LIVRE BLANC :
BONNES PRATIQUES RGPD

à l'attention du secteur des intégrateurs, installateurs, mainteneurs de technologies connectées, sécurisées et pilotées.

CNPP | Prévention et maîtrise des risques

ANITEC
ALLIANCE NATIONALE
DES INTÉGRATEURS DE TECHNOLOGIES
CONNECTÉES, SÉCURISÉES ET PILOTÉES

INTRODUCTION

L'**ANITEC et CNPP** ont souhaité, dans le cadre de leur partenariat, rédiger un guide de bonnes pratiques RGPD pour identifier les principes devant encadrer la collecte et le traitement de données personnelles du secteur des intégrateurs installateurs-mainteneurs de technologies connectées, sécurisées et pilotées.

L'objectif du groupe de travail qui a rédigé ce livre blanc, est d'aboutir à la publication d'un référentiel sectoriel qui a pour objet d'accompagner les prestations des intégrateurs, installateurs et mainteneurs pour :

- identifier les produits des fabricants disposant d'une sécurité native ou en intégrant la protection des données personnelles le plus en amont possible de la conception des installations jusqu'à la maintenance,
- assurer la maîtrise des données, tout en prenant en compte les réalités du secteur.

Ces bonnes pratiques ont vocation à être portées au niveau européen pour permettre aux acteurs de se positionner sur un marché européen voire mondial. C'est en ce sens, qu'il pourrait constituer une ligne directrice européenne en application du règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (ci-après « RGPD »).

Le groupe de travail précise sur ce point que ces lignes directrices sont représentatives de la compréhension, à un moment donné, de technologies et d'usages devant faire l'objet d'un bilan régulier. Elle souhaite donc souligner le caractère évolutif du présent « livre blanc ».

Ce livre blanc a pour ambition d'être la base du référentiel pour l'obtention du label RGPD de CNPP permettant aux donneurs d'ordre de s'assurer de la conformité RGPD d'une entreprise d'intégration, d'installation ou de maintenance de technologies connectées, pilotées, sécurisées.

ANITEC (Alliance Nationale des Intégrateurs de TEChnologies connectées, sécurisées et pilotées) est la première organisation professionnelle regroupant des professionnels experts des métiers de l'information, la communication, de la sécurité des biens et des personnes, et de domotique au sens large du terme. **Elle bénéficie du soutien et adhère à la FFIE (Fédération Française des Intégrateurs électriciens).**
Ses objectifs : accompagner les professionnels experts dans leurs domaines, développer les échanges entre professionnels, valoriser les compétences.

CNPP, expert en prévention et en maîtrise des risques, est un acteur international de référence dans ce domaine. Il intervient en premier lieu dans les domaines de la **sécurité incendie** et de la **sûreté malveillance** en proposant une offre globale et diversifiée (certification, essais de conformité, études et expérimentation, conseil et assistance technique, formation, édition et presse). L'écosystème de CNPP couvre l'ensemble des acteurs de la maîtrise des risques et en particulier les installateurs et mainteneurs des technologies de sécurité. Les certifications de service APSAD, dispensées par CNPP, ont pour objet notamment d'être un gage de confiance pour les différentes parties prenantes et mettent en exergue les règles de l'art et les bonnes pratiques en matière de conception, de mise en oeuvre et de maintenance des technologies de sécurité incendie et de sûreté malveillance.

SOMMAIRE

PÉRIMÈTRE DU GUIDE

SCÉNARIOS

Quatre scénarios ont été identifiés pour illustrer le secteur des intégrateurs, installateurs, mainteneurs de technologies connectées, sécurisées et pilotées. Ces scénarios sont décrits ci-après en respectant les résultats d'une concertation réalisée auprès des professionnels du secteur.

Ces concertations ont permis d'identifier, pour chaque scénario, le cadre et les conditions dans lesquelles les traitements peuvent être mis en œuvre, à l'appui d'exemples de finalités, d'études d'impact sur la vie privée, de catégories de données traitées, de durées de conservation adéquates, de destinataires, de modalités d'information et d'exercice des droits des personnes et de mesures de sécurité adaptées aux risques.

PÉRIMÈTRE DU GUIDE

SCÉNARIO 1
GESTION DES DONNÉES CLIENT :

Les éléments contractuels et les dossiers techniques concernant la conception des installations réalisées sont stockés par l'installateur. Ces données peuvent être statiques (plans d'installation) ou dynamiques (identifiants / mots de passe liés aux systèmes).

L'installateur porte la responsabilité de la protection des données de ses clients et doit mettre en œuvre les mesures de sécurité correspondant à la gestion des données client.

→ **Exemple : cas d'un installateur de système d'alarme intrusion**

Un installateur réalise des installations de systèmes d'alarme mais doit également en assurer la maintenance. Pour cela, l'installateur stocke notamment les informations concernant ses clients et les installations réalisées chez ces derniers. Ces données (plans d'installation, codes d'accès etc..) sont sensibles car elles permettent les accès administrateur aux installations réalisées, en les associant aux noms et adresses de ses clients.

Les mesures applicables à ce scénario doivent permettre à l'installateur de garantir que les données de ses clients sont protégées contre le vol ou la perte (redondance), et que son organisation permet de garantir à ses clients un niveau de confidentialité adapté.

Voir fiche Mémo 1 page 39
pour les mesures applicables à ce scénario.

PÉRIMÈTRE DU GUIDE

SCÉNARIO 2
DONNÉES GÉNÉRÉES PAR L'INSTALLATION :

L'installation réalisée, celle-ci génère des données (journaux de bord avec les connexions, stockage d'informations / d'images...), qui peuvent être consultées localement pour l'exploitation du système.

Les systèmes installés doivent permettre une exploitation locale sécurisée de ces données. L'installateur porte la responsabilité de la capacité de son installation à protéger ces données.

→ **Exemple : cas d'une installation de vidéosurveillance / vidéoprotection**

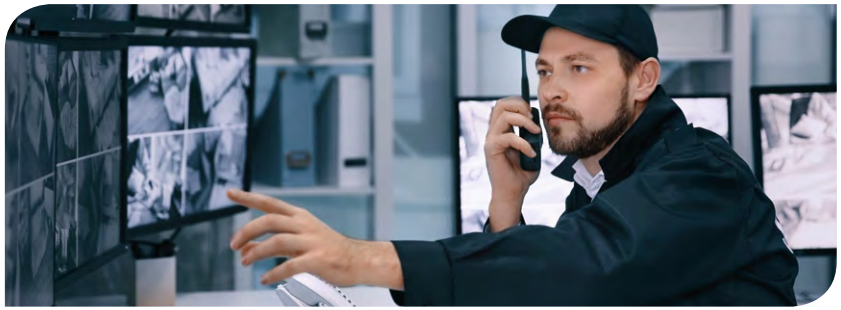
Les installations de vidéosurveillance / vidéoprotection sont assez peu exploitées « en direct ». Et quand bien même elles le sont, l'exploitation « en différé », se basant sur les images enregistrées, est aujourd'hui de très loin le principal mode d'exploitation de systèmes de vidéosurveillance / vidéoprotection.

Les images stockées sont des informations relevant des données personnelles et leur diffusion doit pouvoir être contrôlée.

Les mesures applicables à ce scénario doivent permettre à l'exploitant non seulement de bénéficier d'une information quant à la qualité de l'installation de vidéoprotection au regard de la protection des données (robustesse des matériels et déploiement réseau cohérent), mais aussi de faire en sorte que l'exploitation du système est faite selon des recommandations correspondant à l'état de l'art pour ce qui est de l'hygiène informatique (gestion des identifiants et mots de passe pour les accès aux systèmes, traçabilité de l'exportation des images, fréquence des mises à jour de sécurité, etc.).

Voir fiche Mémo 2 page 40
pour les mesures applicables à ce scénario.

PÉRIMÈTRE DU GUIDE



SCÉNARIO 3
DONNÉES COMMUNIQUÉES À L'EXTÉRIEUR :

L'installation inclut la transmission de données à l'extérieur des locaux de l'entreprise (alarmes, images...), qui peuvent être consultées pour l'exploitation du système par un utilisateur du système ou par un tiers (ex : prestataire de télésurveillance).

L'installateur porte la responsabilité de la sécurité des données lors du transport de celles-ci.

Le prestataire exploitant porte la responsabilité de la confidentialité des données lors de leur réception.

→ Exemple : cas du télésurveilleur

Le rôle du télésurveilleur est la surveillance à distance par des moyens électroniques de sécurité. Toutes les données potentiellement envoyées par les systèmes de sécurité/sûreté vont transiter vers le télésurveilleur, puis faire l'objet d'un enregistrement chez ce dernier.

Si l'envoi et le transport des données ne sont pas nécessairement du ressort du télésurveilleur, leur réception, leur traitement et leur stockage nécessitent un engagement fort de la part du télésurveilleur, du fait de la sensibilité très grande des données, qui peuvent arriver depuis plusieurs milliers de sites différents. Cet engagement tient autant de la mise en œuvre de moyens techniques que de la gestion des ressources humaines.

Les mesures applicables à ce scénario ont pour objectif de permettre au télésurveilleur de proposer à ses clients des éléments tangibles prouvant son engagement pour la protection des données qu'il traite.

Voir fiche Mémo 3 page 41
pour les mesures applicables à ce scénario.

PÉRIMÈTRE DU GUIDE

SCÉNARIO 4
DONNÉES ACCESSIBLES LORS DES OPÉRATIONS DE MAINTENANCE :

L'installation réalisée nécessite des actions de maintenance et peut éventuellement permettre la télémaintenance, donnant l'accès aux données stockées localement au prestataire de maintenance.

Le prestataire de maintenance y compris s'il s'agit de l'installateur ou de l'intégrateur, doit s'engager sur la confidentialité des données traitées.

→ Exemple : cas du contrat de maintenance

Les prestataires de maintenance des systèmes de sécurité/sûreté vont bénéficier d'un accès et d'une connaissance des systèmes de sécurité dont ils vont assurer la maintenance. Leur engagement quant aux données auxquelles ils auront accès et quant aux données qu'ils vont eux-mêmes générer (opérations de mise à jour des identifiants / mots de passe...) doit être cohérent avec celui mis en place lors de la réalisation initiale de l'installation.

Les mesures applicables à ce scénario doivent permettre au mainteneur de prouver qu'il est en mesure de s'engager sur une certaine continuité du niveau de protection des données.

Voir fiche Mémo 4 page 42
pour les mesures applicables à ce scénario.

2

CONTEXTE RÉGLEMENTAIRE

Ce guide ANITEC/CNPP a pour objet de proposer une stratégie collective pour permettre aux entreprises d'anticiper et exécuter dans les meilleures conditions l'application du Règlement Européen sur la Protection des Données Personnelles. À cette fin, nous prenons en compte les trois objectifs définis dans ce règlement qui viennent réformer la protection des données :

- Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et des nouveaux droits qui accompagnent les citoyens dans l'Union européenne ;
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
- Crédibiliser la régulation grâce à une coopération renforcée entre nos entreprises et les autorités de protection des données.

À travers ce livre blanc, transparaît une démarche volontaire de conformité basée sur la transparence et la responsabilisation. Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclarations, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement de l'autorité de contrôle.

2

CONTEXTE RÉGLEMENTAIRE

Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, ANITEC comme ses partenaires en qualité de responsables de traitements ou de sous-traitants s'engagent à travers le label à mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment, selon le principe « d'accountability » défini dans le règlement européen.

ANITEC et CNPP préconisent la mise en œuvre des outils de conformité suivants, à mettre en œuvre par les intégrateurs, installateurs et mainteneurs :

- la tenue d'un registre des traitements mis en œuvre,
- la notification de failles de sécurité (aux autorités et personnes concernées),
- la certification de traitements,
- l'adhésion à des codes de conduite,
- la désignation d'un DPO / DPD (Data Protection Officer / Délégué à la Protection des Données) interne, externe, mutualisé,
- la modélisation de l'analyse d'impact relative à la protection des données (AIPD) pour ses activités de sécurité électronique et ses « données sensibles »,
- la cartographie des données.

Le Règlement Européen sur la Protection des Données Personnelles vise à responsabiliser les acteurs des traitements de données en uniformisant les obligations pesant sur les responsables de traitements et les sous-traitants.

ANITEC et ses partenaires par le biais de leurs activités, porteront ces deux piliers :

- L'adhérent ou son représentant qualifié, en qualité de représentant légal est le point de contact de l'autorité. Il a mandat pour « être consulté en complément ou à la place du responsable de traitement sur toutes les questions relatives aux traitements ».
- En qualité de « sous-traitant », l'adhérent est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'accountability. Il a notamment une « obligation de conseil » auprès du responsable de traitement donneur d'ordre, pour la conformité à certaines obligations du règlement (PIA, failles, sécurité, destruction des données, contribution aux audits). Il est tenu de maintenir un registre et de désigner un DPO dans les mêmes conditions qu'un responsable de traitement.

  Selon l'article 37 du RGPD, le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

  a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

  b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées;

  c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

  C'est essentiellement le cas b qui concerne le domaine des installateurs et des intégrateurs en sécurité incendie et sûreté malveillance.

3

OBLIGATIONS DE SÉCURITÉ PAR RAPPORT AUX DIFFÉRENTS SCÉNARIOS

Les mesures à prendre pour assurer la sécurité et la confidentialité des données sont très variables, d'une part, en fonction des équipements/dispositifs concernés et, d'autre part, du niveau de sensibilité et du circuit des données traitées.

Les risques que fait peser un traitement de données personnelles à grande échelle sur les droits et libertés des personnes concernées doivent être évalués. Pour ce faire, doivent notamment être identifiés :

- les sources de risques et leurs capacités (par exemple, un pirate informatique) ;
- les supports des données personnelles (par exemple, une base de données) ;
- les événements redoutés et leurs impacts pour les personnes concernées (par exemple, l'accès illégitime aux données pour leur exploitation) ;
- les menaces et leurs probabilités de survenance (par exemple, l'interception des communications par une attaque de type man in the middle). Celles-ci peuvent toucher l'informatique de gestion de nos entreprises, mais également l'informatique de production installée chez nos clients (systèmes hypervision). L'attaque de type Distributed Denial of Service attack (DDoS) portée sur les produits installés par nos entreprises, comme les caméras de vidéosurveillance IP.

Les risques doivent être caractérisés au regard de leur gravité (l'importance et l'impact des événements redoutés pour les personnes) et de leur vraisemblance (la probabilité de voir une menace se réaliser).

L'identification des facteurs de risques permet de concevoir des mesures adaptées visant à assurer la sécurité et la confidentialité des données.
Il peut, par exemple, s'agir de mesures techniques (authentification, chiffrement, cloisonnement, sécurisation des équipements, etc.) ou de mesures organisationnelles (gestion des habilitations, encadrement de la maintenance, etc.).

3

OBLIGATIONS DE SÉCURITÉ PAR RAPPORT AUX DIFFÉRENTS SCÉNARIOS

CE QUI CHANGE AVEC LE RGPD

Le RGPD prévoit que dans certains cas (en présence de risques élevés pour les personnes, appréciés sur la base de différents critères mentionnés à l'article 35 du RGPD), les responsables des traitements (fournisseurs de produits et services, etc.) ont l'obligation de formaliser l'analyse des risques et la définition des mesures correspondantes à travers une analyse d'impact relative à la protection des données (AIPD) ou privacy impact assessment (« PIA »).

- Pour les entreprises de l'ANITEC spécialisées dans la sécurité électronique ou fournisseurs de systèmes de supervision ou d'hypervision, il est proposé de renforcer l'analyse de risque par l'utilisation du référentiel APSAD D32 CYBERSÉCURITÉ « Document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique ».

- Pour les adhérents domoticiens, il est proposé de suivre la PIA applicable aux objets connectés.

En savoir plus

4 DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

4.1 ANALYSE D'IMPACT :

Délibération n° 2019-118 du 12 septembre 2019 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise (JO du 22 octobre 2019, texte n° 90).

La Commission Nationale Informatique et Libertés (CNIL) à fait paraître le 22 octobre 2019, une liste des opérations de traitement pour lesquelles une analyse d'impact (AIPD) relative à la protection des données n'est pas obligatoire.

Pour rappel et depuis le 25 mai 2018, le RGPD impose d'effectuer une analyse d'impact (AIPD) avant tout traitement à risque élevé pour les droits et libertés des personnes concernées (RGPD, art. 35).

Cette procédure vise à « responsabiliser » les responsables de traitement et les sous-traitants **qui manipulent des données à caractère personnel** et permet de limiter l'obligation de déclaration préalable à l'autorité de contrôle aux seuls traitements susceptibles d'engendrer ces risques élevés.

L'analyse d'impact est également obligatoire dans trois cas (RGPD, art. 35, § 3)

- L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement informatisé (y compris le profilage) et sur la base de laquelle sont prises des décisions produisant des effets juridiques (ressources humaines, marketing).
- Le traitement à grande échelle de catégories particulières de données (RGPD, art. 9, § 1), ou de données à caractère personnel relatives à des condamnations pénales et infractions.
- La surveillance systématique à grande échelle d'une zone accessible au public (vidéosurveillance, vidéoprotection).

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

La liste adoptée par la CNIL se présente sous la forme du tableau présenté en pages 15 et 16 :

La mise en œuvre d'un traitement figurant sur la présente liste ne dispense pas le responsable de traitement du respect de ses autres obligations prévues par le RGPD. Les traitements, même exonérés d'analyse d'impact, doivent faire l'objet d'une évaluation de leur conformité au RGPD tant sur le plan juridique qu'en matière de sécurité.

En cas de doute quant à la nécessité d'effectuer une AIPD il est recommandé d'en effectuer une.

D'autre part, la CNIL indique à ce titre dans sa délibération que, notamment, le fait qu'une activité de traitement relève de cette « liste de dispenses » ne signifie pas qu'un responsable de traitement est exempté des obligations en matière de sécurité du traitement (nécessitant, par exemple, la pseudonymisation ou le chiffrement des données à caractère personnel, RGPD art. 32).

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

TYPES D'OPÉRATIONS DE TRAITEMENT / LISTE ADOPTÉE PAR LA CNIL

Traitements mis en œuvre uniquement à des fins de ressources humaines (gestion du personnel des organismes qui emploient moins de 250 personnes, à l'exception du recours au profilage).	Traitements de gestion de la relation fournisseurs	Traitements destinés à la gestion des activités des comités d'entreprise et d'établissement
Exemples : • la gestion de la paye, l'émission des bulletins de salaire ; • la gestion des formations ; • la gestion du restaurant d'entreprise, la délivrance des chèques repas ; • le remboursement des frais professionnels ; • le suivi des entretiens annuels d'évaluation ; • la tenue des registres obligatoires ; • l'utilisation d'outils de communication (messagerie électronique, téléphonie, vidéoconférences, outils collaboratifs en ligne) sans recours au profilage ni à la biométrie ; • le contrôle du temps de travail (sans dispositif biométrique, sans données sensibles ni à caractère hautement personnel).	**Exemples :** • les opérations administratives liées : aux contrats, aux commandes, aux réceptions, aux factures, aux règlements, à la comptabilité pour ce qui a trait à la gestion des comptes fournisseurs ; • l'établissement des titres de paiement (traites, chèques, billets à ordre...) ; • l'établissement des statistiques financières et de chiffre d'affaires par fournisseur ; • les sélections de fournisseurs pour les besoins de l'entreprise ou de l'organisme ; • l'entretien d'une documentation sur les fournisseurs.	**Exemples :** • la gestion des programmes socio-culturels de l'entreprise, communication interne ; • la formation des élus ; • l'exercice du droit d'alerte de l'article L 2312-59 du Code du travail ; • la gestion des agendas et réunions, la gestion de leurs membres.

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

TYPES D'OPÉRATIONS DE TRAITEMENT / LISTE ADOPTÉE PAR LA CNIL

Traitements mis en œuvre par une association, une fondation ou toute autre institution sans but lucratif pour la gestion de ses membres et de ses donateurs dans le cadre de ses activités habituelles dès lors que les données ne sont pas sensibles.	Traitements mis en œuvre aux seules fins de gestion des contrôles d'accès physiques et des horaires pour le calcul du temps de travail, en dehors de tout dispositif biométrique. À l'exclusion des traitements des données qui révèlent des données sensibles ou à caractère hautement personnel.	Traitements relatifs aux éthylotests, strictement encadrés par un texte et mis en œuvre dans le cadre d'activités de transport aux seules fins d'empêcher les conducteurs de conduire un véhicule sous l'influence de l'alcool ou de stupéfiants.
Exemples : • la gestion administrative des membres et donateurs, en particulier la gestion des cotisations ; • l'établissement pour répondre à des besoins de gestion, des états statistiques ou des listes de membres ou de contacts, notamment en vue d'adresser bulletins, convocations, journaux (les critères retenus devant être objectifs et se fonder uniquement sur des caractéristiques qui correspondent à l'objet statutaire de l'organisme) ; • l'établissement des annuaires de membres, y compris lorsque ces annuaires sont mis à la disposition du public ou sur le réseau internet ; • la réalisation par tout moyen de communication des opérations relatives à des actions de prospection auprès des membres, donateurs et prospects.	**Exemples :** • la mise en place d'un dispositif par badge sans biométrie pour entrer dans les locaux d'un organisme à des fins de sécurité ; • la mise en place d'un dispositif de contrôle du temps de travail effectué par les salariés, à l'exclusion de toute autre finalité.	**Exemples :** • les traitements ayant pour finalité la mise en place d'éthylotests « anti-démarrage » dans des camions de transport.

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

4.2 PERSONNES CONCERNÉES

Sont concernées toute personne physique à laquelle se rattachent directement ou indirectement les données qui sont collectées et traitées.

4.2.1 RESPONSABLE DU TRAITEMENT

Il s'agit de la personne physique ou morale qui détermine les finalités (ce à quoi sert le traitement) ou les moyens (permettant de répondre à cet objectif) d'un traitement de données personnelles.

Le responsable de traitement est tenu de respecter l'ensemble des obligations découlant de la loi « Informatique et Libertés » et du RGPD (notamment l'information et l'éventuel recueil du consentement de la personne concernée, la mise en place de mesures de sécurité adaptées et, le cas échéant, la réalisation des formalités préalables auprès de la CNIL).

CE QUI CHANGE AVEC LE RGPD

Le RGPD prévoit que plusieurs organismes peuvent être conjointement identifiés comme responsables du traitement, lorsqu'ils déterminent ensemble les finalités et/ou les moyens d'un seul et même traitement.

Dans ce cas, ces derniers doivent définir leurs obligations respectives, s'agissant notamment des modalités d'information et d'exercice des droits des personnes (qui pourront les exercer auprès de chaque responsable).

4.2.2 LE DPO (DATA PROTECTION OFFICER)

Il est désigné par le responsable du traitement et a pour mission de conseiller celui-ci sur le RGPD et les exigences qui en découlent, d'être le point de contact entre le responsable de traitement et l'autorité de contrôle ou une personne désirant mettre en application ses droits (droit à la suppression, droit à la portabilité, ...).

CE QUI CHANGE AVEC LE RGPD

La désignation d'un DPO est une des premières étapes à réaliser.

Plusieurs options sont possibles : désigner un DPO en interne, en externe (avocat ou expert par exemple) ou en mutualisant.

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

4.2.3 SOUS-TRAITANT

Nota : La notion de sous-traitant est utilisée ici au sens des exigences RGPD.

Toute personne, organisme ou autorité à qui le responsable du traitement a confié la réalisation de tout ou partie du traitement. Il collecte et traite les données uniquement au nom et pour le compte du responsable du traitement et sur instruction de celui-ci.

Avec la loi « Informatique et Libertés », seule pèse sur le sous-traitant l'obligation d'assurer la sécurité et la confidentialité des données collectées.

CE QUI CHANGE AVEC LE RGPD

Le RGPD renforce les obligations du sous-traitant qui devra également :

- prêter concours au responsable du traitement dans le respect de ses obligations découlant du RGPD (notamment pour la gestion des droits des personnes) en déployant des mesures techniques et organisationnelles appropriées ;
- supprimer ou renvoyer les données qu'il détient au responsable du traitement au terme de la prestation de service ;
- mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de leurs obligations découlant du RGPD ;
- permettre la réalisation d'audits par le responsable du traitement ou un autre auditeur que celui-ci a mandaté ;
- informer immédiatement le responsable du traitement s'il estime qu'une instruction donnée par ce dernier constitue une violation du RGPD ou d'autres dispositions du droit de l'Union européenne ou du droit national relatives à la protection des données ;
- tenir à jour un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement.
- informer immédiatement le responsable du traitement d'une violation de données personnelles.

4.2.4 DESTINATAIRES

Toutes personnes ou organismes habilités à recevoir communication de ces données autres que la personne concernée, le responsable du traitement, le sous-traitant, les personnes qui sont chargées de traiter les données dans le cadre de leurs fonctions et les autorités légalement habilitées.

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

4.3 CONSENTEMENT :

Toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données personnelles la concernant soient traitées.

Il s'agit de l'une des bases juridiques permettant au responsable du traitement de justifier la mise en œuvre d'un traitement de données personnelles (avec, par exemple, le respect d'une obligation légale, la sauvegarde de la vie de la personne concernée, l'exécution d'un contrat ou l'intérêt légitime du responsable de traitement).

Le consentement recueilli doit être spécifique, c'est-à-dire distingué clairement des autres questions posées à la personne concernée, et formulé en des termes clairs et simples afin qu'elle puisse s'engager en pleine connaissance de cause. De plus, il ne doit pas être subordonné à la souscription d'un autre produit ou service.

Précision : Les responsables des traitements doivent par ailleurs veiller à ce que les personnes concernées aient la capacité de consentir. En cas d'incapacité décidée par l'autorité judiciaire, le consentement de leurs représentants légaux pourra être recueilli (les proches dans le cadre d'une habilitation familiale ou les mandataires judiciaires à la protection des majeurs dans le cadre de leur fonction).

Il est donc nécessaire d'adapter les modalités de recueil du consentement en prenant en compte notamment l'état des personnes concernées, la sensibilité des données collectées et le contexte de mise en œuvre du traitement et d'utilisation du service (remplissage d'un formulaire ou d'une case à cocher non précochée, etc.). En tout état de cause, la seule acceptation de conditions générales n'est pas une modalité suffisante.

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

CE QUI CHANGE AVEC LE RGPD

La personne concernée doit pouvoir retirer son consentement aussi facilement qu'elle l'a donné. Ce retrait doit conduire à l'arrêt du traitement et à la suppression des données s'il s'agissait de la base légale sur laquelle il s'appuyait.

Enfin, le RGPD prévoit que le responsable de traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données personnelles la concernant, par tout moyen adapté (lorsqu'il s'agit de la base légale du traitement). La Commission recommande aux responsables des traitements d'anticiper cette nouvelle obligation.

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Droit à la portabilité :

le droit à la portabilité renforce la maîtrise des personnes concernées sur leurs données personnelles. Il crée également de nouvelles opportunités de développement et d'innovation en facilitant le partage de données personnelles, de manière sécurisée et sous le contrôle de la personne concernée.

Plus concrètement, le droit à la portabilité offre aux personnes concernées la possibilité de récupérer les données personnelles les concernant traitées par un organisme, dans un format structuré, couramment utilisé et lisible par machine, pour leur usage personnel afin, notamment, de les stocker sur un appareil ou un cloud privé.

Ce droit permet également aux personnes concernées de transmettre elles-mêmes leurs données d'un système d'information à un autre, par exemple, en vue de leur réutilisation par un autre responsable de traitement.

Lorsque cela est techniquement possible, les personnes concernées peuvent demander que l'organisme qui détient les données les concernant transfère directement ces données à un autre responsable de traitement.

Le droit à la portabilité ne s'applique qu'aux données personnelles fournies activement et consciemment par la personne concernée au responsable de traitement et aux données générées par l'activité de cette dernière lorsqu'elle utilise un produit ou un service.

À l'inverse, les données personnelles qui sont dérivées, calculées ou inférées à partir des données fournies par la personne concernée, telles que le profil d'un utilisateur créé grâce à l'analyse des données d'usage produites par dispositif sont exclues du droit à la portabilité, dans la mesure où elles ne sont pas fournies par la personne concernée, mais créées par l'organisme.
Par ailleurs, le droit à la portabilité ne s'applique que si les données sont traitées de manière automatisée (les fichiers papiers ne sont donc pas concernés).

Enfin, ce droit ne s'applique qu'aux traitements fondés sur le consentement ou nécessaires à l'exécution d'un contrat auquel elle est partie. Il en résulte que les données personnelles traitées sur la seule base de l'intérêt légitime du responsable de traitement ne peuvent faire l'objet d'une demande de portabilité (par exemple, les données traitées à des fins d'optimisation de modèles ou d'amélioration de produits ou logiciels).

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Droit à la limitation du traitement :

ce droit permet aux personnes concernées de limiter les opérations susceptibles d'affecter les données les concernant via leur cantonnement informatique temporaire. Ce cantonnement a pour but d'empêcher l'accès, la modification ou l'effacement des données sélectionnées, principalement, pendant l'examen d'une demande d'exercice d'un droit par la personne concernée ou à des fins probatoires (en particulier, en cas de contestation quant à la licéité d'un traitement, l'exactitude ou la nécessité des données ou la primauté des motifs légitimes du responsable de traitement sur ceux de la personne concernée).

Ainsi « gelées », les données personnelles ne peuvent (à l'exception de leur conservation), être traitées qu'avec le consentement de la personne concernée, pour la constatation, l'exercice ou la défense de droits en justice, pour la protection des droits d'une autre personne physique ou morale ou pour des motifs importants d'intérêt public.

4

DÉFINITION DES NOTIONS ET PRINCIPES CLÉS À RESPECTER AU REGARD DE LA LOI INFORMATIQUE ET LIBERTÉS ET DU RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

4.4 ANONYMISATION ET PSEUDONYMISATION

Opération irréversible conduisant à rompre tout lien d'identification entre les données et la personne concernée. Les mécanismes d'anonymisation doivent être conformes à l'avis du 10 avril 2014 du G29 (ancien regroupement des autorités de protection des données européennes) sur les mécanismes d'anonymisation.

En savoir plus

Les données anonymes ne sont pas soumises à la loi informatique et libertés ni au RGPD. Elles peuvent donc être librement utilisées et transmises et conservées sans limitation de durée.

Tel n'est en revanche pas le cas des données **pseudonymisées**, qui restent des données à caractère personnel, car le procédé est réversible. La pseudonymisation est une technique qui consiste à remplacer des données personnelles directement identifiantes par un pseudonyme non signifiant. Cela peut par exemple être réalisé par le calcul d'une empreinte obtenue par l'utilisation d'un algorithme de hachage à clé secrète. Le recours à la pseudonymisation des données permet d'améliorer la protection de la confidentialité des informations à caractère personnel en réduisant les risques de mesurage.

5

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

5.1 GÉNÉRALITÉS

Elle est obligatoire pour les traitements susceptibles d'engendrer des risques élevés. L'AIPD est un outil important pour la responsabilisation des organismes, elle aide à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité au RGPD.

Elle se décompose en trois parties :

- **Une description détaillée** du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels.
- **L'évaluation de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux** (finalité du système, données et durées de conservation, information et droits des personnes, etc.).
- **L'étude, de nature plus technique, des risques sur la sécurité des données :** critères de confidentialité, intégrité et disponibilité, mais aussi les impacts potentiels sur la vie privée, qui permettent de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

5

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

5.2 DÉFINIR UN RISQUE SUR LA VIE PRIVÉE

Un « risque sur la vie privée » doit être envisagé par l'adhérent comme un scénario décrivant :

- **un événement redouté** (exemple : une atteinte à la confidentialité, à la disponibilité ou à l'intégrité des données, et ses impacts potentiels sur les droits et libertés des personnes) ;
- **toutes les menaces qui permettraient qu'il survienne.**

Il doit être estimé en termes de **gravité** et de **vraisemblance**. La gravité doit être évaluée pour les personnes concernées, et non pour l'organisme.

Exemple : un salarié soudoyé par un concurrent pourrait lui envoyer le fichier des adresses email des clients par courrier électronique. Si cela se produisait, les clients pourraient ensuite être sollicités et avoir un sentiment d'atteinte à la vie privée, des ennuis personnels ou professionnels, etc. Du point de vue « informatique et libertés », ce risque pourrait être estimé comme peu grave (conséquences peu importantes) et très vraisemblable (dans la mesure où ce scénario s'est déjà produit) par l'entreprise.

L'AIPD doit être menée avant la mise en œuvre du traitement. Elle doit être démarrée le plus en amont possible et sera mise à jour tout au long du cycle de vie du traitement. Il est également nécessaire de revoir une AIPD de manière régulière pour s'assurer que le niveau de risque reste acceptable tout au long de la vie du traitement, dans la mesure où l'environnement, technique notamment, sera amené à évoluer, ce qui nécessitera d'adapter les mesures mises en œuvre. L'intégrateur pourrait faire entrer cette mise en œuvre régulière, dans son contrat de maintenance.

Si le donneur d'ordre ou maître d'ouvrage dispose d'un Data Protection Officer (DPO), celui-ci est susceptible de remettre à l'intégrateur un exemplaire de l'analyse d'impact sur la vie privée ou de faire appel à l'intégrateur en qualité de sous-traitant pour l'aider à mettre en œuvre des solutions techniques facilitant la sécurisation d'un système, si celui-ci ne possède pas de sécurité native. Pour les entreprises ne disposant pas de DPO ou dans le cadre du marché résidentiel, l'intégrateur (domoticien) s'assurera de la prise en compte de l'AIPD pour le compte de son donneur d'ordre.

5

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

5.3 QUELLE MÉTHODOLOGIE SUIVRE A MINIMA

Étape 1

- **Délimiter et décrire le contexte** du (des) traitement(s) considéré(s).

Étape 2

- **Analyser les mesures** garantissant le respect des principes fondamentaux : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées.

Étape 3

- **Apprécier les risques** sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités.

Étape 4

- **Formaliser la validation** de l'AIPD au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

5.4 FAUT IL TRANSMETTRE SON ANALYSE D'IMPACT À LA CNIL ?

Il faut transmettre son analyse d'impact à la CNIL dans les situations suivantes :

- s'il apparait que le niveau de risque résiduel reste élevé (cas où la CNIL doit être consultée) ;
- quand la législation nationale d'un État membre l'exige.

Si votre traitement relève de la directive « Police-Justice », votre AIPD doit être transmise à la CNIL dans les cas suivants :

- elle présente des risques résiduels élevés ;
- en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, le traitement présente des risques initiaux élevés.

Vous avez effectué une analyse d'impact mais vous n'êtes pas dans l'un des cas ci-dessus, vous n'avez pas à consulter la CNIL.

Si vous êtes dans un cas justifiant l'envoi de votre analyse d'impact, vous pouvez l'envoyer par internet :

En savoir plus

PIA
vue d'ensemble des obligations et de la méthode

0.
Lancer un nouveau traitement

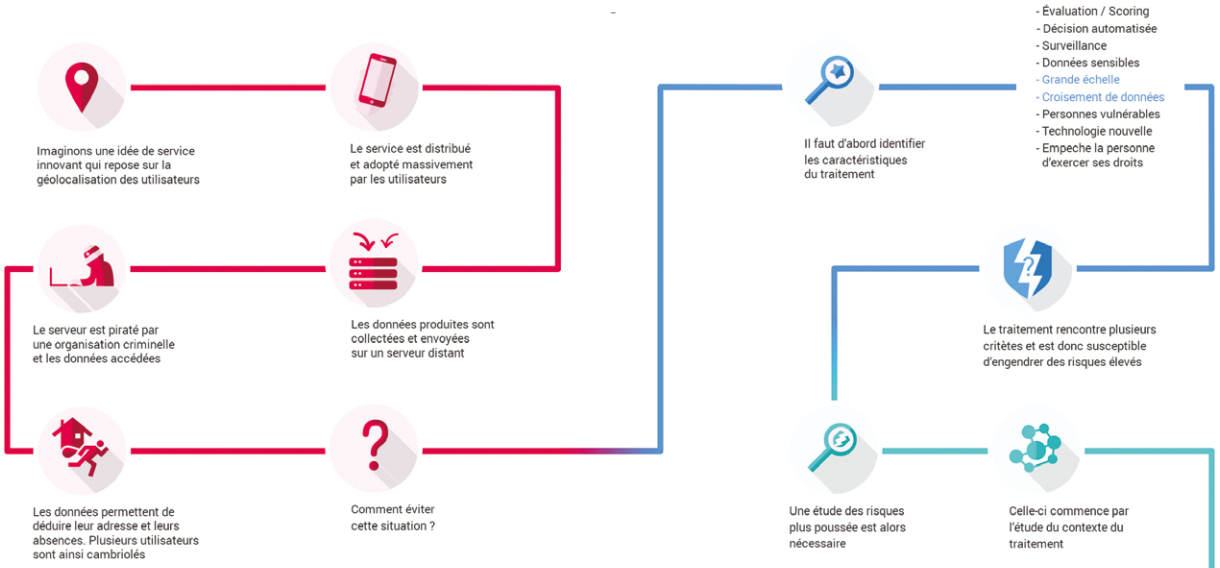
De nombreux services sont créés tous les jours dans le monde du numérique.

Qu'ils répondent aux besoins internes d'organismes ou à ceux de leurs clients, ces services reposent pour la grande majorité sur des traitements de données à caractère personnel.

Adressés à des groupes d'utilisateurs définis, ils collectent ces données à la volée lors de leur usage.

Stockées sur des serveurs, les données collectées sont vulnérables à différents risques : l'accès illégitime, la modification non désirée et la disparition.

Ces risques sont susceptibles d'avoir un impact important sur la vie privée des utilisateurs concernés.



1.
Qualifier le traitement

Ces risques sont indésirables, aussi bien pour le responsable de traitement que pour les utilisateurs du service.

Ainsi, avant de lancer un traitement, il est important d'en faire une première analyse afin d'en déterminer les risques qu'il est susceptible d'engendrer.

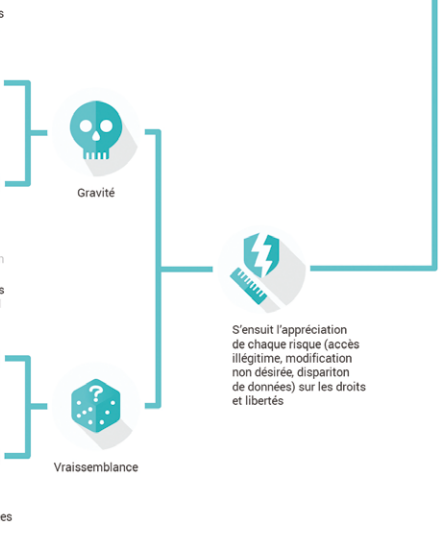
Plusieurs facteurs influencent la dangerosité d'un traitement comme par exemple le type de données traité.

En général, si deux des critères listés sont rencontrés, le traitement comporte probablement des risques importants sur la vie privée. Dans ce cas de figure, il est approprié de mener une *« analyse d'impact relative à la protection des données »*.

2.
Apprécier les risques vie privée

L'analyse établit tout d'abord le contexte dans lequel évolue le traitement, en posant, entre autre, les bases de son rôle et de son fonctionnement.

En complément de l'étude juridique consistant à évaluer la nécessité et la proportionnalité du traitement, il est nécessaire d'analyser chaque risque et d'estimer sa vraisemblance et sa gravité selon les impacts potentiels sur les droits et libertés, les données traitées, les sources de risques, et les vulnérabilités des supports de données.

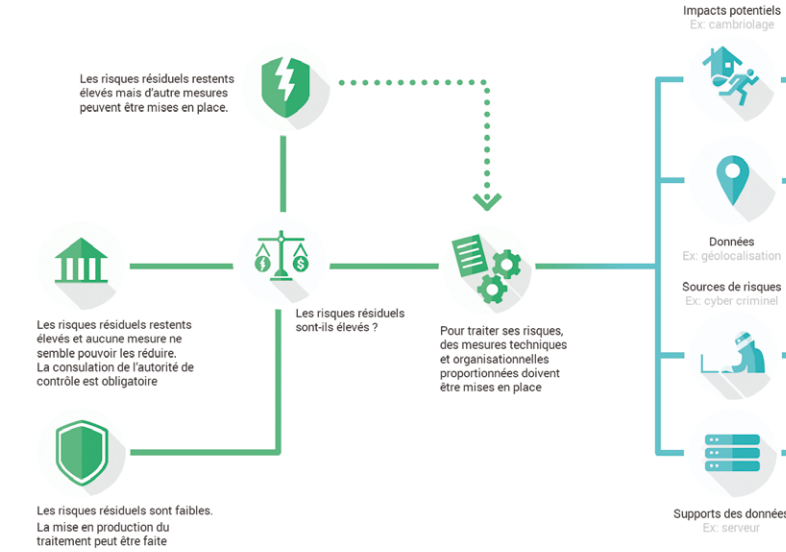


3.
Traiter les risques

Une fois les risques identifiés, des mesures techniques et organisationnelles doivent être déterminées jusqu'à ce que les risques soient réduits à un niveau acceptable.

Si ça ne semble pas possible avec les moyens envisagés, l'autorité de contrôle doit être consultée.

Dans tous les cas, les mesures devront être appliquées avant la mise en œuvre du traitement.



Source : www.cnil.fr

DPIA Data Protection Impact Assessment

Pour plus d'information, la source réglementaire :

Journal officiel de la République française n°0256 du 6 novembre 2018 : délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD). NOR : CNIL1829637X

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

5.5 LES OUTILS ET MÉTHODOLOGIES INDISPENSABLES POUR LES ADHÉRENTS

Le logiciel CNIL AIPD
gratuit

En savoir plus

Le référentiel
APSAD D32

En savoir plus

La méthode EBIOS
RISK MANAGER

En savoir plus

RESPONSABILITÉS DE L'INTÉGRATEUR ET RGPD

Un des objectifs poursuivis par le RGPD est de responsabiliser les acteurs traitant des données et de renforcer la régulation.

La violation du RGPD peut exposer ses auteurs à un risque de plainte auprès de la CNIL ou d'un tribunal réputé compétent en matière civile pour le préjudice subi mais aussi en matière pénale en cas d'infraction (art. 226-16 et suivants du Code pénal notamment). L'art. 32 du RGPD précise que les garanties de sécurité du traitement sont assujetties à « l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités de traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques ».

L'art. 32 précise également que le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque selon les besoins.

L'obligation de moyens est une suite de dispositions à suivre scrupuleusement. L'obligation de résultat définit des performances ou des objectifs à atteindre, les moyens étant laissés à la libre disposition du responsable de traitement des données. Cet article nous laisse à penser que si ce n'est une obligation de résultat qui est attendue, c'est a minima une obligation de moyens renforcée. Le principe d'accountability pourrait faire pencher la balance des tribunaux de justice vers une obligation de résultat.

En premier lieu, identifions les différents types de responsabilités qui pourraient être engagées pour les installateurs mainteneurs.

RESPONSABILITÉS DE L'INTÉGRATEUR ET RGPD

6.1 RESPONSABILITÉ CIVILE

La responsabilité civile régit les rapports des citoyens entre eux et a pour principal objet la réparation des dommages. Notons qu'en matière civile, il est généralement possible de s'assurer (rc pro) et que les assureurs proposent désormais la souscription de contrats spécifiques en matière de cyber risques. Nous ne pouvons que vous conseiller de vous rapprocher à ce sujet de votre apériteur.

On distingue différents types de responsabilité civile :

- **la responsabilité civile contractuelle :** elle découle de tous les contrats comportant une obligation de livrer une chose, de faire ou de ne pas faire, mais non des contrats ayant pour objet unique le paiement d'une somme. Le RGPD implique dès lors qu'il y a un contrat, que l'intégrateur et son sous-traitant satisfassent à leurs obligations règlementaires.

- **la responsabilité civile extracontractuelle :** elle découle d'un fait dommageable intentionnel ou volontaire.

6 RESPONSABILITÉS DE L'INTÉGRATEUR ET RGPD

6.1.1 EN MATIÈRE DE RESPONSABILITÉ CIVILE CONTRACTUELLE, LA JURISPRUDENCE IDENTIFIE DES OBLIGATIONS COMPLÉMENTAIRES À PRENDRE EN COMPTE :

L'obligation de sécurité :

L'exécution normale de la prestation contractuelle ne doit pas donner lieu à des dommages, notamment sur la personne.
Cette approche est notamment consacrée dans le domaine de la sécurité des produits, de la responsabilité du fait des produits défectueux.

L'obligation de renseignement et de conseil :

- La cour de cassation exige que le professionnel, installateur ou mainteneur, rapporte la preuve qu'il a bien satisfait à cette obligation (Cass.1ère civ 25 fév.1997).
- Le devoir de conseil correspond à des recommandations, orientations de choix, préconisations en fonction de la réglementation applicable, en adéquation avec les risques et adaptée aux besoins exprimés par le client.
- Il s'agit d'une obligation de moyens, qui peut être tempérée par le niveau de compétence du client BtoB.
- Le client, pour sa part, dispose d'une obligation de coopération : se renseigner, poser les questions nécessaires, s'impliquer activement en interrogeant le fournisseur sur les éléments qui peuvent lui échapper.
- Il n'appartient pas au fournisseur de s'immiscer dans des considérations de rentabilité.
- La traçabilité est primordiale (écrits notamment).
- L'installateur intégrateur doit s'assurer que l'installation est compatible avec la réglementation en vigueur.
- Il se doit également de respecter les règles de l'art (APSAD, DTU, normes ...), définies comme l'état de la technique au moment de la réalisation de l'ouvrage autrement dit de démontrer l'application des bonnes pratiques professionnelles à respecter pour obtenir le résultat jurisprudentiel.
- Le caractère évolutif des règles de l'art fait qu'il n'y en a pas de définition figée donc récurrente du devoir de conseil. Les bonnes pratiques en matière de RGPD sont ici indiquées à titre d'exemple et ne peuvent pas constituer une liste figée et exhaustive.
- Selon une jurisprudence constante, tout intervenant à une opération de construction est tenu dès le début de l'opération et jusqu'à la réception des travaux d'une obligation de conseil.

  - **Avant le début des travaux :** il doit mettre en garde sur les risques ou insuffisances du projet par rapport à sa finalité, son coût. Il doit veiller au respect des règlementations en vigueur.
  - **Pendant les travaux :** il doit informer sur les erreurs ou omissions constatées, sur les problèmes d'interface entre corps d'état.
  - **À la réception :** le maître d'œuvre doit conseiller le maître d'ouvrage et l'aider à faire des réserves si nécessaire.
    L'entrepreneur doit informer par écrit sur la nécessité d'entretenir les ouvrages, leurs équipements et sur le bon usage des équipements.

RESPONSABILITÉS DE L'INTÉGRATEUR ET RGPD

6.1.2 RESPONSABILITÉ CIVILE LIÉE AUX VICES CACHÉS

La responsabilité civile garantie des vices cachés a pour fondement : l'art.1641 du Code civil « le vendeur est tenu de la garantie à raison des défauts cachés de la chose vendue qui la rendent impropre à l'usage auquel on la destine ou qui diminuent tellement cet usage que l'acheteur ne l'aurait pas acquise, ou n'en aurait donné qu'un moindre prix s'il les avait connus ».

Cela revient donc ici à une obligation de garantie, pour peu que les trois conditions suivantes soient respectées :

- il doit s'agir d'un contrat de vente,
- le vice doit exister à la livraison ou au transfert de propriété,
- le vice doit rendre la chose impropre à son usage normal.

6.1.3 RESPONSABILITÉ CIVILE LIÉE AUX PRODUITS

La responsabilité civile de droit commun pour non-conformité du produit a pour fondement : les art.1604 et 1615 du Code civil prévoient une étendue de l'obligation du vendeur au fait qu'il doit livrer la chose même qui a été vendue. C'est ici à l'acheteur qui conteste d'en établir la réalité. On peut penser que le fait de ne pas respecter les obligations liées au RGPD pourrait être constitutif de la non-conformité du produit.

RESPONSABILITÉS DE L'INTÉGRATEUR ET RGPD

6.1.4 RESPONSABILITÉ CIVILE PRÉCONTRACTUELLE

L'ordonnance 2016-131 du 10 février 2016 (en vigueur depuis le 1er octobre 2016) a pour objectifs :

- d'accroître la lisibilité des contrats,
- de mieux appréhender les étapes de la vie du contrat,
- de définir les notions de l'obligation de bonne foi au devoir d'information,
- d'accomplir leurs propres obligations de bonne foi.

L'obligation d'informer (Art. 1112-1 du Code civil) : celle des parties qui connaît une information dont l'importance est déterminante pour le consentement de l'autre doit l'en informer dès lors que, légitimement, cette dernière ignore cette information ou fait confiance à son cocontractant.

- Ont une importance déterminante les informations qui ont un lien direct et nécessaire avec le contenu du contrat ou la qualité des parties.
- Il incombe à celui qui prétend qu'une information lui était due de prouver que l'autre partie la lui devait, à charge pour cette autre partie de prouver qu'elle l'a fournie.
- Les parties ne peuvent ni limiter, ni exclure ce devoir.
- Outre la responsabilité de celui qui en était tenu, le manquement à ce devoir d'information peut notamment entraîner l'annulation du contrat dans les conditions prévues aux articles 1130 et suivants.

Dans ce cadre, le RGPD a notamment pour objet d'imposer aux professionnels (dont les intégrateurs installateurs mainteneurs font partie) d'assurer la sécurité des données à caractère personnel qu'ils traitent ; il s'agit bien ici d'une obligation de sécurité qui s'applique d'une part, tout au long de la chaîne de traitement des données, qu'il s'agisse du responsable du traitement ou de ses sous-traitants, et d'autre part tout au long des différentes phases de la vie des données considérées (de leur collecte à leur destruction).

L'obligation de mise en garde et d'alerte :

Elle peut être définie comme étant l'obligation d'évaluer la compétence professionnelle de son client au regard de sa maîtrise des opérations envisagées et des risques que ces opérations comportent.

Le métier d'intégrateur, installateur, mainteneur intègre cette notion par l'obligation d'alerter son client sur les contraintes et risques associés au traitement des données. Une vigilance accrue doit être apportée par l'installateur sur le contenu du cahier des charges du client en la matière.

En cas de prise en main ou maintenance à distance du système de sécurité ou de sûreté mis en place par l'installateur/ mainteneur, ce dernier doit informer son client des risques relatifs à ces actions (prise de connaissances de données personnelles notamment). Ce devoir de mise en garde et d'alerte doit bien évidemment être tracé et matérialisé, par exemple par la fourniture d'un livret client.

RESPONSABILITÉS DE L'INTÉGRATEUR ET RGPD

6.2 RESPONSABILITÉ PÉNALE

La responsabilité pénale est la responsabilité qui régit les règles à l'encontre de la société.

Elle vise à réprimer les troubles à l'ordre social. Le droit pénal repose notamment sur le principe de la personnalité des peines, selon lequel seul l'auteur matériel des faits incriminés peut être sanctionné, sauf délégation de pouvoirs. En matière de RGPD, ce principe s'appliquerait en premier lieu aux responsables du traitement des données.

Le RGPD implique de nombreuses obligations, en particulier, la désignation dans certains cas d'un DPO, l'établissement d'un registre d'activité des traitements de données personnelles, la notification des failles de sécurité à l'autorité de contrôle et aux victimes, l'analyse d'impact relative aux données personnelles (dans certains cas), etc. L'ensemble de ces actions doit pouvoir être tracé, faute de quoi les infractions prévues dans le cadre de la règlementation « informatique et libertés » pourraient se voir appliquées par les tribunaux répressifs.

RESPONSABILITÉS DE L'INTÉGRATEUR ET RGPD

6.2 Responsabilité pénale

Voici un rappel de ces principales infractions :

Article du Code pénal	Infraction	Exemple concernant les technologies de sûreté	Quelques actions à mettre en œuvre pour prévenir le risque	Peine encourue
226-1	Atteinte à l'intimité de la vie privée.	Piratage de caméras donnant sur la voie publique.	· Chiffrement. · Pseudonymisation. · Anonymisation des données.	· 1 an d'emprisonnement. · 45 000€ d'amende.
226-16	Défaut de respect des formalités préalables.	Négligence dans la nomination d'un DPO ou manque de rigueur d'une analyse d'impact relative à la protection des données.	· Nomination d'un DPO. · AIPD mise à jour.	· 5 ans d'emprisonnement. · 300 000 € d'amende.
226-16-1	Défaut de mise en place de mesures de sécurité prescrites et proportionnées au risque.	-	· Mise en œuvre de matériels dont la robustesse aux attaques numériques est certifiée (ex A2P@).	
226-18	Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite.	Piratage d'un système vidéo et divulgation publique des données collectées.	· Respect du devoir d'information et du devoir d'alerte auprès du client. · Pseudonymisation. · Chiffrement des données. · Limitation des données aux seules personnes habilitées.	

RESPONSABILITÉS DE L'INTÉGRATEUR ET RGPD

6.2 Responsabilité pénale

Voici un rappel de ces principales infractions :

Article du Code pénal	Infraction	Exemple concernant les technologies de sûreté	Quelques actions à mettre en œuvre pour prévenir le risque	Peine encourue
226-19	Conservation de données sensibles sans le consentement de la personne concernée.	-	· Mise en place d'une collecte et conservation fondée sur une démarche opt-in. · Démarche d'accountability (traçabilité du respect effectif du RGPD à tout moment).	· 5 ans d'emprisonnement. · 300 000 € d'amende.
226-21	Détournement des finalités du traitement.	Cyber attaque ayant pour conséquence la perte de confidentialité d'informations sensibles ou perte d'intégrité des données.	· Démarche d'accountability (traçabilité du respect effectif du RGPD à tout moment). · Limitation des données aux seules personnes habilitées.	
226-22	Divulgation de données portant atteinte à la vie privée de la personne.	Mise en œuvre d'un réseau privé virtuel (VPN) par l'exploitant.	Limitation des données aux seules personnes habilitées.	

CONCLUSION

L'**ANITEC** a été la première organisation à comprendre l'enjeu considérable pour nos entreprises et nos métiers que représentait l'arrivée du RGPD. C'est pourquoi, nous avons rédigé le premier guide sur ce sujet.

Depuis sa démocratisation, nos entreprises se sont emparées du sujet pour se mettre en conformité et veiller à la sécurisation des données des installations qu'elles intègrent chez leurs clients particuliers ou professionnels.

Il nous a donc paru évident, qu'il fallait rédiger un livre blanc des bonnes pratiques pour accompagner toutes les entreprises dans cette nouvelle exigence.
En effet, la particularité du RGPD est qu'il s'applique tant en interne dans l'organisation de l'entreprise et la protection des données qu'elle détient, que dans ses activités auprès de ses clients.

Cet ouvrage servira de base au futur label **ANITEC** avec **CNPP**, qui permettra à nos entreprises de faire reconnaître leur professionnalisme auprès des donneurs d'ordres et répondre ainsi à la demande du marché.

Le comité de rédaction ANITEC,
Les présidents Philippe BLIN et Arnaud BROUQUIER,
La vice-présidente Claire JACQUEMET.

FICHE MÉMO 1 :
GESTION DES DONNÉES CLIENT

GÉNÉRALITÉS

- **Périmètre :**
  - Mesures applicables à tout prestataire de service d'installation pour la protection des données relatives à ses clients (données contractuelles, données techniques concernant la réalisation de l'installation etc.).
- **Exemples de finalités :**
  - Conservation de l'historique client / conservation des paramétrages initiaux des systèmes déployés.
- **Quelles obligations au regard de la loi informatique et libertés et du RGPD ?**
  - Réalisation de l'Analyse d'Impact relative à la Protection des Données (AIPD).
- **Données collectées :**
  - **Données statiques :** coordonnées clients y compris coordonnées bancaires / analyse de risque et plans d'installations / configuration initiale y compris identifiants et mots de passe par défaut.
  - **Données dynamiques** : identifiants et mots de passe permettant l'accès administrateur au système, le cas échéant.
- **Durées de conservation :**
  - À définir contractuellement entre le prestataire d'installation et son client.
- **Destinataires :**
  - Le client, en cas de demande (exemple : oubli de ses identifiants de connexion).
- **Information et droits des personnes :**
  - Le client doit être contractuellement informé du caractère des données conservées.
- **Formalités préalables :**
  - Aucune.

MESURES DE SECURITÉ

- **Mise en place d'une politique de sécurité de l'information** applicable au prestataire d'installation.
- **Définition d'une organisation de la sécurité de l'information** avec mise en évidence de l'ensemble des collaborateurs et matériels concernés chez le prestataire d'installation.
- **Gestion de la sécurité relative aux ressources humaines** (mesures avant embauche / après rupture de contrat à établir).
- **Mode de gestion des données** (suivi / classification…).
- **Contrôle des accès logiques et physiques** aux données stockées.
- **Mesures cryptographiques.**
- **Sécurité physique et environnementale.**
- **Sécurité liée à l'exploitation du système d'information du prestataire d'installation** (procédures / surveillance / audit…).
- **Sécurité des communications.**
- **Relations avec les fournisseurs.**
- **Gestion des incidents liés à la sécurité de l'information.**
- **Aspects de la sécurité de l'information** dans la gestion de continuité d'activité.

FICHE MÉMO 2 :
DONNEES GÉNÉRÉES PAR L'INSTALLATION

GÉNÉRALITÉS

- **Périmètre :**
  - Mesures applicables au prestataire d'installation dans le cadre du déploiement d'une installation chez un client.
- **Exemples de finalités :**
  - Extraction locale des données générées par l'installation pour preuve en cas d'incident.
  - Utilisation locale des données pour signalement des pannes.
- **Quelles obligations au regard de la loi informatique et libertés et du RGPD ?**
  - Réalisation de l'Analyse d'Impact relative à la Protection des Données (AIPD).
- **Données collectées :**
  - Historique de connexions aux systèmes déployés.
  - Historique des conditions d'alarmes et de défauts générés par les systèmes déployés.
  - Images issues d'un système de vidéosurveillance.
  - Données concernant les accès au site.
- **Durées de conservation :**
  - À définir contractuellement.
  - Cas de la vidéosurveillance : durée légale de conservation des images, 30 jours maximum voire moins si les caméras sont sur un espace ouvert au public (délai défini lors de l'autorisation préfectorale).
- **Destinataires :**
  - L'exploitant par consultation locale.
- **Information et droits des personnes :**
  - Le client doit être contractuellement informé du caractère des données conservées.
- **Formalités préalables :**
  - Déclaration à la CNIL (cas de la vidéosurveillance).

MESURES DE SECURITÉ

- **Proposition par le prestataire d'installation d'une politique de sécurité de l'information** applicable chez le client du prestataire d'installation.
- **Sensibilisation du client à la gestion des données** générées par l'installation.
- **Mise en place d'un contrôle d'accès aux données** cohérent avec le niveau de sûreté client.
- **Proposition de mesures cryptographiques cohérentes :**
  - Respect du chapitre 4 du référentiel APSAD D32, notamment au niveau du choix des produits : les mesures de protection de la confidentialité, de l'intégrité et de la disponibilité des données doivent être cohérentes avec l'analyse des besoins et des risques.
  - Les données générées par l'installation et extraites du système installé doivent être chiffrées et leur intégrité protégée.
- **Conseils pour la sécurité physique et environnementale.**
- **Proposition d'une procédure pour l'exploitation des données** générées par le système.
- **Mise en place d'une sécurité des communications** cohérente avec le déploiement.
- **Proposition d'une méthode de gestion des incidents** liés à la sécurité de l'information.
- **Aspects de la sécurité de l'information** dans la gestion de continuité d'activité.

FICHE MÉMO 3 :
DONNÉES COMMUNIQUÉES À L'EXTÉRIEUR

GÉNÉRALITÉS

- **Périmètre :**
  - Mesures applicables au prestataire réalisant l'installation pour la sécurité du transport des données.
  - Mesures applicables au prestataire recevant et exploitant des données (ex : télésurveilleur).
- **Exemples de finalités :**
  - Extraction à distance des données générées par l'installation pour intervention ou pour preuve en cas d'incident.
  - Utilisation à distance des données pour signalement des pannes.
- **Quelles obligations au regard de la loi informatique et libertés et du RGPD ?**
  - Réalisation de l'Analyse d'Impact relative à la Protection des Données (AIPD).
- **Données collectées :**
  - Enregistrements des connexions aux systèmes déployés.
  - Conditions d'alarmes et de défauts générés par les systèmes déployés.
  - Images issues d'un système de vidéosurveillance.
  - Données concernant les accès au site.
- **Durées de conservation :**
  - À définir contractuellement.
  - Cas de la vidéosurveillance : durée légale de conservation des images, 30 jours maximum voire moins si les caméras sont sur un espace ouvert au public (délai défini lors de l'autorisation préfectorale).
- **Destinataires :**
  - Le prestataire exploitant à distance (ex : télésurveilleur).
- **Information et droits des personnes :**
  - Le client doit être contractuellement informé du caractère des données collectées par le prestataire exploitant.
- **Formalités préalables :**
  - Déclaration à la CNIL (cas de la vidéosurveillance).

MESURES DE SECURITÉ

Pour le prestataire réalisant l'installation :

- Proposition de mesures cryptographiques cohérentes :
  - Respect du chapitre 4 du référentiel APSAD D32, notamment au niveau du choix des produits : les mesures de protection de la confidentialité, de l'intégrité et de la disponibilité des données doivent être cohérentes avec l'analyse des besoins et des risques.
  - Formalisation des options retenues pour aider à un choix cohérent d'un prestataire recevant et exploitant les données, au regard de l'analyse des besoins et des risques.
  - Les données générées par l'installation, extraites du système installé et envoyées au télésurveilleur doivent être chiffrées et leur intégrité protégée.

Pour le prestataire recevant et exploitant les informations :

- Mise en place d'une politique de sécurité de l'information applicable chez le prestataire recevant et exploitant des données.
- Définition d'une organisation de la sécurité de l'information avec mise en évidence de l'ensemble des interlocuteurs et matériels concernés.
- Mise en place d'une sécurité des données liée aux ressources humaines (recrutement / formation continue / fin de contrat).
- Mise en œuvre de principes de gestion des données (suivi / classification...).
- Contrôle des accès logiques et physiques aux données.
- Mesures cryptographiques pour le stockage des données.
- Sécurité physique et environnementale.
- Sécurité liée à l'exploitation (procédures / surveillance / audit...).
- Sécurité des communications.
- Relations avec les fournisseurs.
- Gestion des incidents liés à la sécurité de l'information.
- Aspects de la sécurité de l'information dans la gestion de continuité d'activité.

FICHE MÉMO 4 :
DONNÉES ACCESSIBLES LORS DES OPÉRATIONS DE MAINTENANCE

GÉNÉRALITÉS

- **Périmètre :**
  - Mesures applicables au prestataire de maintenance des installations (qui peut être différent de l'intégrateur).
- **Exemples de finalités :**
  - Utilisation à distance des données de signalement de pannes pour envisager les actions de maintenance corrective.
- **Quelles obligations au regard de la loi informatique et libertés et du RGPD ?**
  - Réalisation de l'Analyse d'Impact relative à la Protection des Données (AIPD).
- **Données collectées :**
  - Données de connexion aux systèmes déployés.
  - Conditions de défauts générés par les systèmes déployés.
- **Durées de conservation :**
  - À définir contractuellement avec le prestataire de maintenance.
- **Destinataires :**
  - Le prestataire de maintenance (intégrateur ou tiers).
- **Information et droits des personnes :**
  - Le client doit être contractuellement informé du caractère des données transmises au prestataire de maintenance.
- **Formalités préalables :**
  - Aucune.

MESURES DE SECURITÉ

- **Mise en place d'une politique de sécurité de l'information** applicable chez le prestataire recevant et exploitant des données.
- **Définition d'une organisation de la sécurité de l'information** avec mise en évidence de l'ensemble des interlocuteurs et matériels concernés.
- **Mise en place d'une sécurité des données liée aux ressources humaines** (recrutement / formation continue / fin de contrat).
- **Mise en œuvre de principes de gestion des données** (suivi / classification...).
- **Contrôle des accès logiques et physiques aux données.**
- **Mesures cryptographiques pour le stockage des données.**
- **Sécurité physique et environnementale.**
- **Sécurité liée à l'exploitation** (procédures / surveillance / audit...).
- **Sécurité des communications.**
- **Relations avec les fournisseurs.**
- **Gestion des incidents liés à la sécurité de l'information.**
- **Aspects de la sécurité de l'information** dans la gestion de continuité d'activité.

AUTEURS :

Lilian CAULE
Directeur technique ANITEC

Nathalie LABEYS
Ingénieur certification, CNPP Cert.

Sébastien SAMUELI
Directeur des relations publiques, CNPP

RELECTEURS :

Stéphanie TUCOULET
Secrétaire général, ANITEC

Morgane DARMON
Consultant expert assistance règlementaire, CNPP

CNPP

Prévention et maîtrise des risques

Route de la Chapelle Réanville
CD 64 - CS 22265 - F 27950 SAINT-MARCEL

02 32 53 64 00
marketing@cnpp.com www.cnpp.com

ANITEC
ALLIANCE NATIONALE DES INTÉGRATEURS DE TECHNOLOGIES CONNECTÉES, SÉCURISÉES ET PILOTÉES

Alliance Nationale des Intégrateurs
de Technologies connectées, sécurisées et pilotées

5, rue de l'Amiral Hamelin - 75116 PARIS

01 44 05 84 40
contact@anitec.fr www.anitec.fr