accréditation (COFRAC). Dans un second temps et une fois les premières accréditations délivrées, cela permet aux candidats de se rapprocher des organismes de certification accrédités.

La démarche adoptée participe à apporter de la confiance et de la transparence aux utilisateurs de ces services d'hébergement par la réalisation de contrôles, sur la base du référentiel de certification, par un organisme tiers accrédité par l'autorité nationale compétente.

3 – Mécanismes de transition

L'ASIP-Santé instruit l'ensemble des demandes d'agrément reçues avant le 31 mars 2018. Si l'instruction donne lieu à la délivrance de l'agrément, ce dernier courra sur toute la période de validité de l'agrément soit trois ans. Tout renouvellement d'agrément devra alors basculer sur le mécanisme de certification et imposera aux candidats de se rapprocher d'organismes de certification dûment accrédités.

B À QUI S'ADRESSE-T-IL ?

L'article L. 1111-8 du code de la santé publique prévoit : « Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le

compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article. […] L'hébergeur de données mentionnées au premier alinéa du I sur support numérique est titulaire d'un certificat de conformité […]. ».

L'article R. 1111-9 du code de la santé publique définit l'activité d'hébergement de données de santé le fait d'assurer pour le compte du responsable de traitement […] tout ou partie des activités suivantes :

- la mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;
- la mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;
- la mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;
- la mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;
- l'administration et l'exploitation du système d'information contenant les données de santé ;
- la sauvegarde des données de santé.

Par exemple, sont considérés comme hébergeurs de données de santé :

- les départements (ou conseils départementaux) hébergeant les données de santé des MDPH ;
- les communes hébergeant les données de santé des CCAS

C QUE CONTIENT-IL ?

Le référentiel de certification [REF_HDS] sur lequel la conformité des candidats sera évaluée par des organismes de certification, s'appuie sur une démarche d'amélioration continue organisée autour de la gestion de

risques. À ce titre, tout candidat souhaitant obtenir la certification HDS doit disposer d'un système de management de la sécurité de l'information (SMSI) certifié selon la norme ISO/CEI 27001:2013.

En plus des exigences de la norme ISO/CEI 27001:2013, le référentiel de certification impose aux candidats un certain nombre d'exigences issues de l'ISO/CEI 20000 – 1:2012, norme sur les systèmes de management des services informatiques :

- spécificités liées à la protection de données de santé à caractère personnel ;
- spécificités liées au domaine de la santé.

POUR PLUS D'INFORMATION :

Fiche n°1 : Aide à la mise en œuvre des réglementations – *page 56*
Fiche n°2 : Se préparer et réagir en cas d'incident de sécurité – *page 62*
Fiche n°6 : Recourir à l'externalisation pour la gestion du système d'information – *page 93*
Fiche n°7 : Mise en œuvre d'un système de management de la sécurité de l'information (SMSI) dans le contexte HDS – *page 105*

Liste des hébergeurs de données de santé agréés : esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees
Liste des hébergeurs de données de santé certifiés : esante.gouv.fr/services/liste-des-hebergeurs-certifies-hebergeur-de-donnees-de-sante-a-caractere-personnel

Autorité de contrôle : ASIP-Santé

CHAPITRE III

Transformation numérique de l'État

I/ Le service de coffre-fort numérique

Dans le cadre de la dématérialisation des démarches administratives, les collectivités territoriales vont être amenées à gérer électroniquement les échanges d'information avec le citoyen. Les solutions de messagerie électronique montrant rapidement leur limite lorsque les informations échangées sont sensibles (données à caractère personnel, données financières, etc.), un cadre règlementaire a été défini pour cadrer la mise en œuvre de services de coffre-fort numérique.

Ce service, introduit par l'article 87 de la loi pour une République numérique (LRN), précise les exigences fonctionnelles que ce dernier doit satisfaire. Ainsi le service de coffre-fort numérique doit :

- garantir l'intégrité des données ou documents électroniques durant tout leur cycle de vie au sein du service ;
- tracer les opérations effectuées sur le service (maintien en condition opérationnelle et de sécurité) ou sur les données et documents électroniques eux-mêmes ;
- garantir la confidentialité des données en autorisant l'accès au coffre-fort numérique aux seuls utilisateurs ou tiers explicitement autorisés par l'utilisateur principal (le cas échéant le prestataire de service de coffre-fort numérique) ;
- garantir la portabilité des données notamment par leur restitution dans des standards ouverts aisément réutilisables et exploitables par un système d'information.

Le décret n° 2018-418 relatif aux modalités de mise en œuvre du service de coffre-fort numérique vient préciser les déclinaisons techniques minimales de ces exigences fonctionnelles.

La loi prévoit également un mécanisme de certification par l'État (non obligatoire) permettant d'accroître la fiabilité du service et de renforcer la confiance des utilisateurs vis-à-vis de celui-ci. Cette certification est établie selon un cahier des charges proposé par l'ANSSI après avis de la CNIL.

II/ L'envoi recommandé électronique et la lettre recommandée électronique

Dans le cadre de certaines démarches administratives, les collectivités territoriales peuvent recourir à la lettre recommandée.

L'article 93 de la LRN introduit l'envoi recommandé électronique à l'article L. 100 du Code des postes et des communications électroniques (CPCE) et prévoit que ce dernier est équivalent à l'envoi par lettre recommandée s'il respecte certaines conditions.

L'envoi recommandé électronique est l'un des services couverts par le règlement eIDAS. L'article 43 du règlement prévoit que les données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique qualifié bénéficient d'une présomption quant à leur intégrité, à leur envoi par un expéditeur identifié, à leur réception par un destinataire identifié ainsi qu'à l'exactitude de la date et de l'heure de leur envoi et de leur réception.

L'article 44 du règlement vient quant à lui préciser les exigences applicables aux services qualifiés d'envoi recommandé électronique. Le recours à un service qualifié d'envoi recommandé électronique permet d'assurer le respect de ces exigences par le prestataire concerné et de bénéficier de la présomption prévue par l'article 43 du règlement.

L'article L. 100 du CPCE prévoit que seul un service d'envoi recommandé électronique respectant les exigences de l'article 44 du règlement eIDAS (donc qualifié) bénéficie de l'équivalence avec la lettre recommandée.

De plus, le décret n° 2018-347 relatif à la lettre recommandée électronique fixe les modalités d'application de l'article L. 100 et précise en particulier les exigences requises quant à l'identification de l'expéditeur et du destinataire, à la preuve du dépôt électronique de l'envoi et à la preuve de la réception électronique de l'envoi [ces exigences sont identiques à celles prévues par l'ANSSI pour la qualification d'un service d'envoi recommandé électronique].

La liste des prestataires d'envoi recommandé électronique est éditée et maintenue à jour par l'ANSSI qui est l'organe de contrôle pour la France [LIST_CONF].

III / L'archivage électronique

A GÉNÉRALITÉS

Dans le cadre de leurs activités, les collectivités territoriales sont amenées à manipuler des documents administratifs qui peuvent contenir des informations publiques*. L'archivage de tels documents demande la clarification de la notion même d'archivage. En effet on distingue différents types d'archivages, chacun dépendant d'une phase particulière du cycle de vie de l'information, comme le montre le schéma ci-dessous.

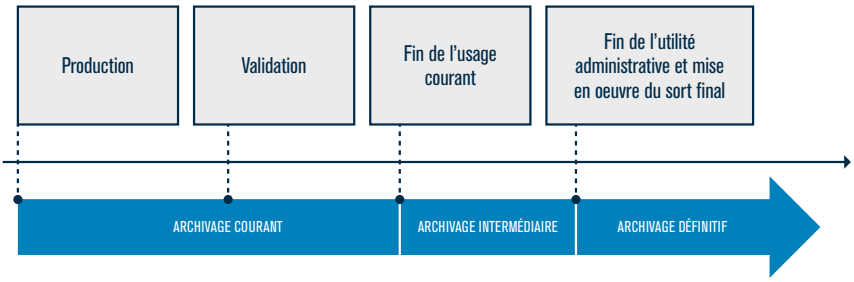


Figure 2 : Différents types d'archivages – source : référentiel général de gestion des archives (RGGA)

Les collectivités territoriales sont soumises à un certain nombre d'exigences en matière de conservation et plus particulièrement sur les durées de conservation qui sont spécifiées dans l'instruction DAF/DPCACI/RES/2009/018[INSTR_2009_018].

B MUTUALISATION

L'externalisation est également rendue possible par le code du patrimoine pour tout producteur d'archives publiques qui souhaiterait confier la conservation de ses archives courantes et intermédiaires, sur support papier ou numérique, à un prestataire.

Ce prestataire doit préalablement avoir obtenu l'agrément du ministère de la Culture (art. L212-4) suite à l'instruction des demandes par le service interministériel des Archives de France qui tient à jour la liste des prestataires agréés [PREST_ARCHIVAGE].

C EXTERNALISATION

Dans un objectif de rationalisation des coûts liés à l'archivage, le code du patrimoine autorise les collectivités territoriales et leurs groupements à confier la conservation de leurs archives à d'autres collectivités. Ainsi :

- une région peut confier, par convention, la conservation de ses archives aux Archives départementales du chef-lieu de région (art. L. 212-6) ;
- un groupement de communes peut confier, par convention, la conservation de ses archives au service d'archives de l'une des communes membres du groupement ou les déposer au service départemental d'archives compétent (art. L. 212-6-1) ;

Une commune de plus de deux mille habitants peut confier, par convention, et après délibération du conseil municipal, la conservation de ses archives anciennes, telles que définies à l'article L. 212-11, aux archives du groupement de communes dont elle est membre ou les déposer au service département d'archives compétent (art. L. 212-12).

POUR PLUS D'INFORMATION :

Liste des prestataires qualifiés d'envoi recommandé électronique : www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/liste-nationale-de-confiance/
www.ssi.gouv.fr/liste-produits-et-services-qualifies/

Fiche n°6 : Recourir à l'externalisation pour la gestion du système d'information – *page 93*

CHAPITRE IV

Renforcer la sécurité des acteurs critiques (OIV, OSE)

I/ Les dispositions ordinaires de la loi de programmation militaire 2014-2019 (LPM)

EN BREF :

La LPM, en modifiant le code de la défense, s'adresse aux opérateurs d'importance vitale (OIV)*. Les collectivités territoriales concernées par ce dispositif sont celles qui se sont vues désignées par arrêté.

Ces OIV sont désignés parmi les organisations qui, si elles venaient à subir un incident grave, pourraient porter gravement atteinte au potentiel de guerre ou économique, à la sécurité ou à la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

A QU'EST-CE QUE LA LPM ?

La loi n° 2013-1168 du 18 décembre 2013 portant diverses dispositions concernant la défense et la sécurité nationale est une loi inscrite dans la stratégie de défense et de sécurité nationale. Elle découle du Livre blanc sur la défense et de sécurité nationale, qui, par le biais d'une analyse des risques stratégiques, donne des orientations en matière de défense et de sécurité nationale. Ses dispositions sont codifiées dans le code de la défense.

1 – Quel apport pour la sécurité numérique ?

La LPM 2014-2019 innove par la prise en compte des risques stratégiques liés à la sécurité numérique. Cette prise en compte se traduit par

l'obligation pour les OIV de protéger leurs systèmes d'information d'importance vitale (SIIV) concourant aux activités d'importance vitale codifié aux articles L. 1332-6-1 et suivants du code de la défense.

2 – Le dispositif sécurité des activités d'importance vitale (SAIV)

Le dispositif SAIV [PLAQ_SAIV] doit assurer la protection des activités d'importance vitale* contre les actes de malveillance (terrorisme, sabotage, etc.). Pour atteindre cet objectif, il se concentre sur les OIV répartis au sein de douze secteurs d'activité [8] tels que les transports, l'énergie ou encore les industries de défense. Le législateur a introduit dans ce dispositif, à l'origine essentiellement orienté sur la sécurité physique et des personnes, un volet sécurité numérique.

B À QUI S'ADRESSE-T-ELLE ?

Les articles L. 1332-6-1 et suivants, ainsi que leurs mesures d'application concernent :

- les OIV ;
- les prestataires pour les besoins de sécurité des systèmes d'information introduits par le décret n° 2015-350 du 27 mars 2015.

1 – Les OIV

Comme le rappelle l'article R. 1332-4 du code de la défense : « les opérateurs d'importance vitale sont désignés pour chaque secteur d'activité d'importance vitale par arrêté du ministre coordonnateur ». Cette désignation par arrêté d'une organisation publique ou privée n'intervient qu'après des discussions entre l'OIV pressenti et le ministre coordonnateur.

---

8 Cf. section 1.2 de l'Instruction Générale Interministérielle 6600 du 7 janvier 2014

2 – Les prestataires pour les besoins de sécurité des systèmes d'information

Le fait, pour une organisation privée ou publique, de devenir un prestataire pour les besoins de sécurité des systèmes d'information se fait sur la base du volontariat. L'entreprise qui décide de s'inscrire dans cette démarche va alors suivre le processus de qualification définit dans le décret nº 2015-350 du 27 mars 2015 (article 8 et suivants).

C QUE CONTIENT-ELLE ?

Concernant la sécurité numérique, les articles L. 1332-1 à L. 1332-6 du code de la défense, imposent aux OIV la mise en œuvre de certaines mesures de sécurité précisées par arrêté du Premier ministre sur les SIIV. D'autres référentiels résultent par ailleurs de cette loi :

- le décret nº 2015-350 ;
- le décret nº 2015-351 ;
- un ensemble d'arrêtés sectoriels.

1 – Le décret n° 2015-350

Le décret nº 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information [9] précise les modalités et autorités chargées de qualifier les produits et services introduits par la LPM, à savoir :

- les prestataires pour les besoins de la sécurité des systèmes d'information:
  - les prestataires de détection d'incidents de sécurité (PDIS) ;
  - les prestataires de réponse aux incidents de sécurité (PRIS) ;
  - les prestataires d'audit de sécurité des systèmes d'information (PASSI LPM).
- les produits de sécurité (sondes, etc.).

9 www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405903

2 – Le décret n° 2015-351

Le décret nº 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale [10] précise les mesures de sécurité que les OIV sont tenus de mettre en place sur leurs SIIV et appelle des mesures complémentaires spécifiées par arrêté du Premier ministre. Ces mesures incluent :

- la cartographie des SIIV : l'opérateur est chargé de tenir à jour une liste des SIIV qu'il transmet à l'ANSSI et qui peut faire l'objet d'arbitrages sur sa pertinence ;
- les modalités de détection des événements de sécurité ;
- les modalités de qualification des systèmes de détection ou des prestataires exploitant des systèmes de détection ;
- les modalités de déclaration des incidents de sécurité ;
- les modalités de contrôles de sécurité (audits).

3 – Les arrêtés sectoriels

Parus à partir d'août 2016, les arrêtés sectoriels précisent les mesures de sécurité prévues dans le décret nº 2015-351 que les OIV sont dans l'obligation d'appliquer sur les SIIV préalablement déclarés auprès de l'ANSSI.

Chaque arrêté, dans sa construction, s'appuie sur le modèle suivant :

- le corps de l'arrêté prévoit l'inventaire et la déclaration des SIIV auprès de l'ANSSI et la déclaration des incidents de sécurité ;
- l'annexe I [11] présente les vingt mesures de sécurité que sont tenus de mettre en œuvre les OIV sur leurs SIIV, détaillées de la manière suivante :

Règle 1 : définition et mise en œuvre d'une PSSI pour le SIIV (pour cela, on peut se référer au [GUIDE_PSSI])	**Règle 11** : mise en œuvre de dispositif d'identification des utilisateurs du SIIV

10 www.legifrance.gouv.fr/eli/decret/2015/3/27/PRMD1502905D/jo/texte/fr
11 Pour certains secteurs, cette annexe n'est pas publique. Au moment de la désignation en tant qu'OIV par le SGDSN, ce dernier joint l'annexe I à la lettre de notification.

Règle 2 : application d'une démarche d'homologation	**Règle 12** : mise en œuvre de dispositif d'authentification des utilisateurs du SIIV
Règle 3 : élaboration et tenue à jour d'une cartographie physique et logique des SIIV	**Règle 13** : définition et application de processus de gestion des droits d'accès au SIIV
Règle 4 : mise en œuvre d'un processus de maintien en condition de sécurité des SIIV	**Règle 14** : définition et application de processus de gestion des comptes d'administration du SIIV
Règle 5 : mise en œuvre d'un système de journalisation des événements de sécurité des SIIV	**Règle 15** : gestion du système d'information d'administration SIIV
Règle 6 : analyse et corrélation des événements de sécurité remontés des SIIV	**Règle 16** : conception et mise en œuvre de dispositif de cloisonnement du SIIV vis-à-vis des autres composants du système d'information de l'OIV
Règle 7 : mise en œuvre de système de détection (sondes) d'événements de sécurité	**Règle 17** : conception et application de mécanismes de filtrage sur le SIIV pour éviter la circulation de flux inutiles
Règle 8 : définition et application d'une organisation pour le traitement des incidents affectant le SIIV	**Règle 18** : définition et mise en œuvre de mécanismes de sécurité dans les accès à distance au SIIV par l'OIV ou son (ses) prestataire(s)
Règle 9 : définition et application d'une organisation pour le traitement des alertes transmises par l'ANSSI	**Règle 19** : définition et mise en œuvre d'une politique de durcissement* des systèmes composant le SIIV
Règle 10 : définition et application de procédure de gestion de crise	**Règle 20** : mise en place, production, suivi et communication à l'ANSSI d'indicateurs de sécurité

- l'annexe II [12] précise les délais de mise en œuvre des règles de sécurité listées ci-dessus ;
- l'annexe III [13] donne les types de systèmes d'information pouvant être considérés comme d'importance vitale et sur laquelle se repose l'OIV pour réaliser son analyse d'impact qui doit donner lieu à la déclaration d'un système d'information comme SIIV ;
- l'annexe IV [14] décrit les typologies d'incidents de sécurité qui doivent faire l'objet d'une déclaration auprès de l'ANSSI.

---

12 Cette annexe n'est pas publique. Au moment de la désignation en tant qu'OIV par le SGDSN, ce dernier joint l'annexe II à la lettre de notification.
13 Cette annexe n'est pas publique. Au moment de la désignation en tant qu'OIV par le SGDSN, ce dernier joint l'annexe III à la lettre de notification.
14 Cette annexe n'est pas publique. Au moment de la désignation en tant qu'OIV par le SGDSN, ce dernier joint l'annexe IV à la lettre de notification.

POUR PLUS D'INFORMATION :

Liste des prestataires LPM :

- PDIS : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/
- PRIS : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/
- PASSI LPM : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/

Fiche n°1 : Aide à la mise en œuvre des réglementations – *page 56*
Fiche n°2 : Se préparer et réagir en cas d'incident de sécurité – *page 62*
Fiche n°6 : Recourir à l'externalisation pour la gestion du système d'information – *page 93*

Autorité compétente : Agence nationale de la sécurité des systèmes d'information (ANSSI)

II / La directive européenne *Network and Information Systems* (NIS)

EN BREF :

La directive NIS est un texte européen transposé en droit français qui s'adresse aux collectivités territoriales qui se sont vues désignées comme opérateur de services essentiels (OSE) par arrêté du Premier ministre.

Les OSE sont désignés parmi les organisations qui supportent des services dits essentiels au fonctionnement de la société ou de l'économie (alimentation, sanitaire, etc.) et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services.

A QU'EST-CE QUE LA DIRECTIVE NIS ?

Le Parlement européen et le Conseil de l'Union européenne (CUE) ont adopté le 6 juillet 2016 la directive UE nº 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne. Contrairement aux règlements européens (comme par exemple le RGPD) qui sont directement applicables, les directives font l'objet d'une transposition dans les différents États membres.

Cette transposition a été faite par :

- la loi nº 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité [15] ;

15 www.legifrance.gouv.fr/eli/loi/2018/2/26/INTX1728622L/jo/texte

- le décret nº 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de services numériques qui précise les modalités d'application de ladite loi.

La directive NIS développe 4 axes principaux :

- la gouvernance : cet axe est développé par le renforcement des capacités nationales en matière de sécurité numérique des États membres par :
  - le développement d'une doctrine en matière de sécurité numérique (illustrée en France par la stratégie nationale pour la sécurité du numérique [16] du 16 octobre 2015) ;
  - l'institution d'une autorité nationale en matière de sécurité numérique (par exemple l'ANSSI pour la France) ;
  - un centre de réponse aux incidents, fonction assurée par le CERT-FR pour la France, impliqué dans les échanges opérationnels avec les *computer security information response team* (CSIRT)* nationaux des différents États membres existants ;
- la coopération : la mise en place d'un réseau de coopération entre les différents États membres portant notamment sur les aspects politiques et opérationnels en matière de sécurité numérique pour :
  - soutenir et faciliter la coopération stratégique entre les États membres ;
  - faciliter l'échange d'informations et renforcer la confiance mutuelle ;
  - élever le niveau global de maturité et les capacités nationales en matière de sécurité numérique.
- la sécurité numérique des opérateurs de services essentiels (OSE) : la France s'est dotée d'un cadre légal lui permettant de réguler la sécurité des systèmes d'information des acteurs essentiels à la vie économique et sociétale des États membres ;
- la sécurité numérique des fournisseurs de service numérique (FSN) : la France s'est également dotée d'un cadre légal permettant de réguler la sécurité des systèmes d'information des FSN.

16 www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques

B À QUI S'ADRESSE-T-ELLE ?

1 – Les OSE

Tous les « opérateurs publics ou privés qui se sont vus notifiés comme OSE, et rentrant dans les catégories [ci-dessous], par arrêté du Premier ministre » [17] sont concernés par cette directive.

SECTEUR	SOUS-SECTEUR
Énergie	Électricité
	Pétrole
	Gaz
Transport	Aérien
	Ferroviaire
	Guidé
	Par voie d'eau
	Routier
Logistique	N/A
Banques	
Infrastructures de marchés financiers	
Services financiers	
Assurance	
Social	
Emploi et formation professionnelle	
Santé	Établissements de soins de santé
	Produits pharmaceutiques
Fourniture et distribution d'eau po-table	N/A
Traitement des eaux non potables	
Infrastructures numériques	
Éducation	
Restauration	

17 Décret 2018-384 – article 3

2 – Les FSN

La directive NIS s'applique de plus à l'ensemble des FSN dont :

- la masse salariale excède 50 salariés ;
- le chiffre d'affaire annuel excède 10 millions d'euros ;
- le siège social ou l'établissement principal est établi sur le territoire national ou un représentant a été désigné sur le territoire national ;
- l'activité (à destination des particuliers, des professionnels ou des administrations) est comprise dans une des catégories suivantes :
  - **les places de marché en ligne**, qui permettent à des consommateurs ou à des professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels, soit sur le site Internet de la place de marché en ligne, soit sur le site Internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ;
  - **les moteurs de recherche en ligne** ;
  - **les services d'informatique en nuage** (ou *cloud*), qui permettent l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées.

C QUE CONTIENT-ELLE ?

1 – Concernant les OSE

Les exigences applicables aux OSE sont décrites dans le décret n° 2018-384 du 23 mai 2018 et enrichies de règles définies par arrêté. Ainsi nous retrouvons :

- le mode opératoire de (fin de) désignation des OSE ;
- l'identification et la communication d'un représentant de l'OSE auprès de l'ANSSI ;
- l'établissement, la communication auprès de l'ANSSI et la tenue à jour d'un inventaire des systèmes d'information nécessaires à la fourniture

des services essentiels, y compris ceux dont l'exploitation est confiée à un tiers ;

- les règles de sécurité précisées par l'**arrêté du 14 septembre 2018** :

Règle 1 : l'OSE identifie les systèmes d'information essentiels (SIE), réalise et tient à jour une analyse de risques sur ces systèmes.	**Règle 13** : l'OSE met en œuvre, dans la mesure du possible, des dispositifs d'identification individuels pour tous les utilisateurs des SIE.
Règle 2 : l'OSE élabore, tient à jour et met en œuvre une politique de sécurité des systèmes d'information (PSSI) (pour cela, on peut se référer au [GUIDE_PSSI]).	**Règle 14** : l'OSE met en œuvre des moyens de protection des informations d'authentification aux SIE.
Règle 3 : l'OSE procède à l'homologation de sécurité de chacun de ses SIE.	**Règle 15** : l'OSE prend des mesures de restriction d'accès aux ressources de chacun de ses SIE.
Règle 4 : l'OSE évalue et tient à jour, pour chacun de ses SIE, des indicateurs.	**Règle 16** : l'OSE élabore et met en œuvre des procédures de maintien en condition de sécurité de chacun de ses SIE.
Règle 5 : l'OSE réalise, à intervalles réguliers, des audits de sécurité de chacun de ses SIE.	**Règle 17** : l'OSE élabore et met en œuvre des mesures de protection physique de chacun de ses SIE.
Règle 6 : l'OSE élabore et tient à jour une cartographie de chacun de ses SIE.	**Règle 18** : l'OSE élabore, met en œuvre et tient à jour des mesures de détection d'incidents de sécurité de chacun de ses SIE.
Règle 7 : l'OSE prend des dispositions lors de la configuration de chacun des SIE initiale et tout au long du cycle de vie de l'information.	**Règle 19** : l'OSE met en œuvre des dispositifs de journalisation des événements sur chacun de ses SIE.
Règle 8 : l'OSE s'assure du cloisonnement de chacun ses SIE.	**Règle 20** : l'OSE met en œuvre des mécanismes de corrélation et d'analyse des événements journalisés sur chacun de ses SIE.
Règle 9 : l'OSE protège les accès distants à chacun de ses SIE effectués à travers des SI tiers.	**Règle 21** : l'OSE élabore, met en œuvre et tient à jour des mécanismes de réponse aux incidents de sécurité affectant chacun de ses SIE.
Règle 10 : l'OSE met en place des mécanismes de filtrage des flux de données depuis ou à destination de chacun de ses SIE.	**Règle 22** : l'OSE met en place un service de traitement des alertes transmises par l'ANSSI.
Règle 11 : l'OSE met en place des mesures de protection des comptes d'administration de chacun de ses SIE	**Règle 23** : l'OSE élabore, met en œuvre et tient à jour des mesures de gestion de crise en cas d'incident de sécurité affectant l'un de ses SIE.
Règle 12 : l'OSE met en œuvre des mesures de protection des SI d'administration de chacun de ses SIE	

- la déclaration et la communication du suivi des incidents à l'ANSSI ;
- les contrôles de sécurité.

2 – Concernant les FSN

La loi n° 2018-133 du 26 février 2018 prévoit également des dispositions particulières pour les FSN précisées dans le décret n° 2018-384 du 23 mai 2018 ainsi que dans le règlement d'exécution (UE) n° 2018/151 [18] et synthétisées comme suit :

- la désignation auprès de l'ANSSI d'un représentant du FSN sur le territoire national ;
- l'établissement, la communication et la tenue à jour d'un inventaire des systèmes d'information nécessaires à la fourniture des services, y compris ceux dont l'exploitation est confiée à un tiers ;
- les règles de sécurité à appliquer qui s'articulent autour des trois grands principes suivants :
  - la cartographie et l'analyse de risques pesant sur les systèmes d'information assurant les services numériques rendus par le fournisseur ;
  - la mise en œuvre de mesures de sécurité techniques et organisationnelles décidées à l'issue de l'analyse de risques ;
  - la gestion des incidents de sécurité affectant les systèmes d'information assurant les services numériques rendus par le fournisseur avec, en fonction de la gravité de l'incident, une obligation de déclaration à l'ANSSI.
- les audits et contrôles.

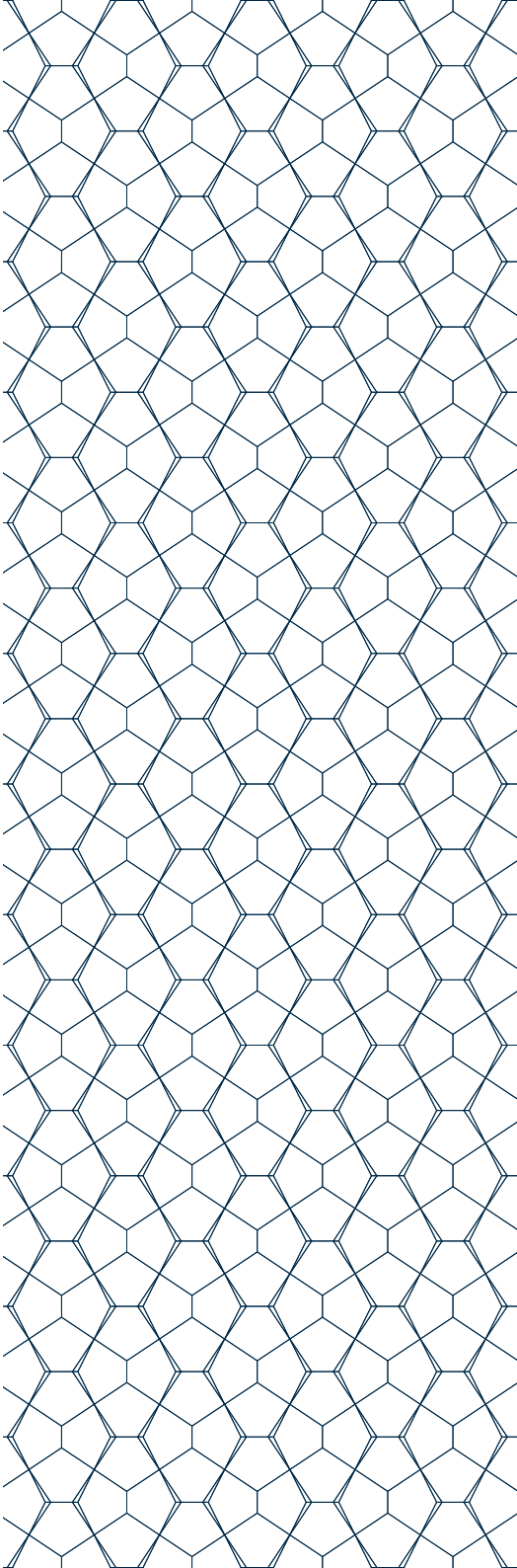
18 eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R0151&from=FR

POUR PLUS D'INFORMATION :

Fiche n°1 : Aide à la mise en œuvre des réglementations – *page 56*
Fiche n°2 : Se préparer et réagir en cas d'incident de sécurité – *page 62*
Fiche n°6 : Recourir à l'externalisation pour la gestion du système d'information – *page 93*

Autorité compétente : Agence nationale de la sécurité des systèmes d'information (ANSSI)

PARTIE II : RECOM-MANDATIONS



FICHE N°1

Aide à la mise en œuvre des réglementations

Les réglementations présentées dans la partie I comportent un ensemble d'exigences qui nécessitent une assistance dans leur mise en œuvre. Cette fiche a vocation à lister l'ensemble des moyens (produits, prestataires, autorités) qui pourront aider les collectivités territoriales à se mettre en conformité.

I / Mise en œuvre du RGS

Afin de mettre en œuvre le RGS, il est possible d'avoir recours à des prestataires de services de confiance ou des produits dits « qualifiés ».

La qualification est la recommandation par l'État français de produits ou services approuvés par l'ANSSI :

- à travers le processus de qualification des prestataires de service, l'ANSSI s'assure qu'un service est rendu en toute confiance, par des sociétés et des intervenants compétents dans leur domaine ;
- à travers le processus de qualification des produits, l'ANSSI s'assure que les produits atteignent un certain niveau de sécurité et de confiance.

La qualification atteste de la conformité du produit ou du prestataire de service aux exigences règlementaires, techniques et de sécurité fixées par l'ANSSI.

En fonction des besoins, différentes catégories de prestataires de services de confiance qualifiés [PSCO] existent :

- les **prestataires de services de certification électronique (PSCE)** : ces prestataires proposent des services conformes aux règles du RGS pour l'authentification (personne ou serveur), la signature électronique*, le cachet électronique* et la confidentialité (ou chiffrement). Ils sont généralement qualifiés pour une durée de deux ans renouvelables, le processus de qualification s'assurant que les services qu'ils fournissent sont conformes aux règles du RGS pour un niveau de sécurité choisi (*, **, ou ***) ;

- les **prestataires de services d'horodatage électronique (PSHE)** : ces prestataires proposent des services conformes aux règles du RGS pour l'horodatage électronique. Ils sont généralement qualifiés pour une durée de deux ans et leur qualification est renouvelable, le processus de qualification s'assurant que les services qu'ils fournissent sont conformes aux règles du RGS ;
- les **prestataires d'audit de la sécurité des systèmes d'information (PASSI)** : la qualification PASSI a pour but de garantir la qualité des audits de sécurité. Ils sont généralement qualifiés pour une durée de trois ans renouvelables. Pour le commanditaire, il est donc recommandé de demander une prestation qualifiée lors du recours à un PASSI.

ATTENTION :

Au sens du RGS, une prestation qualifiée est une activité d'audit (audit organisationnel et physique, de code source, de configuration ou test d'intrusion) réalisée par un ou plusieurs auditeurs reconnus compétents pour cette activité et travaillant pour un prestataire d'audit qualifié pour cette même activité. De plus, une prestation d'audit qualifiée prévoit la fourniture au commanditaire de l'audit de recommandations destinées à élever le niveau de sécurité du système d'information de l'audité. (RGS – Annexe C)

De même pour les produits de sécurité, l'ANSSI tient à jour sur son site les informations relatives aux produits qualifiés / certifiés [LIST_PROD]. Ces produits sont catégorisés selon le niveau de garantie (du plus faible au plus élevé). Nous retrouvons ainsi :

- l'évaluation de produits au niveau **élémentaire** qui s'appuie sur la certification de sécurité de premier niveau (CSPN) ;
- l'évaluation de produits au niveau **standard** qui s'appuie sur les *common criteria* (CC). Le produit doit alors atteindre le niveau d'assurance (EAL [19]) 3 augmenté des paquets d'assurance prévus par la qualification (« EAL 3+ ») ;
- L'évaluation de produits au niveau **renforcé** qui s'appuie également sur les *common criteria* (CC). Le produit doit alors atteindre le niveau (EAL) 4 augmenté des paquets d'assurance prévus par la qualification (« EAL 4+ »).

II / Mise en œuvre du règlement eIDAS

Dans le cadre de l'application du règlement, l'ANSSI a été désignée en tant qu'organe de contrôle pour le volet « services de confiance », dont les missions sont définies à l'article 17 du règlement eIDAS, auprès de la Commission européenne. De plus, l'ANSSI est garante de la sécurité des moyens d'identification électronique dont les schémas ont été notifiés à la Commission européenne.

Comme le prévoit le règlement, chaque État membre doit disposer et publier une liste de confiance [LIST_CONF] comprenant des informations relatives aux prestataires de services de confiance qualifiés par la France et suivant un processus de qualification similaire à celui décrit dans le chapitre relatif au RGS.

---

19 *Evaluation Assurance Level* : permet d'identifier le niveau de fiabilité d'un produit par rapport à un usage donné et des objectifs de sécurité prédéfinis. Les niveaux s'échelonnent de EAL1 à EAL7 et traduisent la fiabilité croissante dans le produit évalué.

III / Mise en œuvre du RGPD

Le DPO a pour mission d'accompagner la collectivité territoriale dont il dépend dans sa mise en conformité au RGPD. Ce rôle, au sein de différents organismes, peut-être assumé par une même personne.

Dans le cadre du RGPD, la **CNIL est la seule autorité nationale compétente en matière d'accompagnement, d'établissement des référentiels et de contrôle.** Elle constitue, à ce titre, l'interlocuteur de référence des organisations publiques et privées s'inscrivant dans une démarche de mise en conformité avec le règlement européen. La CNIL fournit à cette fin sur son site, un ensemble documentaire (fiches pratiques, référentiels métiers, cours en ligne, etc.) destiné à faciliter la compréhension du règlement pour mieux s'y conformer [20].

L'ANSSI ne dispose d'aucun rôle formel vis-à-vis de la mise en œuvre du RGPD. Toutefois, les recommandations et outils fournis par l'agence en matière de sécurité numérique, constituent autant de ressources utiles pouvant aider les responsables de traitement dans leur démarche de renforcement de la sécurité des données à caractère personnel.

L'ANSSI met, en ce sens, à disposition du public un « kit de la sécurité des données », composé de nombreux supports et outils pour accompagner les TPE/PME, grandes entreprises, administrations et collectivités dans leur mise en conformité avec le règlement.

IV / Mise en œuvre de HDS

L'investissement financier (coût de la certification, etc.) et les délais d'obtention de la certification HDS peuvent amener les collectivités terri-

---

20 www.cnil.fr/professionnel – rubrique « Ma conformité au RGPD »

toriales à contractualiser avec un hébergeur disposant déjà de l'agrément/certification. L'ASIP-Santé tient à disposition une liste des hébergeurs agréés/certifiés [LIST_HDS].

V / Mise en œuvre de la LPM

La mise en œuvre de certaines règles peut-être sous-traités auprès de prestataires qualifiés [PREST_LPM] au sens du décret nº 2015-350 du 27 mars 2015. Ces prestataires sont :

- prestataires de détection d'incidents de sécurité (PDIS) ;
- prestataires de réponse aux incidents de sécurité (PRIS) ;
- prestataires d'audit de sécurité des systèmes d'information (PASSI LPM).

VI / Mise en œuvre de la directive NIS

Pour les OSE, les audits et contrôles doivent être réalisés par des prestataires d'audit en sécurité des systèmes d'information qualifiés par l'ANSSI. Cette obligation peut, sur décision du Premier ministre, également s'appliquer à certains audits et contrôles menés sur les systèmes d'information des FSN.

FICHE N°2

Se préparer et réagir en cas d'incident de sécurité

De nombreuses études existent sur les incidents de sécurité et révèlent qu'en moyenne, une organisation, quel que soit son secteur d'activité, met environ 196 jours [21] pour détecter un incident de sécurité. Ce constat pousse les autorités nationales ou internationales à élaborer guides et normes pour aider les organisations à mettre en place un processus de gestion des incidents. Ces guides prennent appui sur la méthodologie décrite dans la norme ISO 27035–1:2016, norme internationale sur la gestion des incidents et représentée sur la **Figure 3**.

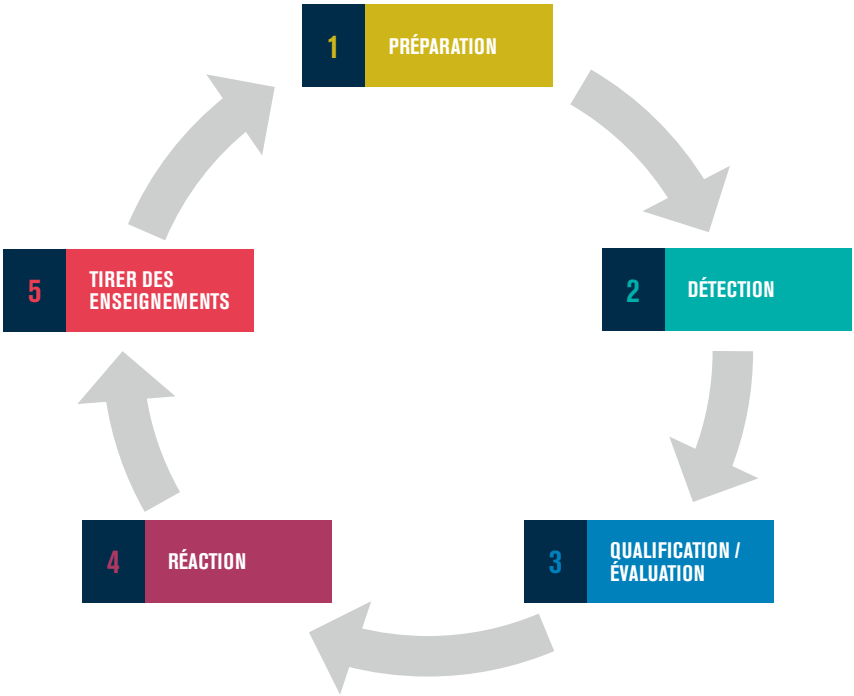


Figure 3 : Cycle de vie de gestion d'un incident de sécurité

21 Ponemon Institute : 2018 Cost of a Data Breach Study

I / La préparation

Cette phase doit être l'occasion pour l'organisation de mettre en place un processus de gestion des incidents. Ce processus s'attache à :

- définir et communiquer ce qui est considéré, au sein de l'organisation, comme un incident de sécurité. L'objectif est de s'assurer que l'ensemble du personnel de l'organisation dispose d'un vocabulaire commun et permet à tout un chacun d'identifier par lui-même un incident de sécurité sans recourir systématiquement au responsable de la sécurité des systèmes d'information (RSSI) ;
- définir une organisation autour de la gestion des incidents qui listera les rôles et responsabilités de chacun dans la gestion des incidents. On trouve, sans être exhaustifs : le RSSI, la direction des systèmes d'information (DSI), la communication, la cellule de crise, le DPO, etc. ;
- définir et tester des fiches réflexes qui, en fonction des types d'incidents (*phishing**, déni de service, rançongiciel, etc.) détaillent les actions à réaliser afin de limiter les conséquences de l'incident en améliorant la réactivité.

II / La détection

Un processus de gestion des incidents de sécurité doit s'appuyer sur des moyens pour détecter lesdits incidents au plus tôt afin de permettre à l'organisation de réagir rapidement et ainsi limiter leurs conséquences (en termes de niveau de propagation comme de ressources à allouer pour le résoudre). La veille, la supervision et la vigilance des utilisateurs figurent parmi les moyens essentiels à ce processus.

A LA VEILLE

La veille permet de se tenir informés de l'état de la menace ainsi

que des vulnérabilités rendues publiques par les éditeurs de solutions. Elle vise à anticiper d'éventuels incidents par l'étude des modes opératoires des attaquants en vue de mettre en œuvre les mesures de sécurité adéquates pour s'en protéger (par exemple assurer le maintien en condition de sécurité du système d'information).

Parmi les sources pertinentes de veille, le [CERT-FR] tient à jour la liste des alertes et avis de sécurité avec pour chacun d'eux des solutions préventives et réactives.

B LA SUPERVISION

Le marché regorge d'outils de supervision qui permettent de suivre en temps réel l'état d'un équipement (poste de travail, serveur, équipement réseaux, etc.) mais également l'état d'un réseau pouvant aller jusqu'à l'analyse du contenu des flux réseaux par une analyse des paquets.

L'ensemble de ces dispositifs s'accompagne généralement d'une capacité de remontée d'alerte en fonction des seuils préalablement définis par l'administrateur de l'outil.

Pour répondre à un besoin identifié, l'ANSSI a mis en place une qualification de prestataires de détection d'incidents de sécurité (PDIS) qui permet d'apporter de la confiance aux utilisateurs dans les services de détection d'incidents de sécurité.

ATTENTION :

Les outils utilisés doivent l'être dans le respect de la réglementation en vigueur (RGPD, code des postes et communications électroniques, etc.).

C LES UTILISATEURS

Les utilisateurs, souvent présentés comme un maillon faible de la sécurité numérique, peuvent être de très bons vecteurs de remontée d'événements de sécurité (outil de travail ralenti, mail suspect, etc.) s'ils ont suivi une sensibilisation sur la notion d'incident de sécurité ainsi que sur les canaux de remontée d'incidents.

De plus, cybermalveillance.gouv.fr [22] publie des contenus de sensibilisation afin de permettre la montée en compétence des utilisateurs en matière de sécurité du numérique.

ATTENTION :

De manière générale, les utilisateurs doivent être régulièrement sensibilisés à la sécurité numérique afin de les responsabiliser et de leur faire prendre connaissance des règles de sécurité qui doivent être observées au sein et en dehors de l'organisation.

III / La qualification / l'évaluation

Cette phase consiste à analyser les événements de sécurité à l'aide de critères préalablement définis et ainsi permettre de les catégoriser en tant qu'incident de sécurité pour pouvoir y réagir. Cela doit permettre de filtrer les événements pour se concentrer uniquement sur ceux représentant un risque élevé pour l'organisation.

22 www.cybermalveillance.gouv.fr/tous-nos-contenus/

IV / La réaction

A LA NOTIFICATION

1 – Les obligations

Les collectivités territoriales sont tenues de déclarer leurs incidents aux autorités (CNIL, ANSSI, etc.), notamment lorsque ces derniers ont un impact élevé. La CNIL a illustré ces obligations dans le schéma ci-dessous.

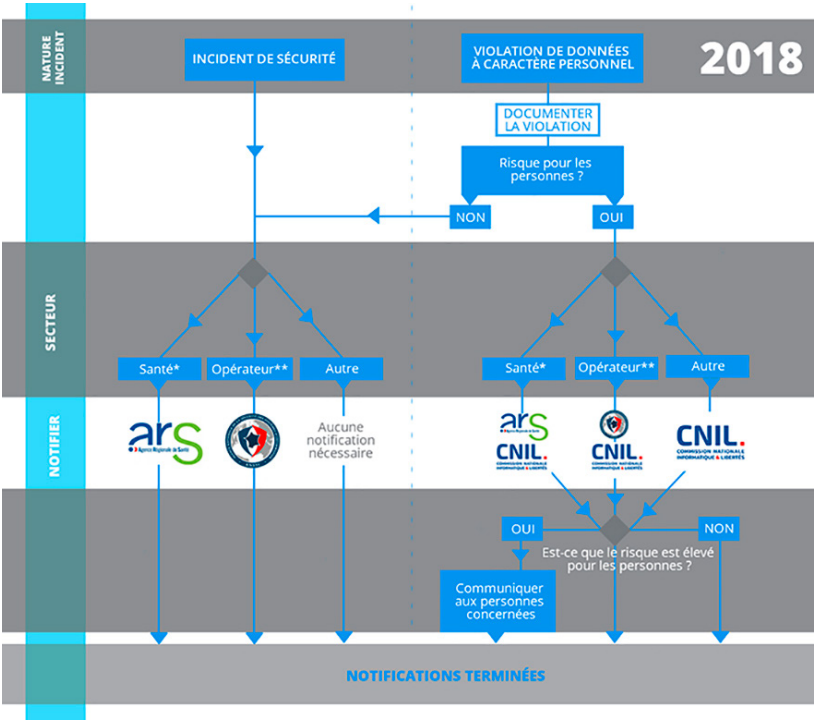


Figure 4 : Schéma de notification des incidents aux autorités compétentes

* Établissements de santé, hôpitaux des armées, laboratoires de biologie médicale et centres de radiothérapie
** OIV, OSE, FSN, prestataires de service de confiance ou opérateurs de communications électroniques

2 – Dispositif national d'assistance aux victimes de cybermalveillance (Cybermalveillance.gouv.fr)

Depuis 2017 [23], l'État a mis en place un groupement d'intérêt public d'assistance aux victimes de cybermalveillance : Cybermalveillance.gouv.fr. Les personnes auxquelles s'adressent Cybermalveillance.gouv.fr sont les particuliers, les entreprises et collectivités territoriales (hors entreprises et collectivités territoriales désignées comme OIV ou OSE).

Les objectifs de la plateforme sont :

- l'assistance aux victimes *via* une aide au diagnostic qui accompagne la victime dans la connaissance de l'acte de cybermalveillance dont elle fait l'objet, pour lui conseiller soit des mesures immédiates de remédiation, soit une orientation vers un autre service d'aide, soit une mise en relation avec des prestataires d'assistance de proximité, en capacité d'assister les victimes de cyberattaques (investigation numérique, récupération de données, etc.) ;
- la prévention et sensibilisation *via* la production et la diffusion de contenus de sensibilisation sur les bonnes pratiques en matière de sécurité numérique [24] ;
- l'observation de la menace numérique par la remontée d'informations, l'analyse et le partage des données statistiques sur le nombre de déclarations ou encore le type d'actes de cybermalveillance afin de mieux l'anticiper.

B LE TRAITEMENT DE L'INCIDENT

Le traitement d'un incident requiert une attention particulière compte-tenu du fait que la victime peut, éventuellement, conserver des éléments en vue d'un dépôt de plainte. Nous allons ici présenter les réflexes à avoir lors de la survenance d'un incident de sécurité :

1. **constater l'infraction** ;
2. **définir la nature de l'incident** : identifier dans quelle catégorie d'infraction l'organisation se situe. Sommes-nous en présence d'une infraction spécifique aux technologies de l'information et de communication ou d'une infraction

23 www.legifrance.gouv.fr/eli/arrete/2017/3/3/PRMD1704935A/jo
24 www.cybermalveillance.gouv.fr/tous-nos-contenus/

commise ou facilitée par l'usage des technologies de l'information et des communications (TIC) ?

3 **agir en première attention** : prendre les mesures nécessaires afin de limiter la propagation ou la gravité de l'incident. Pour cela, et en fonction du type d'incident, vous pouvez être amenés à :
   - mettre en quarantaine les équipements concernés (postes de travail, serveurs, supports amovibles, etc.) ;
   - isoler le réseau afin de mettre un terme à l'incident (par exemple : empêcher les machines infectées de contacter les serveurs de commande et de contrôle*, interrompre un déni de service, etc.).

4 **collecter des enregistrements** pour conserver des preuves :
   - effectuer et protéger les sauvegardes et informations relatives à l'incident (journaux d'événements, images disques des équipements concernés, alertes remontées par les outils de supervision, fichiers incriminés [mails, pièce jointe, etc.], etc.) ;

ATTENTION :

Afin que les enregistrements aient une valeur probante dans le cadre d'une enquête, des précautions doivent être observées quant à l'investigation à mener :

- des copies complètes des équipements doivent être réalisées (copie dite « bit-à-bit ») et dupliquées autant que nécessaire pour effectuer l'investigation ;
- une empreinte de chaque enregistrement conservé doit-être réalisée grâce aux fonctions de hachage* (par exemple SHA-2);
- une main courante doit permettre de retracer toute les manipulations effectuées sur les enregistrements conservés (équivalent à « chain of custody »).

- réaliser des entretiens auprès des personnes internes et/ou externes (prestataires d'infogérance, FAI, etc.) à l'origine de l'alerte ou témoins de l'incident ;

ATTENTION :

Des prestataires spécialisés dans la réponse aux incidents de sécurité peuvent vous accompagnez dans le traitement des incidents de sécurité. Pour cela, l'ANSSI a mis en place une qualification de prestataire de réponse aux incidents de sécurité (PRIS). La plateforme cybermalveillance.gouv.fr dispose également de mécanismes facilitant la mise en relation avec des professionnels pour vous assister.

5 **déposer plainte** : en tant que victime vous disposez d'un délai légal pour déposer plainte. Ce délai dépend du type de situation :
   - 1 an pour les contraventions
   - 3 ans pour les délits
   - 10 ans pour les crimes

   Vous devez vous rendre dans le **service territorial de police ou de gendarmerie** le plus proche du lieu de survenance de l'incident. Ces services disposent de réseaux territoriaux spécialisés en cybercriminalité à l'instar de :

- la sous-direction de lutte contre les cybercriminalités (SDLC) ;
- la brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI), qui concentre ces activités sur Paris et la petite couronne ;
- le centre de lutte contre les criminalités numériques (C3N) du service central du renseignement criminel (SCRC) de la gendarmerie nationale.

Vous pouvez également **adresser un courrier de plainte auprès du procureur de la République du Tribunal de Grande Instance dont vous dépendez.**

ATTENTION :

Dans le cadre du dépôt de plainte et en supplément des documents attestant de l'identité du plaignant ainsi que de la personne morale concernée, vous serez amené à communiquer des éléments intéressant l'enquête, à savoir :

- le descriptif de l'incident ;
- les coordonnées de l'ensemble des personnes impliquées ;
- l'ensemble des éléments techniques qui ont pu être collectés ;
- les documents d'architecture technique du réseau ;
- tout autre élément jugé opportun dans le déroulement de l'enquête.

V / Tirer les enseignements

Après la résolution d'un incident de sécurité, l'organisation doit prendre le temps d'analyser :

- les causes qui ont engendré l'incident ;
- comment l'organisation a réagi.

Les éléments issus de cette analyse doivent permettre à l'organisation d'établir un plan d'actions préventives qui empêche la survenance d'un incident similaire. Le plan d'actions préventives peut prévoir :

- la mise à jour de l'appréciation des risques ;
- la réalisation d'audits ;
- la mise à jour des mesures de sécurité mises en œuvre ;
- etc.

Cette phase doit également être l'occasion pour l'organisation de capitaliser sur les incidents subis et les plans d'action associés et de tenir à jour un journal des incidents.

POUR PLUS D'INFORMATION :

PDIS : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/
PRIS : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/
Outils et démarches de sensibilisation approuvés par Cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr/tous-nos-contenus/

Autorité compétente : Cybermalveillance.gouv.fr

FICHE N°3

L'usage de la signature électronique

Un certain nombre de démarches administratives concernant directement ou indirectement les collectivités territoriales peuvent nécessiter le recours à la signature électronique (par exemple : la dématérialisation des marchés publics, etc.).

I / Qu'est-ce que la signature électronique ?

La signature électronique est l'équivalent de la signature manuscrite (en référence au Code civil), pour un document dématérialisé (fichier texte, tableur, fichier PDF, etc.).

ATTENTION :

Une signature manuscrite ayant fait l'objet d'une numérisation et apposée sur un document électronique n'est pas reconnue comme un procédé de signature électronique.

Au sens du RGS et pour les signatures électroniques avancées ou qualifiées au sens du règlement eIDAS, **la signature électronique s'appuie nécessairement sur l'usage d'un certificat électronique**. Ce certificat électronique est généralement installé sur une **carte à puce** ou un **jeton USB**, nécessitant de fait le matériel (lecteur de carte, etc.) et l'applicatif (les pilotes, les librairies, etc.) nécessaires pour reconnaître et communiquer avec le composant stockant le certificat.

ATTENTION :

Lors de la mise en œuvre de la signature électronique au sein d'une collectivité territoriale, il est indispensable de se rapprocher des gestionnaires du système d'information afin de réaliser une étude d'impact sur la mise en œuvre d'un tel projet.

La signature électronique doit permettre de répondre aux critères de sécurité suivants :

- **l'intégrité** : permettre de détecter la modification d'un document dématérialisé une fois l'acte de signature électronique réalisé ;
- **l'authenticité** : permettre de rattacher un document dématérialisé signé à un seul et unique signataire. La signature électronique doit donc être protégée contre les falsifications ou copies.

II / Cadre juridique de la signature électronique

A CADRE GÉNÉRAL

L'article 1367 du code civil prévoit que « Lorsqu'elle est électronique, [la signature] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État. ».

C'est le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature

électronique qui précise dans son article 1 que « La fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée. Est une signature électronique qualifiée une signature électronique avancée, conforme à l'article 26 du [règlement nº 910/2014 dit eIDAS] et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement. »

B ARTICULATION RGS / EIDAS

L'articulation du règlement eIDAS et du RGS fait naître deux situations particulières.

1 – Les échanges entre autorités administratives

Le RGS s'applique pleinement. En effet, si l'appréciation des risques (rendue obligatoire par le RGS) réalisée prévoit la mise en place d'un procédé de signature électronique, ce dernier doit être conforme au RGS.

2 – Les échanges entre les autorités administratives et les usagers

Concernant les échanges entre les autorités administratives et les usagers, le règlement eIDAS n'impose pas d'exigences particulières autres que la reconnaissance mutuelle des moyens de signatures des autres États membres de l'Union Européenne. Ainsi, la démarche générale prévue par le RGS reste applicable mais, dans le cas où l'appréciation des risques prévoit le recours à un procédé de signature électronique, **la collectivité territoriale sera dans l'obligation d'accepter des moyens de signature électronique qualifiés selon le règlement eIDAS mais potentiellement non conforme au RGS.**

III/ Se procurer un certificat de signature électronique

Un nombre important d'organismes commercialise des solutions de signature électronique. En fonction des usages et des exigences, il peut être imposé le recours à des certificats conformes au RGS ou encore des certificats qualifiés selon le règlement eIDAS.

Lorsque les collectivités territoriales doivent mettre en œuvre un procédé de signature électronique, il leur est recommandé de recourir à un service qualifié à la fois au sens du RGS et du règlement eIDAS.

De la même manière, les prestataires de certification électronique qualifiés sont encouragés à proposer des solutions qui disposent de la double qualification à la fois au titre du RGS et du règlement eIDAS.

A CERTIFICATS QUALIFIÉS SELON LE RÈGLEMENT EIDAS

Le règlement eIDAS introduit quatre niveaux de fiabilité pour la signature électronique. Ces niveaux peuvent être répartis en deux catégories.

1 – La signature électronique à faible niveau de fiabilité

Dans cette catégorie, nous retrouvons la **signature électronique simple** qui doit répondre aux exigences précisées au point 10 de l'article 3 et la **signature électronique avancée** qui doit répondre aux exigences de l'article 26 :

- être lié au signataire de manière univoque ;
- permettre d'identifier le signataire ;
- créer à l'aide de données de création que le signataire peut utiliser sous son contrôle exclusif (ex. : clé privé du certificat) ;
- être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Les exigences énoncées ne sont pas soumises à l'obligation d'audit par un tiers compétent et indépendant, ne donnant que très peu d'assurance quant à la fiabilité des dispositifs mettant en œuvre ces niveaux de signatures.

2 – La signature électronique à haut niveau de fiabilité

Dans cette catégorie, nous retrouvons la **signature électronique avancée basée sur l'usage d'un certificat qualifié** qui reprend les exigences précisées à l'article 26 mais nécessitant l'usage d'un certificat qualifié dans les conditions prévues à l'article 28. La liste comprend également la **signature électronique qualifiée** qui répond à la définition du point 12 de l'article 3.

La fiabilité de ces deux types de signature est notamment apportée par le recours, dans les deux cas, à un **certificat qualifié**, certificat dont les processus de vérification du demandeur et de délivrance répondent à des **exigences de sécurité contraignantes** et qui **font l'objet d'un audit par un organisme d'évaluation de la conformité suivi d'une décision de qualification par l'organe de contrôle** (l'ANSSI pour la France).

Dans le cas de la **signature électronique qualifiée**, qui bénéficie d'une équivalence juridique avec la signature manuscrite, il est obligatoire de recourir en complément à un dispositif de création de signature électronique (*Qualified Signature Creation Device* – [QSCD]), répondant aux exigences de l'annexe II du règlement. Un tel dispositif garantit, avec un haut niveau de confiance, que la signature ne peut être réalisée que par le signataire légitime.

L'ANSSI maintient une liste de confiance répertoriant l'ensemble des prestataires de services de confiance qualifiés au titre du règlement eIDAS [LIST_CONF].

B CERTIFICATS CONFORME AU RGS

L'ordonnance 2005-1516 du 8 décembre 2005, portant notamment sur la création du RGS, introduit la notion de qualification de prestataires de service de certification électronique (PSCE).

Les certificats qualifiés au sens du RGS sont répartis en 3 catégories (1, 2 ou 3 étoile[s] |*, **, ***). Le nombre d'étoiles indiquant le niveau de fiabilité de la signature. La détermination du niveau de fiabilité attendu par le procédé de signature électronique s'appuiera sur une appréciation des risques qui prendra en compte les besoins de sécurité, notamment sur l'intégrité, pour orienter le choix vers un procédé de signature électronique *, ** ou ***.

L'ANSSI est responsable du processus de qualification de ces prestataires et maintient une liste des prestataires qualifiés actualisée [PSCO].

FICHE N°4

Ouvrir un téléservice dans le respect des règles de sécurité

La démarche poussée par le RGS s'appuie sur deux concepts fondamentaux et largement adoptés dans d'autres référentiels internationaux liés à la sécurité des systèmes d'information (par exemple l'ISO/CEI 27001:2013) : l'**approche par les risques** et l'**amélioration continue**. La mise en œuvre de ces deux concepts se traduit, lors de la mise en production d'un nouveau téléservice, par l'application d'une démarche qui prévoit :

- la réalisation d'une analyse de risque ;
- la définition des objectifs de sécurité ;
- le choix et la mise en œuvre des mesures appropriées de protection et de défense du SI ;
- l'homologation de sécurité du système d'information ;
- le suivi opérationnel de sécurité du SI.

Le RGS prévoit également une démarche qui couvre les systèmes d'information en exploitation dans l'optique de sa mise en conformité à ce référentiel qui se déroule comme suit :

- la réalisation d'un audit de la sécurité du système d'information en interne ou externalisé auprès d'un prestataire ;
- la réalisation d'une analyse des risques simplifiée ;
- la mise en œuvre des mesures correctives fixées dans le rapport d'audit ;
- l'homologation de sécurité du système d'information ;
- le suivi opérationnel du SI.

I / L'analyse de risques

L'analyse de risques doit permettre de délimiter le contour du téléservice et, sur ce périmètre, d'identifier l'écosystème dans lequel évolue le système d'information, le contexte de l'autorité administrative (social, sociétal, etc.), les menaces qui pèsent sur l'autorité administrative, d'analyser la vraisemblance et les conséquences, d'évaluer la criticité et

de proposer un traitement des risques. La finalité de cette étape est de permettre, pour les risques insoutenables :

- de proposer un plan d'action visant la mise en œuvre de mesures de sécurité (organisationnelles, techniques ou contractuelles) ;
- d'estimer et de faire accepter les risques résiduels résultant de la mise en œuvre de ce plan d'action.

ATTENTION :

En fonction de la criticité du système d'information à externaliser, l'analyse de risque à mener devra être plus ou moins détaillée.

1. Pour un système peu critique, on pourra se limiter à une analyse d'écart [GUIDE_HYG], à la réglementation applicable (RGS, RGPD, etc.) et à d'éventuels autres guides ou standards pertinents ;
2. Pour un système sensible, on effectuera une analyse de risque macroscopique ;
3. pour un système critique, on effectuera une analyse de risque en respectant la méthode [EBIOS *Risk Manager*].

II / Les objectifs de sécurité

À l'issue de l'analyse de risques, l'autorité administrative définira des objectifs de sécurité qui doivent couvrir, au minimum, les principaux critères de sécurité que sont la disponibilité, l'intégrité et la confidentialité qui peuvent être élargis en fonction du contexte (traçabilité, authenticité).

Les objectifs de sécurité doivent également permettre à l'autorité administrative de mesurer son niveau de maturité en sécurité des systèmes d'information et s'assurer de sa conformité avec la réglementation.

Voici quelques exemples, non exhaustifs, d'objectifs de sécurité :

- définir une PSSI (pour cela, on pourra se référer au [GUIDE_PSSI])
- durcir les systèmes d'exploitation et applications en n'activant que les services/fonctionnalités nécessaires au fonctionnement du système et en désactivant les services/fonctionnalités inutiles ;
- mettre en place des mécanismes d'authentification multi-facteurs* sur les téléservices (*via* l'utilisation de carte à puce [carte agent, etc.], la combinaison d'un mot de passe et d'un code PIN généré aléatoirement par une application mobile, etc.) ;
- mettre en œuvre un système de journalisation des événements (pour cela, on s'attachera à respecter les recommandations et exigences règlementaires mentionnées dans le [GUIDE_JOURNA]) ;
- réaliser des revues régulières des comptes utilisateurs ;
- mettre en place un procédé de signature électronique ;
- etc.

III / La mise en œuvre des mesures de sécurité

À l'issue de l'analyse de risques et en fonction des objectifs de sécurité définis, l'autorité administrative va devoir mettre en œuvre les mesures de sécurité adéquates pour pouvoir atteindre lesdits objectifs. On considère quatre catégories de mesures :

- les mesures qui ont trait à la **gouvernance de la sécurité** : l'application de PSSI, la mise en place d'une organisation et de processus pour gérer la sécurité, etc. ;

- les mesures qui ont trait à la **protection des systèmes d'information** : la mise en œuvre de mesures de sécurité préventives à la survenance d'incidents de sécurité telles que le cloisonnement des réseaux, l'application d'une hygiène informatique, etc. ;
- les mesures qui ont trait à la **défense des systèmes d'information** : la définition, l'application d'un processus de gestion des incidents ainsi que les exercices et tests associés ;
- les mesures qui ont trait à la **résilience des systèmes d'information** : la mise en œuvre de mesures permettant à l'organisation d'atténuer les conséquences de la survenance d'un incident de sécurité. De telles mesures sont liées à la continuité d'activité comme la définition et la mise en œuvre d'un plan de continuité d'activité (PCA), mais également les mesures liées à la sauvegarde des informations et à leur restauration.

Afin de s'assurer qu'aucune thématique liée à la sécurité n'a été omise lors de la mise en œuvre du système d'information, l'utilisation du guide d'hygiène informatique de l'ANSSI [GUIDE_HYG] comme socle de base avec, pour chacune des règles, les justifications de sa non mise en œuvre est fortement recommandée.

Lors de la mise en œuvre de ces mesures de sécurité, le recours à des produits [LIST_PROD_QUAL] et services [PSCO] qualifiés par l'ANSSI est recommandé. Le choix du niveau de garantie est à apprécier en fonction des risques à couvrir (élémentaire, standard, renforcé pour les produits / *, **, *** pour les services de confiance). De plus, l'ANSSI publie régulièrement des référentiels qui vont du recueil de bonnes pratiques élémentaires aux guides techniques [25].

25 www.ssi.gouv.fr/administration/bonnes-pratiques/

ATTENTION :

Dans le cadre d'un téléservice mis en œuvre entre deux autorités administratives, il convient de définir une convention qui définit les rôles et responsabilités de chacune des autorités administratives ainsi que les mesures de sécurités mises en œuvre.

IV / L'homologation de sécurité du système d'information

La démarche d'homologation vise à **faire connaître et comprendre** aux responsables d'une autorité administrative (identifiés comme l'autorité d'homologation) les **risques liés à l'exploitation du téléservice**. Il s'agit d'un processus de responsabilisation aboutissant à la prise de décision par l'autorité d'homologation d'homologuer un système d'information, exigence règlementaire préalable à toute mise en service d'un système d'information soumis au RGS.

La décision d'homologation atteste, au nom de l'autorité administrative, que le système d'information est protégé conformément aux objectifs de sécurité fixés et que les risques liés à la sécurité de l'information sont maîtrisés. Elle est rendue sur la base de l'analyse du dossier d'homologation. Lorsqu'elle concerne un téléservice, **cette décision doit être accessible aux usagers**.

La décision d'homologation est prononcée pour une certaine durée (5 ans maximum dans le cadre du RGS) et doit faire l'objet d'une révision à

l'expiration de cette durée. De même, des impondérables doivent amener l'autorité administrative à revoir son homologation, comme par exemple :

- le changement d'autorité d'homologation ;
- la survenance d'incidents propres à remettre en cause l'homologation prononcée ;
- un changement majeur dans le téléservice ou une succession de modifications mineures (architecture, prestataire, interconnexion, etc.) ;
- etc.

Pour vous accompagner dans la démarche d'homologation, l'ANSSI a publié un guide d'homologation en 9 étapes simples [GUIDE_HOMOL] qui permet de mener à bien cette démarche.

V/ Le suivi opérationnel de la sécurité du système d'information

Le suivi opérationnel se définit par la mise en œuvre de dispositifs de surveillance (par exemple : outils de supervision des systèmes) et de détection (par exemple : sondes, IDS*) afin de pouvoir réagir au plus tôt aux incidents de sécurité.

En plus de ces dispositifs, des audits du système d'information doivent être réalisés à intervalles réguliers (les rapports de ces audits étant notamment des éléments composant le dossier d'homologation). Ces audits doivent couvrir l'ensemble du système d'information tel que décrit dans le référentiel PASSI, à savoir :

- un audit organisationnel et physique ;
- un audit de configuration ;
- un audit d'architecture ;
- des tests d'intrusion ;
- un audit de code, le cas échéant.

Les résultats de ces activités d'audit doivent amener l'autorité administrative, en cas de non-conformités relevées, à identifier les causes de ces dernières, prévoir et mettre en œuvre un plan d'actions correctives et préventives.

POUR PLUS D'INFORMATION :

Autorité compétente : Agence nationale de la sécurité des systèmes d'information (ANSSI)
www.ssi.gouv.fr/rgs
mél. : rgs@ssi.gouv.fr

FICHE N°5

Ouvrir un service numérique au public dans le contexte eIDAS

I / Démarche générale

Dans l'optique de l'ouverture d'un service en ligne, ouvert au public, exigeant une identification, une signature ou un cachet, le RGS s'applique. Il est nécessaire d'appliquer la démarche présentée dans la *Fiche n°4 : Ouvrir un téléservice dans le respect des règles de sécurité*, à savoir :

- la réalisation d'une analyse de risque ;
- la définition des objectifs de sécurité ;
- le choix et mise en œuvre des mesures appropriées de protection et de défense du SI ;
- l'homologation de sécurité du système d'information ;
- le suivi opérationnel de sécurité du SI.

II / Quelle particularité dans le contexte eIDAS ?

La particularité liée au contexte eIDAS va se manifester lors des choix qui seront effectués à l'issue de l'analyse de risques, notamment en ce qui concerne :

- l'identification et l'authentification des usagers ;
- l'usage de services de confiance : signatures électroniques, cachets électroniques ou envois recommandés électroniques.

A L'IDENTIFICATION ÉLECTRONIQUE ET FRANCECONNECT

L'analyse des risques réalisée peut faire apparaître des risques liés à l'identification des usagers. En fonction de la criticité de ces derniers et des objectifs que vous fixerez, la mise en œuvre d'une identification de niveau faible, substantiel ou élevé peut-être identifiée. Afin de tenir compte de l'obligation de reconnaissance mutuelle des moyens d'identification des États membres prévue dans le règlement eIDAS, la France, et plus particu-

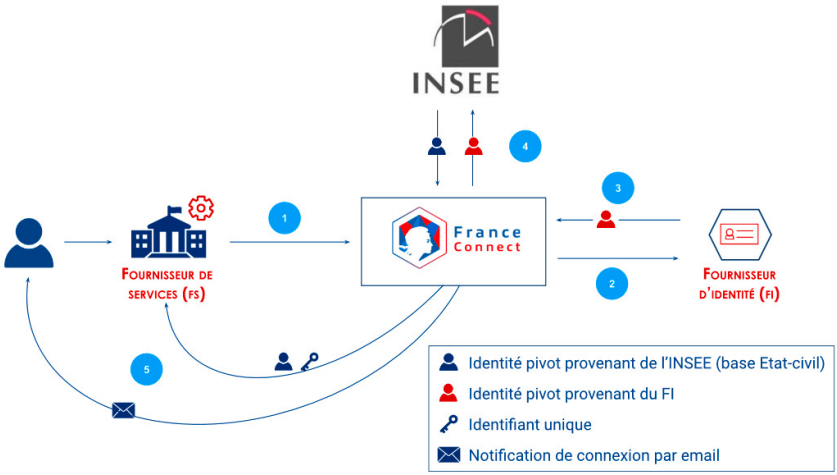
lièrement la direction interministérielle du numérique (DINUM), a mis en place la solution FranceConnect [26].

FranceConnect se présente comme un fédérateur d'identité qui assure l'interface avec les solutions d'identité électronique notifiées par les États membres de l'Union européenne. Ainsi et afin de permettre à tout citoyen européen d'accéder à leurs services, les collectivités territoriales peuvent alors se « raccorder » techniquement à FranceConnect en effectuant une demande d'habilitation auprès du service [27].

PAR EXEMPLE :

Un État membre (hors France) notifie un moyen d'identification électronique (type carte d'identité nationale électronique) au niveau élevé. Une collectivité territoriale décide de mettre en œuvre un système d'information permettant aux citoyens de s'inscrire dans les crèches disponibles dans son périmètre géographique. L'analyse de risque sur ce système d'information met en lumière la sensibilité des informations traitées et notamment le fait que ces informations soient accessibles aux seules personnes concernées. Le plan d'actions issu de cette analyse implique la mise en œuvre d'un moyen d'identification électronique de niveau substantiel. La mise en œuvre technique de ce moyen devra s'attacher à permettre à un citoyen de cet État membre d'utiliser sa carte nationale d'identité électronique pour recourir à ce service.

26 etatplateforme.modernisation.gouv.fr/actualite/france-connect-eidas-vers-une-identite-numerique-europeenne
27 franceconnect.gouv.fr/partenaires?source=homepage_header



1. Le fournisseur de service (FS) demande à FranceConnect (FC) de lui renvoyer l'identité pivot de l'usager : nom, prénom, date et lieu de naissance, sexe et adresse électronique
2. L'usager sélectionne un fournisseur d'identité (FI) et s'identifie en utilisant les identifiants de son compte chez le FI.
3. Le FI renvoie l'identité pivot de l'usager à FC.
4. FC demande validation de l'identité pivot à l'INSEE, qui la redresse en cas de faible écart. FC génère un identifiant unique de l'usager, spécifique au FS.
5. FC retourne l'identité pivot et l'identifiant unique au FS. L'usager est connecté au service et informé par mail.

Figure 5 : Fonctionnement de FranceConnect

B L'USAGE DE SERVICES DE CONFIANCE

En fonction des services proposés (par exemple l'usage de la signature électronique dans le cadre de marché public), les collectivités territoriales peuvent avoir recours à des services de confiance en faisant appel à des prestataires pour les accompagner dans l'implémentation du service.

Pour choisir les prestataires de services de confiance, le règlement eIDAS impose que chaque État membre publie et maintienne à jour une liste de confiance [LIST_CONF] reprenant les informations relatives aux prestataires de services de confiance qualifiés ainsi que les services de confiance qu'ils fournissent.

POUR PLUS D'INFORMATION :

Autorité compétente : Agence nationale de la sécurité des systèmes d'information (ANSSI)
www.ssi.gouv.fr/eidas
mél. : supervision-eidas@ssi.gouv.fr

FICHE N°6

Recourir à l'externalisation pour la gestion du système d'information

De plus en plus d'organisations ont recours à l'externalisation pour la gestion de tout ou partie de leurs systèmes d'information. Ce constat est également valable pour les collectivités territoriales et s'explique par les raisons suivantes :

- la réduction des budgets alloués ;
- l'absence ou la perte des compétences nécessaires ;
- la simplicité de gestion ;
- la mise en conformité avec les exigences légales et règlementaires.

Cependant, recourir à l'externalisation n'est pas exempt de risques de sécurité, notamment en matière de gestion des données à caractère personnel. Cela étant, il convient de faire preuve d'une attention toute particulière à l'égard d'un certain nombre de risques. Ces derniers peuvent rester résiduels, à condition d'observer certaines bonnes pratiques.

I/ Risques liés à l'externalisation

A LA CHAÎNE DE SOUS-TRAITANCE

Lors du recours à l'externalisation, le titulaire du marché peut lui-même recourir à la sous-traitance. Le recours à la sous-traitance peut impliquer des risques liés aux ressources (humaines, financières, etc.) ainsi que des risques liés aux compétences des sous-traitants.

Afin de traiter ce problème, le marché peut explicitement interdire le recours à la sous-traitance ou encore l'autoriser en appliquant un certain nombre de clauses qui permettront de s'assurer que le sous-traitant dispose des capacités techniques et financières pour exécuter les prestations.

B LA LOCALISATION DES DONNÉES

L'émergence de l'informatique en nuage peut amener les collectivités territoriales à s'interroger sur la localisation de leurs données. Pour elles, cette

incertitude peut entraîner des difficultés à exercer son droit de regard et de contrôle sur les traitements de données ainsi que pour répondre à d'éventuelles injonctions de la justice.

Le cadre règlementaire que nous venons de présenter n'impose aucune restriction quant à la localisation des données. De plus, dans le cadre particulier des données à caractère personnel, leur transfert hors de l'Union européenne (UE) ou de l'espace économique européen (EEE) est possible sous réserve que le responsable de traitement puisse assurer un niveau de protection suffisant des données.

C LES RISQUES TECHNIQUES

1 – L'infogérance

La mise en place de l'externalisation introduit de nombreux risques liés aux aspects techniques. Par exemple dans le cadre de l'infogérance, il peut être nécessaire de permettre l'accès à distance au système d'information. Cela impose aux collectivités territoriales, via l'analyse de risques, de réfléchir aux problématiques liées à l'interconnexion des systèmes d'information :

- l'usage de tunnels VPN chiffrés et authentifiés ;
- la sécurisation des moyens d'authentification (usage de double facteur) ;
- la gestion des habilitations des personnels du sous-traitant accédant au système d'information ;
- le *reporting* des interventions, difficultés et autres incidents liés à l'exécution du marché ;
- etc.

2 – L'hébergement physique

Ce modèle d'hébergement est le plus proche de l'hébergement internalisé. Les seules responsabilités incombant au sous-traitant sont la mise à disposition des locaux et les dispositifs de sécurité physique (protection incendie, refroidissement, alimentation électrique) et la connexion au réseau Internet.

Même si les responsabilités sont limitées, elles ne sont pas pour autant négligeables. Les risques liés au cloisonnement physique entre les différents environnements client, la gestion électrique, les mécanismes de protection physique (refroidissement, protection incendie, etc.) mais également les risques logiques comme le contrôle de flux, la disponibilité des connexions réseaux par exemple sont à prendre en compte.

Suite à l'appréciation des risques, les collectivités territoriales peuvent imposer des clauses de sécurité dans les contrats par exemple sur le taux de disponibilité du service.

3 – L'informatique en nuage (ou *Cloud Computing*)

a/*Infrastructure as a Service* (IaaS)

Ce mode d'hébergement donne les mêmes responsabilités au sous-traitant que précédemment en ajoutant la gestion du matériel informatique et du réseau interne. La responsabilité des collectivités territoriales porte sur la partie logicielle c'est-à-dire la gestion des différents systèmes, applications et données.

Des risques liés à la prise en charge des services d'infrastructure (les sauvegardes, le stockage, la virtualisation, le réseau) par le sous-traitant sont à considérer. Afin de couvrir ces risques, l'analyse de risques réalisée par les collectivités territoriales doit permettre de faire émerger des besoins sur ces différents services d'infrastructure (fréquence des sauvegardes, externalisation, volume des stockages, conception, dimensionnement des flux et de l'architecture réseau, isolation des différents environnements client, etc.).

b/*Plateform as a Service* (PaaS)

Ce mode d'hébergement réduit davantage encore les responsabilités des collectivités territoriales, accroissant ainsi celles du sous-traitant. Les collectivités sont uniquement responsables de la couche applicative (*i.e.*

installation des applications) et de la couche de données.

De nouveaux risques apparaissent avec l'externalisation de la gestion de la couche logicielle qui peuvent se traduire, à l'issue de l'analyse de risques, par l'inclusion d'exigences dans les marchés relatives à la configuration, au maintien en condition de sécurité de la plateforme et au durcissement* des systèmes.

c/*Software as a Service* (SaaS)

Les prestataires proposant ce type d'hébergement offrent une infrastructure complète adaptée aux besoins de leurs clients avec les services associés (application, sauvegarde, stockage, réseau, etc.), ces derniers n'ayant plus qu'à procéder au dépôt de leurs données.

Les risques précédemment évoqués sont valables également pour ce type d'offre de service. Vient s'ajouter à cela la transmission des données pour les intégrer dans l'environnement client nouvellement créé. En effet, les collectivités territoriales peuvent être amenées à transmettre les données en amont pour intégration dans l'environnement. En fonction de la criticité de celles-ci, des précautions doivent être prises (chiffrement des flux, conteneur chiffré, etc.).

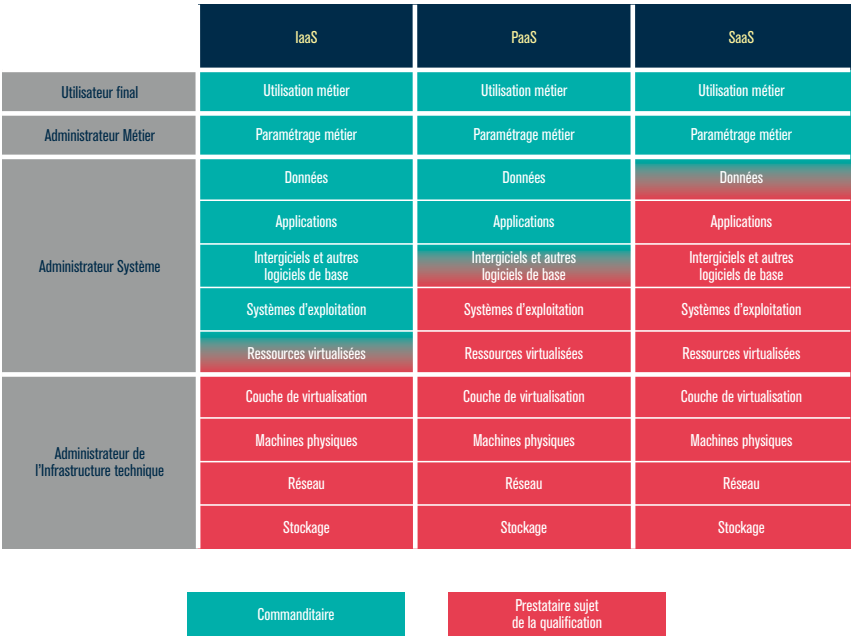


Figure 6 : Synthèse des répartitions de responsabilités selon les différents types d'hébergement

II/ Synthèse des recommandations liées à l'externalisation

ATTENTION :

Les recommandations présentées ici ne sont pas exclusives et respectent une suite logique : mener l'analyse de risque doit permettre à la collectivité territoriale de savoir si, compte-tenu de la sensibilité des informations, le recours à l'externalisation peut être envisageable ou non. Si le recours à l'externalisation est possible, alors la collectivité territoriale doit choisir le prestataire sur la base d'exigences fonctionnelles, techniques et de sécurité à formuler.

A LA RÉGLEMENTATION APPLICABLE

Il est important que le commanditaire inventorie les réglementations applicables (par exemple : la réglementation sur la protection des données à caractère personnel ou sur la protection des informations relevant de la protection du secret de la défense nationale) dans le cadre du marché à pourvoir afin de s'assurer des responsabilités qui lui incombent ainsi qu'aux prestataires.

B L'ANALYSE DE RISQUES

Réaliser l'analyse de risques permet, dans un premier temps, de s'interroger sur la possibilité de recourir à l'externalisation. Dans un second temps l'analyse de risques permet d'identifier les besoins de sécurité et ainsi

de prendre connaissance des risques qui pèsent sur l'organisation et plus particulièrement ceux qui nécessitent le recours à l'externalisation.

Toutefois, l'externalisation ne transfert pas totalement le risque au sous-traitant. Le risque existe toujours et les collectivités territoriales s'appuient sur une tierce partie qui dispose des compétences nécessaires pour réduire ce risque, à condition que les objectifs de sécurité soient bien rappelés dans les clauses du marché pour les rendre opposables au sous-traitant.

ATTENTION :

En fonction de la criticité du système d'information à externaliser, l'analyse de risque à mener devra être plus ou moins détaillée.

1. Pour un système peu critique, on pourra se limiter à une analyse d'écart au [GUIDE_HYG].
2. Pour un système sensible, on effectuera une analyse de risque macroscopique.
3. Pour un système critique, on effectuera une analyse de risque en respectant la méthode [EBIOS *Risk Manager*].

C LE CHOIX DU PRESTATAIRE

ATTENTION :

Les éléments mentionnés dans cette section sont des recommandations à privilégier vis-à-vis d'autres offres de *cloud*.

1 – Le recours au *cloud*

Aucun des référentiels listés dans la partie précédente ne se positionne en faveur ou en défaveur du *cloud*. En revanche, dans le cadre de la mise en œuvre d'un projet de migration de tout ou partie d'un système d'information vers une offre *cloud*, il est fortement recommandé (voire rendu obligatoire par la réglementation) de réaliser une analyse de risque. L'objectif est d'identifier, dans ce contexte, les mesures de sécurité les plus adéquates et ainsi orienter la collectivité territoriale vers le choix d'une solution présentant les meilleurs compromis entre la sécurité d'une part et l'exploitation du système d'information d'autre part.

L'État a par ailleurs développé une stratégie *cloud*. Introduite par la circulaire nº 6049–SG du 8 novembre 2018, cette stratégie développe trois types de solutions :

- le « *cloud* interne » : instances de *cloud* interministériels permettant d'accueillir des données, des traitements et des applications sensibles et de répondre à des besoins régaliens d'infrastructures numériques imposant des exigences d'internalisation des données et de sécurité des systèmes d'information ;
- Le « *cloud* dédié » : offre de *cloud* standard exploitée par un industriel du secteur. Cette offre est personnalisée pour les besoins de l'État et repose sur des infrastructures dédiées. L'acquisition d'une telle offre, prévue pour 2019/2020, est sous la responsabilité de la direction des achats de l'État et la DINUM ;
- Le « *cloud* externe » : offres de *cloud* externes génériques accessibles sur Internet. Un catalogue de ces offres est porté par les centrales d'achat pour en faciliter la commande.

Parallèlement à cette stratégie, l'ANSSI a mis en place une qualification de prestataires de service d'informatique en nuage – SecNumCloud – permettant de promouvoir des offres *cloud* aux organisations souhaitant externaliser l'hébergement de leurs données ou applications auprès de prestataires de confiance. Le référentiel prévoit

des exigences quant au prestataire de service d'informatique en nuage, à son personnel ainsi qu'à la localisation des données au sein de l'Union européenne. Les dernières évolutions du référentiel ont été réalisées en collaboration avec la CNIL afin d'intégrer des exigences cohérentes vis-à-vis du RGPD. L'ANSSI tient à jour la liste des prestataires qualifiés SecNumCloud [LIST_CLOUD].

2 – La mutualisation

Devant les contraintes de ressources et de moyens auxquelles font face les collectivités territoriales, la mutualisation peut représenter un atout non négligeable dans le cadre d'une rationalisation des coûts tout en garantissant un niveau de sécurité. Pour cela, l'État a mis en place l'intercommunalité qui regroupe différentes formes de coopération entre les collectivités territoriales afin qu'elles puissent mutualiser leurs compétences (gestion des déchets, transports urbain, etc.) ou développer des services (développement logiciel, accompagnement à la transformation numérique, prestation de sécurité numérique, etc.). Parmi elles, nous pouvons lister :

- les établissements publics de coopération intercommunale (EPCI) sont un type d'établissements au sein desquels sont regroupées plusieurs communes (exemple : les communautés d'agglomération, les syndicats intercommunaux, métropoles, etc.) ;
- les syndicats mixtes sont le regroupement de collectivités locales (communes, départements, régions) avec d'autres personnes morales de droit public (exemple : Soluris) ;
- etc.

D LES CLAUSES DE SÉCURITÉ

Parmi les résultantes majeures de l'analyse de risques figurent les objectifs de sécurité que vous souhaitez voir respectés par le prestataire.

Ces objectifs de sécurité doivent être traduits en termes de clauses à inclure dans les marchés publics et contrats de prestations.

1 – Le contrôle et l'audit

Cette clause primordiale doit vous permettre de contrôler que le marché respecte les clauses du contrat, notamment du point de vue de la sécurité numérique. La clause doit notamment prévoir la fréquence, les conditions de réalisation de l'audit, le rapport d'audit, la possibilité de délégation à un tiers et le suivi des actions issues de l'audit.

2 – Le niveau de service

Peu importe l'offre de service choisie, il est toujours nécessaire d'établir un niveau de service qui réponde aux contraintes opérationnelles des collectivités territoriales. Ce niveau de service peut s'établir sur différents domaines : le taux de disponibilité moyen de la plateforme, le délai moyen de traitement des demandes (modifications de l'environnement, problèmes/bogues, incidents de sécurité, etc.).

3 – Les rôles et responsabilités

Selon le type d'hébergement, les responsabilités entre le prestataire et les collectivités territoriales évoluent. Il est indispensable au sein du contrat de clarifier les responsabilités de chacune des parties.

4 – La confidentialité

Il est important de préciser que les informations portées à la connaissance du prestataire durant toute la durée de l'exécution du marché sont la propriété des collectivités territoriales et ne doivent en aucun cas être transmises à des tiers ou tout autre membre du personnel sans l'autorisation explicite du responsable de la collectivité territoriale.

E LE PLAN D'ASSURANCE SÉCURITÉ (PAS)

Le PAS est un document contractuel qui peut être demandé dans le cadre de marchés. Rédigé par le prestataire, il décrit les moyens que ce dernier met en œuvre pour répondre aux différentes exigences décrites dans le marché.

POUR PLUS D'INFORMATION :

SecNumCloud :
www.ssi.gouv.fr/actualite/secnumcloud-la-nouvelle-reference-pour-les-prestataires-dinformatique-en-nuage-de-confiance/
www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/

Guide d'externalisation de l'ANSSI :
www.ssi.gouv.fr/administration/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/

FICHE N°7

Mise en œuvre d'un système de management de la sécurité de l'information (SMSI) dans le contexte HDS

I / Présentation succincte de l'ISO/CEI 27001:2013

La norme ISO/IEC 27001:2013 est un référentiel d'exigences pour la mise en œuvre d'un SMSI. C'est vis-à-vis de ce référentiel, entre autres, que les organisations qui souhaitent se faire certifier sont évaluées par des organismes de certification.

La norme s'accompagne d'une annexe qui aborde, à travers 114 mesures, l'ensemble des thématiques de sécurité [28]. Ces mesures doivent notamment être reprises dans la déclaration d'applicabilité*, document requis par la norme.

II / Principe de mise en œuvre du SMSI

La mise en œuvre du SMSI peut être génératrice de changement plus ou moins importants au premier rang desquels figure le passage d'une tradition orale à une tradition écrite, dans le but de fournir des éléments à auditer pour les organismes de certification. Ainsi la norme impose la notification écrite d'un certain nombre d'éléments tels que la politique de sécurité ou la déclaration d'applicabilité.

La philosophie du SMSI repose sur deux principes fondamentaux que sont **l'appréciation des risques** et **l'amélioration continue**.

A L'APPRÉCIATION DES RISQUES

Prenant en compte les éléments recueillis lors de la phase d'étude du contexte interne et externe de l'organisation (le positionnement sur le

---

28 On y retrouve ainsi les ressources humaines, le contrôle d'accès, l'exploitation du système d'information, la gestion des incidents ou encore la gestion des tiers

marché de l'organisation, le contexte social interne, la situation géographique) ainsi que les attentes des parties intéressées* vis-à-vis du SMSI, le responsable du SMSI (RSMSI) définit en conséquence le domaine d'application du système de management.

Le RSMSI réalise ensuite une appréciation des risques [29] sur le domaine d'application défini. Cette appréciation des risques doit amener le RSMSI à mettre en œuvre les mesures de sécurité nécessaires pour protéger les informations ou processus considérés comme essentiels. Les livrables à fournir au terme de l'appréciation sont :

- L'inventaire des risques résiduels et leur approbation par les propriétaires des risques ;
- le plan de traitement des risques (PTR) ;
- les objectifs de sécurité ;
- la politique de sécurité ;
- la déclaration d'applicabilité.

B L'AMÉLIORATION CONTINUE

Le principe d'amélioration continue s'appuie sur la boucle Plan, Do, Check, Act (PDCA) également appelée Roue de Deming. Cette boucle d'amélioration continue se traduit dans la norme par l'obligation pour l'organisation de définir des objectifs de sécurité qu'elle souhaite atteindre. Ces objectifs sont pris en compte, ainsi que les exigences légales, règlementaires et contractuelles auxquelles l'organisation est soumise, pour réaliser l'appréciation des risques et décider des mesures de sécurité à mettre en œuvre pour traiter ces risques. Régulièrement, l'organisation doit réaliser des audits et contrôles sur le SMSI et les mesures de sécurité mis en œuvre. Ces audits et contrôles peuvent remonter des non-conformités que la norme prévoit de traiter par la définition d'un plan d'actions correctives et

29 Pour réaliser l'appréciation des risques, on peut s'appuyer sur la méthodologie EBIOS RM ou encore la norme ISO/IEC 27005:2018

préventives qui doivent permettre d'une part de traiter la non-conformité lors de sa survenance et d'autre part de prendre les dispositions adéquates pour éviter qu'elles se reproduisent dans la durée.

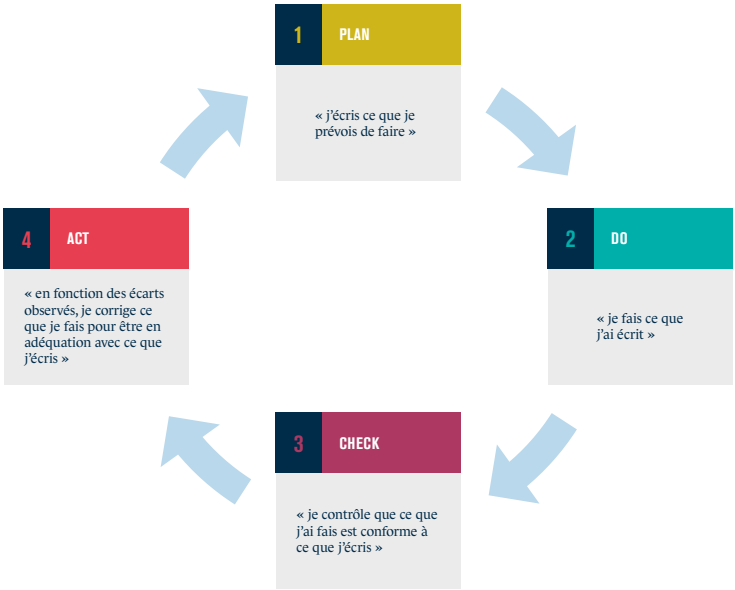


Figure 7 : Démarche d'amélioration continue

C LES SPÉCIFICITÉS DU SMSI DANS LE CONTEXTE HDS

1 – Le domaine d'application

Le référentiel applicable aux hébergeurs de données de santé (HDS) oblige les candidats à la certification HDS à définir un domaine d'application qui couvre, au minimum, les activités d'hébergement de données de santé. L'objectif est d'éviter que les candidats à la certification HDS l'obtiennent alors que la certification 27001 couvre un domaine d'application qui n'est pas lié à l'activité d'hébergement.

2 – La déclaration d'applicabilité

Le référentiel HDS oblige les candidats à la certification HDS à fournir une déclaration d'applicabilité dans laquelle sont listées les 114 mesures de l'Annexe A de la 27001 ainsi que les exigences supplémentaires prévues dans le référentiel HDS lui-même.

III / La certification

L'obtention de la certification nécessite que l'organisation signe un contrat avec un organisme de certification accrédité pour les audits de SMSI.

La certification se déroule sur un cycle de 3 ans avec :

- l'audit initial durant lequel l'organisation de certification auditera l'ensemble du SMSI via un audit de la documentation et un audit par observations, visites, entretiens, etc. ;
- l'audit de surveillance vérifiera partiellement que le SMSI est toujours conforme avec la norme ;
- l'audit de renouvellement se présente quant à lui comme un audit initial.

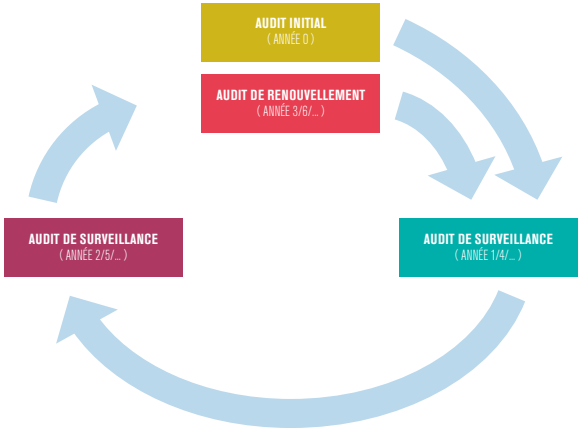


Figure 8 : Présentation du cycle d'audits de certification

TABLE DES ILLUSTRATIONS

INDEX

GLOSSAIRE

ACTIVITÉ D'IMPORTANCE VITALE

Activités difficilement remplaçables ou substituables pour des raisons économiques, sociales ou encore de défense et de sécurité (*cf.* art. R. 1332-2 du code de la défense).

AUTHENTIFICATION

L'authentification a pour but de vérifier l'identité dont une personne se réclame. L'authentification est généralement précédée d'une identification qui permet à cette personne de se faire reconnaître du système par un élément dont on l'a doté (mail, nom d'utilisateur, etc.). S'**identifier revient donc à communiquer son identité et s'authentifier à apporter la preuve de son identité**.

AUTHENTIFICATION MULTI-FACTEUR

L'authentification multi-facteur repose sur au moins deux secrets choisis parmi :

- ce que l'on sait (par exemple un mot de passe) ;
- ce que l'on a (par exemple une carte à puce, un smartphone) ;
- ce que l'on est (par exemple les empreintes digitales, le réseau veineux, les empreintes rétiniennes).

CACHET ÉLECTRONIQUE

Données électroniques sont jointes ou associées logiquement à d'autres données électroniques en vue de garantir l'origine et l'intégrité de ces dernières (*cf.* règlement eIDAS – article 3 – alinéa 25).

CERTIFICAT ÉLECTRONIQUE

Document électronique attestant du lien entre une clé publique et l'identité de son propriétaire. (*cf.* annexe A2 du RGS – I.3.2).

CERTIFICATE REVOCATION LIST (CRL)

Liste maintenue par une autorité de certification référençant les certificats électroniques émis et désormais révoqués ou invalidés (expiration, suspicion de compromission de la clé privée ou de l'autorité de certification, etc.).

COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT)

Organisation ayant pour missions :

- la centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations ;
- le traitement des alertes et réactions aux attaques informatiques ;
- l'établissement et la maintenance d'une base de données des vulnérabilités ;
- la prévention par la diffusion d'informations de bonnes pratiques préventives ou réactives ;
- la coordination éventuelle avec les autres organisations (hors du domaine d'action).

DÉCLARATION D'APPLICABILITÉ

Ce document se présente comme la liste, au minimum, des 114 mesures de l'ISO/CEI 27002. Le responsable du SMSI (RSMSI) y renseigne, pour chacune d'elles, leur application ou non et la justification associée ainsi que leur statut de mise en œuvre. Il permet au RSMSI de s'assurer qu'aucune mesure/thématique de sécurité n'a été omise. Il s'agit d'un document essentiel puisqu'il va déterminer le champ d'application de l'audit.

DURCISSEMENT

Le durcissement vise à limiter l'installation d'applications et l'activation de services sur les systèmes d'information pour ne conserver que ceux indispensables au fonctionnement dudit système d'information.

SERVICE D'ENVOI RECOMMANDÉ ÉLECTRONIQUE

Service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée. (*cf.* règlement eIDAS – article 3 – alinéa 36).

FONCTION DE HACHAGE

Fonction cryptographique qui transforme une chaîne de caractères de taille quelconque en une chaîne de caractères de taille fixe et généralement inférieure. Cette fonction satisfait entre autres deux propriétés :

- la fonction est « à sens unique » : il est difficile pour une image de la fonction donnée de calculer l'antécédent associé ;
- la fonction est « sans collision » : il est difficile de trouver deux antécédents différents de la fonction ayant la même image.

FOURNISSEUR DE SERVICE NUMÉRIQUE (FSN)

Fournisseur de service numérique : toute personne morale qui fournit l'un des services suivants : place de marché en ligne, moteur de recherche en ligne et les services d'informatique en nuage (*Cloud Computing*). Ne sont pas concernées les entreprises de moins de cinquante salariés et dont le chiffre d'affaire n'excède pas 10 millions d'euros (art. 10, alinéa 2 et art. 11 de la loi n° 2018-133 du 26 février 2018).

HORODATAGE ÉLECTRONIQUE

Données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant. (*cf.* règlement eIDAS – article 3 – alinéa 33).

INTRUSION DETECTION SYSTEM (IDS)

Dispositif de remontée d'événements de sécurité permettant la supervision d'un système d'information aussi bien au niveau du réseau ou d'une machine/serveur.

INFORMATIONS PUBLIQUES

Informations figurant dans les documents administratifs quel qu'en soit le support. « Elles peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celle de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus » dans la limite de la communicabilité de ladite information (exemple : information protégée par la propriété intellectuelle, par le secret de la défense, etc.).

ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

Alternative à la CRL, l'OCSP est un protocole de communication permettant d'obtenir le statut d'un certificat électronique (*good, unknown, revoked*).

OPÉRATEURS D'IMPORTANCE VITALE (OIV)

L'art. R. 1332-1 du code de la défense précise que les opérateurs d'importance vitale sont désignés parmi les opérateurs publics ou privés mentionnés à l'article L. 1332-1 du même code, ou parmi les gestionnaires d'établissements mentionnés à l'article L. 1332-2. Un opérateur d'importance vitale :

- exerce des activités mentionnées à l'article R. 1332-2 et comprises

dans un secteur d'activités d'importance vitale ;

- gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population.

OPÉRATEURS DE SERVICES ESSENTIELS (OSE)

Opérateurs publics ou privés offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services (art. 5 de la loi nº 2018-133 du 26 février 2018).

PARTIE INTÉRESSÉE

Personne physique ou morale qui sera impactée par la mise en œuvre du SMSI parce qu'elle prend part à sa mise en œuvre ou à son exploitation (ex. : le personnel, les tiers, etc.) ou encore qu'elle impose des exigences aux SMSI en matière de sécurité de l'information (ex. : l'État par le biais de la réglementation, les clients par le biais des contrats, etc.).

HAMEÇONNAGE OU *PHISHING*

Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

Remarque : les sites sont reproduits, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.

PSEUDONYMISATION

Traitement de données à caractère personnel réalisé de telle sorte que celles-ci ne puissent plus être attribuées à une personne précise sans avoir recours à des informations supplémentaires. Pour ce faire, elles doivent être conservées séparément et soumises à des mesures techniques et institutionnelles afin de garantir que ces données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

La pseudonymisation est à distinguer de l'anonymisation.

SÉCURITÉ NUMÉRIQUE

Processus visant à protéger les données numériques traitées. Lorsque l'on traite de la sécurité de l'information, au moins trois critères doivent être considérés : la disponibilité, l'intégrité et la confidentialité.

En fonction des besoins, d'autres critères peuvent être pertinent tels que la traçabilité, l'authenticité, etc.

SERVEUR DE COMMANDES ET DE CONTRÔLES (C2/C&C)

Serveur communément utilisé dans le cadre de machines enrôlées dans un réseau de machines zombies (*botnet*) permettant, de manière centralisée, de donner des ordres à tout ou partie des machines compromises.

SIGNATURE ÉLECTRONIQUE

Données électroniques, jointes ou associées à d'autres données électroniques et que le signataire utilise pour signer (cf. règlement eIDAS – article 3 – alinéa 10).

SYSTÈME D'INFORMATION

Ensemble des ressources matérielles (postes de travail, serveurs, etc.) et logicielles (suite bureautique, outil de messagerie, etc.) nécessaires pour réaliser une activité.

TÉLÉSERVICE

Est considéré comme téléservice, tout système d'information permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives (art. 1 de l'ordonnance n° 2005-1516).

TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Constitue un traitement de données à caractère personnel toute opération ou ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation ou modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction. (art. 2 de la loi n° 78-17 du 6 janvier 1978 modifiée)

BIBLIOGRAPHIE

[CERT-FR]

Page consacrée au CERT-FR : www.cert.ssi.gouv.fr/

[EBIOS RISK MANAGER]

Page consacrée à la méthodologie EBIOS RM : www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

[GUIDE_EXT]

Guide pratique sur l'externalisation : www.ssi.gouv.fr/administration/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/

[GUIDE_HOMOL]

Guide d'homologation en 9 étapes : www.ssi.gouv.fr/actualite/lhomologation-en-9-etapes-simples-nouvelle-publication-de-lanssi/

[GUIDE_HYG]

Guide d'hygiène informatique : www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

[GUIDE_JOURNA]

Recommandations de sécurité pour la mise en œuvre d'un système de journalisation : www.ssi.gouv.fr/uploads/IMG/pdf/NP_Journalisation_NoteTech.pdf

[GUIDE_PSSI]

Guide d'élaboration de politiques de sécurité des systèmes d'information : www.ssi.gouv.fr/administration/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/

[INSTR_2009_018]

Instruction sur le tri et conservation des archives produites par les services communs à l'ensemble des collectivités territoriales et structures intercommunales
circulaire.legifrance.gouv.fr/pdf/2009/09/cir_29574.pdf

[LIST_CLOUD]

Liste des prestataires disposant de la qualification SecNumCloud : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/

[LIST_CONF]

Liste de confiance des prestataires de confiance qualifiés par la France dans le cadre du règlement eIDAS : webgate.ec.europa.eu/tl-browser/#/tl/FR
www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/liste-nationale-de-confiance/

[LIST_HDS]

Liste des hébergeurs de données de santé agréés : esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees

Liste des hébergeurs de données de santé certifiés : esante.gouv.fr/services/liste-des-hebergeurs-certifies-hebergeur-de-donnees-de-sante-a-caractere-personnel

[LIST_PROD]

Liste des produits qualifiés : www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/

Liste des produits certifiés :

- CSPN : www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/
- CC : www.ssi.gouv.fr/administration/produits-certifies/cc/produits-certifies-cc/

[LIVRE_BLANC]

Livre blanc sur la défense et de la sécurité nationale : www.livreblanc-defenseetsecurite.gouv.fr/index.html

[PLAQ_SAIV]

Plaquette SAIV : www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

[PREST_ARCHIVAGE]

Liste des prestataires d'archivage agréés : francearchives.fr/article/26287438

[PREST_LPM]

Liste des prestataires qualifiés au sens LPM :

- PDIS : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-detection-dincidents-de-securite-pdis/
- PRIS : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/
- PASSI LPM : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/

[PSCO]

Liste des prestataires qualifiés au sens RGS :

- PSCE : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-services-de-certification-electronique-psce-et-dhorodatage-electronique-pshe-qualifies/
- PSHE : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-services-dhorodatage-electronique-pshe-qualifies/
- PASSI : www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/

[REF_HDS]

Référentiel de certification HDS : esante.gouv.fr/sites/default/files/asset/document/asip_-_exigences_et_controles_du_referentiel_hds_-_v1.1.pdf

[SECNUMCLOUD]

Référentiel et prestataires qualifiés SecNumCloud : www.ssi.gouv.fr/actualite/secnumcloud-la-nouvelle-reference-pour-les-prestataires-dinformatique-en-nuage-de-confiance/

Version 1.1 – Mars 2020
ANSSI-PA-071

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI – 51, boulevard de la Tour-Maubourg – 75 700 PARIS 07 SP
www.ssi.gouv.fr – communication@ssi.gouv.fr – ebios@ssi.gouv.fr