Connect Wave

LA RÉFÉRENCE DES OBJETS CONNECTÉS PROFESSIONNELS

IDO PRIVACY

GUIDE D'IMPLÉMENTATION DU RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES DANS LES APPLICATIONS DES OBJETS CONNECTÉS PROFESSIONNELS.

AVEC LE SOUTIEN DE :

DGE

Document préparé par le comité éditorial composé de :

Hichem Bourak (NG Horizons)
Sophie Chabridon (Télécom SudParis)
Pierre Crégo (Mercury Technologies)
Stéphane Guilloteau (Orange)
Laurent Inquiété (Oxelar)
Nathalie Launay (Consultant experte NTIC et DPO)
Jean François Menier (Elyos Avocats)
Claude Tételin (Connectwave)

À PROPOS DE CONNECTWAVE

Fort de 9 ans d'expertise dans les technologies digitales, Connectwave est un acteur majeur dans la promotion et le développement de solutions IoT. Il soutient les PME, startups et grands groupes dans la mise en œuvre de solutions digitales notamment par la mise en œuvre de projets IoT, l'organisation de journées Open Innovation et de formations IoT/RFID, l'accompagnement à la protection des données personnelles, la réalisation d'objets connectés et le développement business.

Reconnu pour son expertise et sa neutralité, il fédère 140 acteurs nationaux et internationaux engagés dans la transformation digitale. Véritable référence des Objets Connectés Professionnels, Connectwave est impliqué dans les comités de standardisation nationaux (AFNOR) et internationaux (ISO, CEN, ETSI) ainsi que dans la solution Objet Intelligent de la Nouvelle France Industrielle.

En collaboration avec Euroméditerranée et Aix-Marseille French Tech, Connectwave a créé un espace d'immersion dans les Objets Connectés situé en plein cœur du quartier d'affaires de Marseille dans un espace appelé « la Coque ».

Contact : **contact@connectwave.fr - www.connectwave.fr - Tél : 04 42 37 09 37**

TABLE DES MATIÈRES

TABLE DES MATIÈRES

ACRONYMES

FRANÇAIS

- ANSSI : Agence Nationale de Sécurité des Systèmes d'Information
- CNIL : Commission Nationale Informatique et Libertés
- DCP : Données à Caractère Personnel
- DPD : Délégué à la Protection des Données (voir DPO)
- DSI : Direction des Services Informatiques
- EIVP : Evaluation d'Impact sur la Vie Privée ou analyse d'impact relative à la protection des données (voir PIA, DPIA)
- IdO : Internet des Objets (voir IoT)
- OIV : Opérateur d'Importance Vitale
- PbD : Privacy by Design, respect de la vie privée dès la conception
- RFID : Identification par Radio Fréquences
- R.G.P.D. : Règlement Général sur la Protection des Données[1] (voir GDPR)
- RH : Ressources Humaines
- RT : Responsable de Traitement (voir DC)
- ST : Sous-traitant (voir DP)

ANGLAIS

- ANSSI : French National Cybersecurity Agency
- DC : Data Controller (voir RT)
- DP : Data Processor (voir ST)
- DPIA : Data Protection Impact Assessment
- DPO : Data Protection Officer (voir DPD)
- GDPR : General Data Protection Regulation (voir R.G.P.D.)
- IoT : Internet of Things (voir IdO)
- PbD : Privacy by Design
- PET : Privacy Enhancing Technologies
- PIA : Privacy Impact Assessment (voir EIVP)
- RFID : Radio Frequency Identification

[1] *http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679*

AVANT-PROPOS

Avec l'entrée en vigueur des sanctions prévues par le Règlement Général sur la Protection des Données (R.G.P.D.) en mai 2018, bon nombre d'acteurs, notamment des PME, se posent la question de sa mise en pratique.

Quels sont les grands principes de ce nouveau règlement ? Comment mettre en place les bonnes pratiques qui aideront à prouver la conformité des traitements de données déployés dans le cadre, notamment, des applications de l'Internet des Objets ?

Si la majeure partie des grandes sociétés disposent des ressources nécessaires à la mise en place d'une politique de protection des données conforme au règlement, les petites et moyennes entreprises, voire les start-up, sont souvent démunies face à ce challenge technico-juridico-organisationnel. C'est la raison pour laquelle, Connectwave, avec l'appui financier de la Direction Générale des Entreprises du Ministères de l'Économie et des Finances, a mis en place un groupe de travail appelé « IdO Privacy ». Ce groupe rassemble plus de 40 experts couvrant les domaines techniques, organisationnels et juridiques en lien avec la protection des données et de la vie privée dans le but de réaliser un guide de bonnes pratiques.

L'objectif de ce guide est de sensibiliser et d'aider les chefs d'entreprises et chefs de projet IoT à prendre en compte la protection des données personnelles et de présenter des bonnes pratiques à l'intention de tous les acteurs qui souhaitent rapidement comprendre les enjeux du R.G.P.D.

Ce guide apporte les informations essentielles sur les principes de protection des données personnelles dès la conception. Il permet aux chefs de projet une mise en pratique opérationnelle. Des exemples permettent d'illustrer les bonnes pratiques à respecter et les réflexes ou points de vigilance à adopter.

En effet, parmi les nouveaux objectifs fixés par le règlement R.G.P.D., l'article 25 est dédié à la protection des données dès la conception et par défaut, ou « data protection by design and by default » qui exige en conséquence la mise en place de mesures techniques et organisationnelles appropriées en amont de la mise en œuvre du traitement.

Il nous paraît important de rappeler que l'entreprise qui collecte et traite des données personnelles doit protéger ces données, de bout en bout, lesquelles sont et restent la propriété de l'utilisateur ou du client, dont l'entreprise n'est que le dépositaire, l'utilisatrice et qu'à ce titre elle en est le plus souvent la gardienne et non le propriétaire ; le droit à la portabilité[2] - nouveau droit reconnu par le Règlement Général sur la Protection des Données Personnelles aux personnes concernées - en est l'illustration même.

Le R.G.P.D. pourrait être considéré comme une contrainte égale supplémentaire. Il est en réalité une formidable opportunité de développement, un moyen de sécuriser le patrimoine informationnel de l'entreprise, un critère marketing de conformité et un atout commercial concurrentiel et un facteur de confiance des consommateurs.

[2] Droit reconnu à la personne de récupérer tout ou partie de ses données afin de les transmettre facilement d'un système d'information à un autre, en vue de leur réutilisation à des fins personnelles.

1

GRANDS PRINCIPES DU R.G.P.D.

Le R.G.P.D. constitue un cadre législatif « garde-fou » de la protection des données personnelles, afin de protéger les individus contre une exploitation illégitime ou abusive de leurs données personnelles. Il reconnaît néanmoins la valeur économique de ces données et tend à encadrer leur libre circulation dans le contexte d'un marché économique du numérique[3]. La Commission européenne a récemment mis en ligne une page web qui présente les grands principes du R.G.P.D. sous forme de FAQ (Frequently Asked Questions)[4]. Le lecteur peut s'y référer pour compléter certains points abordés dans ce guide.

1.1 - RAPPEL DU CADRE LÉGISLATIF EUROPÉEN

Jusqu'à présent, les outils du cadre législatif européen en matière de protection des données, s'appuyaient sur un ensemble de directives. A partir du 25 mai 2018, le nouveau règlement R.G.P.D. s'appliquera directement dans tous les États membres sans qu'une transposition en droit national soit nécessaire.

Il pourra être complété par d'autres règlements et directives communautaires ou encore des lois nationales, telles que la loi Informatique et Libertés II actuellement en préparation.

Se pose alors la question d'un éventuel effet rétroactif sur des traitements de données personnelles mis en place avant le 25 mai 2018. La CNIL, propose sur son site[5] une réponse assez claire à cette question.

Le Règlement prévoit la suppression quasi-totale des formalités préalables à accomplir auprès de la CNIL.

La loi française pourra toutefois prévoir un cadre spécifique pour certaines données sensibles (données biométriques, de santé, sur l'origine ou les appartenances politiques, religieuses, la santé et la vie sexuelle), ou traitements répondant à des missions d'intérêt public (par exemple pour la protection sociale ou la santé publique) ou encore pour les situations particulières de traitement (numéro de sécurité sociale, relations de travail).

Les traitements pour lesquels des formalités ont déjà été régulièrement effectuées auprès de la CNIL (déclarations, autorisations accordées et avis rendus) avant le 25 mai 2018 pourront être poursuivis après cette date sans devoir faire l'objet d'une éventuelle étude d'impact sur la vie privée tant qu'ils ne seront pas modifiés de façon substantielle[6].

A savoir : il ne sera pas nécessaire d'adresser à la CNIL une demande de suppression de ces formalités déjà accomplies !

Attention ! Même si vous n'avez pas à effectuer d'étude d'impact sur la vie privée pour vos fichiers déjà déclarés à la CNIL, les nouvelles obligations prévues par le Règlement européen seront applicables. Vous devrez les respecter et veiller au respect des droits des personnes fichées.

[3] Ce document fait référence à de nombreux articles du R.G.P.D.. Nous invitons les lecteurs à en prendre connaissance sans oublier l'ensemble des considérants.
http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

[4] https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/reform/rules-business-and-organisations_fr

[5] https://www.cnil.fr/cnil-direct/question/1255?visiteur=part

[6] Le projet de révision de Loi Informatique et liberté garantirait au moins pour 10 ans les documents de la CNIL tels que les Normes Simplifiée (NS) et AU (Autorisations Uniques) pour lesquelles les entreprises auraient déjà effectué des engagements de conformité. D'autre part, le R.G.P.D. ne requiert pas de nouvelle étude d'impact pour des traitements anciens conformes mais uniquement pour des traitements non conformes, nouveaux, ou anciens pour lesquels des modifications nécessitent un nouveau PIA. Toutefois cette conformité ne vaut que pour 3 ans et tous les ans un check up doit être fait pour vérifier l'absence de modifications.

Exemple : en cas de traitement des données personnelles fondé sur le consentement des personnes, les modalités du recueil de ce consentement devront respecter le Règlement européen. Si tel n'est pas le cas, le traitement ne pourrait pas être poursuivi après le 25 mai 2018 et les personnes devront donner à nouveau leur consentement.

Par ailleurs, les objets connectés sont souvent des équipements radioélectriques, soumis au marquage CE Telecom, en application de la Directive 2014/53/CE du 16 avril 2014, dite RED.

L'article 3 de cette Directive spécifie que les objets radioélectriques doivent être compatibles avec la sauvegarde des données personnelles présentes sur les équipements radioélectriques. Cette Directive indique que la certification CE Telecom ne concerne pas uniquement l'électronique, mais aussi le logiciel embarqué et les éventuelles futures mises à jour de celui-ci.

1.2 - CHANGEMENTS DE PARADIGMES ENTRE LA DIRECTIVE DE 1995 ET LE R.G.P.D.

La gouvernance des données personnelles et de leur traitement deviennent des enjeux stratégiques et structurants du chef d'entreprise et/ou du comité de direction (board).

1.2.1 - CHANGEMENT DE PHILOSOPHIE

Sous l'empire des textes précédents, l'entreprise procédait par voie de déclaration auprès de la CNIL, cette dernière procédant immédiatement à une vérification de conformité, ne se retournant vers le déclarant qu'en cas de difficulté.

Dorénavant, le R.G.P.D. responsabilise l'entreprise, l'obligeant à mettre en place un processus interne de conformité au RGPD, charge à l'entreprise d'en justifier lors des contrôles a posteriori par l'autorité de contrôle compétente ou les parties prétendant avoir vu leurs droits violés ou exerçant ceux-ci.

Le processus déclaratif a ainsi disparu, remplacé par un processus de suivi interne permanent, à mettre en place. Il est également possible de recourir à des mécanismes de certification/labellisation qui constituent des commencements de preuve de conformité.

1.2.2 - CHANGEMENT DE MÉTHODE

Sous l'empire des textes précédents, l'entreprise procédait à un état des lieux pour aboutir au processus déclaratif.

Dorénavant, le R.G.P.D. impose le respect et la prise en compte dans le processus organisationnel de l'entreprise d'un certain nombre de principes, clairement identifiés, dont notamment :

- **Principe de « Privacy by Design » et « Privacy by Default »** : dès la conception de la solution et/ou du produit (sécurité hardware et software renforcée, limitation de la collecte et du traitement à ce que nécessaire au regard de la finalité et de la nature des données collectées...).

- **Principe de minimisation** : les données personnelles collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire et en lien avec la finalité pour laquelle les données sont traitées, la durée de conservation des données doit être limitée au strict minimum. Ce principe est complété par celui du droit à la limitation du traitement qui réduit les droits du RT en cas de contestation sur la légitimité du traitement : dans ce cas, seul le consentement de la personne concernée autorise le RT à traiter les données sauf pour quelques cas spécifiques.

- **Principe de transparence et d'auditabilité de la conformité**, tout le long de la vie de la solution (incluant matériel et logiciel) impliquant un traitement de données personnelles.

- **Principe de responsabilité et de redevabilité** ; l'entreprise devient personnellement et directement redevable envers la personne dont les données ont été collectées et traitées, des atteintes aux droits de ladite personne.

De plus, il appartient dorénavant à l'entreprise d'être en mesure de démontrer qu'elle est effectivement en conformité avec le Règlement, et non à la personne ou à l'Autorité de contrôle de démontrer que l'entreprise ne l'est pas. Ce renversement de la charge de la preuve implique pour l'entreprise d'être en permanence en conformité avec le Règlement Général sur la Protection des Données Personnelles, dans l'ensemble de ses composantes et de pouvoir, à tout instant, démontrer celle-ci (ce principe est également exprimé sous le vocable anglais d' « accountability »).

1.2.3 - CHANGEMENT D'ÉCHELLE DANS LES SANCTIONS ET RESPONSABILITÉS

Sous l'empire des textes précédents, les conséquences des manquements étaient relativement faibles, voir quasi-inexistantes : quelques dizaines de millier d'euros, outre une très rare publicité des condamnations, même si l'on a pu constater la remise au goût du jour de celle-ci par leur multiplication.

Le R.G.P.D. est marqué par une volonté évidente de dissuader et de sanctionner les manquements au règlement ainsi que d'indemniser les atteintes aux droits des personnes, au moyen de lourdes sanctions financières outre celui de la publication créant une atteinte forte à la réputation et pouvant mettre à mal la confiance de consommateurs envers l'entreprise à qui ils ont confiés leurs données :

- Fortes amendes : la CNIL ou les autres CNIL européennes (harmonisation G29) peuvent prononcer des amendes pouvant atteindre 4 % du CA mondial globalisé ou jusqu'à 20 millions d'euros, le plus élevé des deux en fixant le plafond de la condamnation.

- Des dommages et intérêts : le renforcement du droit à indemnisation - sous forme de dommages et intérêts - des personnes victimes de manquements et d'atteintes à leurs droits personnels ; en outre les associations agréées pourront engager des actions de groupe[7].

- Extension du spectre des personnes responsables : le RT et/ou son sous-traitant peuvent être attraits conjointement ou alternativement devant une juridiction, le plus souvent, au plus solvable des deux.

1.2.4 - DES NOUVEAUX DROITS ET DES DROITS RENFORCÉS

Au-delà du changement de paradigmes, le Règlement Général sur la Protection des Données Personnelles porte des nouveautés ou renforce certaines exigences antérieures qui doivent être prises en compte à l'aune du principe de Privacy by Design and by default :

- **Droit à la portabilité** : il permet à la personne concernée de récupérer ses données afin de les confier à une autre personne que celle qui les a collectées initialement : ce principe rend les données personnelles « utilisables » ou « réutilisables » directement par l'individu ou sous son contrôle et à son initiative hors du contrôle du Responsable de traitement qui les a collectées initialement. Ce droit est mis en œuvre à la demande de l'usager en cas de changement de prestataire : le nouveau prestataire récupérant les DCP de la personne concernée auprès de celle-ci ou auprès du précédent prestataire et les exploite personnellement, y compris en les complétant. Le guide de bonnes pratiques du G29 peut être consulté pour plus de détails[8].

[7] Le R.G.P.D. n'impose pas les actions de groupe qui sont à la discrétion du choix des États membres. Pour la France, il conviendra de se référer à la future loi relative à la protection des données personnelles.

- **Expression du consentement renforcée** : le consentement devra être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, et en tout état de cause, dénuée d'ambiguïté. Cela pourra se faire notamment en cochant une case spécifique, distincte de celle relative à l'acceptation des Conditions Générales d'Utilisation ou de Service lors de la consultation d'un site internet ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte spécifiquement le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité ou de consentement induit par l'acceptation des Conditions Générales d'Utilisation / Conditions Générales de Service.

- Protection des mineurs : lorsque l'enfant est âgé de moins de 16 ans, le traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de l'autorité parentale sur l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas inférieur à 13 ans. (Art. 8 R.G.P.D.)

- Encadrement du profilage et interdiction de principe de décision automatisée, sauf trois cas d'exception (consentement explicite de la personne, nécessaire pour la réalisation ou l'initiation d'un contrat, légitime du fait de textes légaux européens)[9].

- Nouvelle protection contre la traçabilité du comportement de l'utilisateur, via le risque de ré-identification, avec un encadrement de la technique de pseudonymisation par des mesures d'organisation technique et de sécurité.

1.2.5 - CONCLUSION

La gouvernance des données personnelles et de leur traitement devient un enjeu stratégique et structurant de l'entreprise dont le chef d'entreprise et/ou le comité de direction d'une entreprise de l'IoT sont, au final, responsables.

Mais ceux-ci ne sont pas seuls ! Leur meilleur allié se trouve dans la personne du Data Privacy Officer - le DPO - qu'il soit interne ou externe à l'entreprise[11].

Notre conseil : saisissez le R.G.P.D. comme une opportunité de développement, un moyen de sécuriser le patrimoine informationnel de votre entreprise, un critère marketing de conformité et un atout commercial concurrentiel en particulier à l'international et un enjeu de confiance pour vos clients finaux, qu'ils soient consommateurs ou professionnels, plutôt que comme une contrainte légale supplémentaire.

[8] *https://ec.europa.eu/newsroom/document.cfm?doc_id=44099Tr*

[9] *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, wp251*

[10] *« pseudonymisation » : le traitement de données à caractère personnel doit être pseudonymisé de telle façon que les données collectées ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. La pseudonymisation se distingue de l'anonymisation, la seconde étant définitive alors que la première est réversible et permets, par la suite, la réattribution à la personne concernée.*

[11] *Même si le R.G.P.D. n'impose la nomination d'un DPO que dans des cas spécifiques, les auteurs de ce guide recommandent fortement le recours à un DPO pour conseiller/accompagner les entreprises : il peut être externe ou mutualisé.*

1.3 - CHAMPS D'APPLICATION DU R.G.P.D. AVEC EXEMPLES POUR LE DOMAINE DE L'IOT

Le Règlement Général sur la Protection des Données Personnelles vise à encadrer les traitements de données à caractère personnel relatifs à des personnes physiques, au regard de critères de localisation de la personne ou du traitement.

1.3.1 - TRAITEMENT DE DONNÉES (ART. 2 DU R.G.P.D.)

Constitue un traitement de données, toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Cela concerne tout type de fichier, quelle que soit la forme du fichier.

Exemples :

- Fichiers des données de paiements liés à une carte NFC, avec circularisation[12] des paiements pour atteinte des plafonds.
- Fichier de gestion des accès aux locaux d'entreprise.
- Comportement alimentaire et actes d'achat tracés par les réfrigérateurs connectés (habitudes alimentaires et d'achat).

1.3.2 - DONNÉES À CARACTÈRE PERSONNEL (ART. 4 DU R.G.P.D.)

Constitue une donnée à caractère personnel, toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »). Est réputée être une «personne physique identifiable », une personne physique qui peut être identifiée, directement ou indirectement, 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.

Exemples :

- Données de géolocalisation : un abonnement permet de rattacher les déplacements à un véhicule, identifié comme propriété de Monsieur X.
- Adresse IP et/ ou MAC, n° de série de la puce RFID si associé à une personne (autre que non-randomisé, telle que la puce des cartes de transport et autres fonctionnalités « sans contact », cartes de paiement sans contact).
- Données comportementales (données d'activité physique, données sur les habitudes d'achat), données produites par des algorithmes (de profiling/profilage, d'intelligence artificielle) de données massives d'individus.

Attention aux données sensibles !

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 sont interdits à moins que des conditions soient satisfaites, comme le consentement explicite de la personne concernée au traitement de ses données (Article 9 R.G.P.D.)

[12] La circularisation consiste à demander à un tiers ayant des liens d'affaires avec l'entreprise vérifiée (fournisseurs ou clients) de confirmer directement au réviseur l'existence d'opérations, de soldes ou de tout autre renseignement.

1.3.3 - CHAMP TERRITORIAL ET EXTRATERRITORIAL ET CADRE PUBLIC/PRIVÉ (ART. 3 DU R.G.P.D.)

Le R.G.P.D. s'applique pour tout responsable de traitement ou sous-traitant :

- Localisé sur le territoire de l'UE, même si le traitement a lieu hors UE

  Exemple : Un constructeur automobile européen sous-traite la gestion de la géolocalisation de véhicules circulant en Europe à une société tierce, située en Tunisie : le Règlement Général sur la Protection des Données Personnelles s'applique.

- Localisé hors UE si les activités de traitement sont liées à une offre de biens et service (gratuits ou pas), et/ou au suivi du comportement qui a eu lieu sur le territoire européen.

  Exemple : Un opérateur de service de télécommunication américain traite, depuis la Californie, les données de citoyens français émises via des téléphones vendus en France : le Règlement Général sur la Protection des Données Personnelles s'applique.

1.4 LES SIX GRANDS PRINCIPES DU R.G.P.D.

Nous avons choisi de décliner ces principes au regard d'un cas fictif :

- la personne concernée : un salarié travaillant dans une centrale nucléaire

- l'outil de collecte : badge d'accès - sans contact - confié à un sous-traitant sur ce site sensible.

- les données collectées : nom, prénom, société d'appartenance, rôle/fonction, niveau d'habilitation, date et heure d'entrée et de sortie, numéro de porte utilisée correspondant à des zones identifiées comme sensibles au sein même de l'établissement (porte d'accès aux locaux de la DSI, salles de de contrôle, direction générale, aux zones de manipulations ou de stockage de matériel nucléaire, etc.), numéro du badge ou de la carte, date de validité.

- les finalités de la collecte : sécurité des personnes et des biens, géolocalisation aux fins de protection des salariés.

- les risques identifiés pour l'entreprise : atteinte au patrimoine et à la sécurité de l'entreprise, risques pour l'intégrité physique des personnes

1.4.1 - 1ER PRINCIPE : TRAITEMENT LICITE, LOYAL ET TRANSPARENT

- **Le traitement est licite** parce que conforme à l'Art. 6 du R.G.P.D. : intérêt légitime du RT ou autre base légale

- **Le traitement est transparent et Loyal** parce que le responsable du traitement a préalablement informé le salarié de la collecte de ses déplacements et de la présence d'un objet RFID pouvant faire du tracking à distance, de l'existence du traitement et de l'ensemble de ses droits.

1.4.2 - 2ÈME PRINCIPE : FINALITÉS PRÉCISES, EXPLICITES ET LÉGITIMES

- **Les finalités sont précises :**

  1) contrôle des accès à des locaux limitativement identifiés de l'entreprise et faisant l'objet d'une restriction de circulation,

  2) géolocalisation aux fins d'enclencher des secours, en cas d'incident dans les parties à risque des locaux de l'entreprise, limitativement identifiés et faisant l'objet d'une restriction de circulation.

- **Les finalités sont explicites** : le salarié est informé des seules finalités qui sont de protéger (1) les biens matériels et immatériels de l'entreprise et (2) sa propre sécurité physique (risque d'exposition aux radiations par exemple, localisation pour faciliter l'évacuation en cas d'incident).

- **Les finalités sont légitimes** : la collecte et le traitement sont mis en œuvre pour des raisons liées (1) à la sécurité et à la sûreté des biens de l'entreprise, et (2) à la protection du salarié (risque d'exposition aux radiations, risques pour la victime et les secours) ; la légitimité est renforcée compte tenu du caractère sensible des lieux, des risques pour les personnes et pour les intérêts supérieurs de la Nation.

A contrario, constituerait un traitement illégitime, la collecte de données liée aux accès aux lieux de pause et d'aisance. Dans ce cas, les droits et libertés de la personne prévalent sur l'intérêt de l'entreprise à la collecte des données qui est ici très peu évident.

1.4.3 - 3ÈME PRINCIPE : DES DONNÉES ADÉQUATES, PERTINENTES ET LIMITÉES AU REGARD DES FINALITÉS

Selon le principe de minimisation des données, les données personnelles collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité pour laquelle les données sont traitées.

Le responsable du traitement ne doit donc traiter que les données qui sont indispensables aux finalités déterminées. Il ne faut donc traiter que le strict minimum et sous réserve que la finalité du traitement ne puisse pas être atteinte autrement.

- **Les données sont adéquates** : sont collectées les seuls numéros de porte donnant accès aux zones sensibles et à restriction de circulation.

- **Les données sont pertinentes** : le numéro exact des portes et leur localisation, justifiant qu'il s'agisse bien des zones sensibles.

- **Le traitement est limité** : ne sont collectés que les numéros de porte donnant accès aux seules zones sensibles et aux seules fins d'assurer la sécurité des biens et des personnes

1.4.4 - 4ÈME PRINCIPE : DONNÉES EXACTES ET TENUES À JOUR

- Les données collectées via les badges portent sur le numéro exact des portes ouvertes, leur heure exacte d'ouverture, lesdites portes étant effectivement celles qui concernent des zones à restriction d'accès ou les zones sensibles, les badges sont attribués à des personnes identifiées et déterminées et ne peuvent être confondus avec ceux attribués à d'autres personnes.

- Les données sont tenues à jour parce que lorsque le badge nominatif est réattribué à un autre intervenant, les identifiants de celui-ci sont immédiatement et exactement substituées à celui du précédent détenteur ; en cas de perte, le badge est désactivé afin de ne pouvoir être utilisé par une autre personne dont les déplacements seraient alors attribuables au détenteur original, créant un risque de confusion.

Ce principe nécessite de la part du responsable du traitement la mise en place d'une politique de gestion organisationnelle de l'identification effective du porteur du badge et tenue à jour des fichiers d'octroi des badges (enrôlement, gestion de cycle de vie du badge).

1.4.5 - 5ÈME PRINCIPE : LES DONNÉES NE RESTENT IDENTIFIANTES QUE PENDANT UNE DURÉE N'EXCÉDANT PAS CELLE NÉCESSAIRE AU REGARD DES FINALITÉS

- Les données liées aux portes ouvertes par le porteur sont effacées au bout de quelques jours lorsqu'il est raisonnablement manifeste de penser qu'aucune difficulté n'a émaillé les déplacements du porteur : absence d'atteinte aux biens matériels ou immatériels de l'entreprise dans les zones franchies par la personne ou encore la personne concernée n'a pas subi d'atteinte à sa personne (absence d'exposition aux combustibles nucléaires).

Des durées de conservation légitimes sont parfois définies dans des textes législatifs sectoriels.

Les données peuvent toutefois être utilisées après désidentification directe ou indirecte, notamment dans des agrégats de données issues de données personnelles individuelles.

La prise en compte du cycle de vie de la donnée à caractère personnel doit se faire dès la conception (privacy by design and by default).

Ce principe nécessite de la part du responsable du traitement la mise en place d'une politique de gestion organisationnelle des données et de destruction après une durée dépendante de la finalité (anonymisation vs identification nominative, notamment en fin de mission).

1.4.6 - 6ÈME PRINCIPE : SÉCURITÉ APPROPRIÉE POUR ASSURER L'INTÉGRITÉ ET LA CONFIDENTIALITÉ DES DONNÉES

- L'entreprise a déployé un ensemble de mesures de sécurité physique (contrôle d'accès, dispositif anti-incendie) et logique (gestion des habilitations et contrôle des accès, traçabilité des droits d'accès au traitement, chiffrement, sécurisation de point en point, authentification de l'ensemble des parties ayant accès, stockage sécurisé, surveillance des logs et détection des attaques d'intrusion, suivi des alertes et préconisations du CERT-FR[13], politique de sécurité globale via une charte informatique annexée au règlement intérieur de travail) qui garantit que, de bout en bout, la chaîne de traitement des données ne puisse être corrompue d'une façon ou d'un autre et que des tiers n'ayant pas un intérêt légitime à accéder à ces données puisse le faire.

Ces mesures de protection doivent être proportionnées au niveau de risque que portent les activités de traitement des données.

Ce principe nécessite de la part du responsable du traitement la mise en place d'une politique de gestion organisationnelle des données permettant leur sécurisation physique et logique.

1.5 - DROITS RENFORCÉS ET NOUVEAUX DROITS POUR LES PERSONNES PHYSIQUES

1.5.1 - L'INFORMATION APPROFONDIE DE LA PERSONNE CONCERNÉE : LE CONSENTEMENT LIBRE, EXPLICITE, ÉCLAIRÉ ET UNIVOQUE

Nombre de traitements sont licites par nature lorsqu'ils reposent sur le consentement de la personne aux traitements des données qui le concerne.

Encore faut-il que ce consentement soit une manifestation de volonté, libre, spécifique et éclairée par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair - univoque - que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Le véritable point d'attention est le caractère « éclairé » du consentement. Pour être éclairée, la personne concernée doit se voir communiquer TOUTES les informations utiles afin qu'elle puisse connaître les tenants et les aboutissants du traitement, mais aussi en quoi ses droits peuvent être mis en jeu, comment elle

[13] *https://www.cert.ssi.gouv.fr/*

les mettra elle-même en œuvre (la finalité, les durées de conservation, les personnes pouvant y accéder, les éventuels transferts, etc.)

Dans ce cadre, il appartient au responsable du traitement de démontrer que le consentement a été effectivement donné dans ces conditions.

Dans le domaine de l'IoT, la collecte du consentement - en particulier dans un cadre B-to-C - et le principe de la minimisation de la collecte trouvent tout leur sens puisqu'au moment de déterminer si le consentement est donné librement, il y aura lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

L'exigence du consentement libre et éclairé est un des points d'attention majeur du chef d'entreprise pour les cas où le traitement est mis en œuvre sur la base du consentement de la personne concernée, ce qui sera le cas dans bien des situations et de façon quasi systématique dans le cadre de relations commerciales B-to-C.

1.5.2 DES DROITS D'INFORMATION RENFORCÉS

1.5.2.1 - L'information approfondie de la personne concernée : le consentement libre, explicite, éclairé et univoque

- Lors de la collecte des données, directement auprès de celle-ci ou de façon indirecte, un nombre certains d'information doit impérativement être donné à la personne concernée : une liste exhaustive est précisée aux articles 13 et 14 du règlement.

La quantité d'information à donner et leur précision augmente sensiblement par rapport à la loi Informatique et Liberté.

La nature de l'information dépend du mode de collecte : direct ou indirect. Ce point est important, notamment pour le cas où les données collectées par l'objet connecté sont ensuite transférées à des tiers. Il faudra donc attirer l'attention de ce tiers de cette obligation d'information spécifique.

Le traditionnel droit d'accès est maintenu et renforcé puisque des informations complémentaires doivent être communiquées à la personne qui en fait la demande.

Notons aussi que le principe de transparence implique que ces informations données le soit sous une forme lisible et claire.

- La personne concernée est en droit de savoir, à tout instant et pas seulement lors de la collecte, si des données le concernant sont traitées et, si oui, d'y avoir accès et d'en obtenir une copie. Ces droits, qui existaient déjà, sont clarifiés et rendus plus exploitables pour la personne concernée.

1.5.2.2 - Droit à l'information en cas de violation de données à caractère personnel

Le titulaire dispose dorénavant d'un droit à l'information lorsque ses données à caractère personnel sont violées : ce droit à l'information peut être personnalisé (information directe de chaque victime par le responsable du traitement) ou généralisé (information globale, non individualisée).

1.5.2.3 - Droit à la notification en cas de manipulations internes

Lorsque le responsable du traitement efface, rectifie ou limite les données qu'il traite, il a l'obligation de notifier ces manipulations aux personnes à qui il a transféré les données de la personne concernée, de telle sorte que les données qui sont tenues exactes et à jour remplacent, chez les destinataires, les données qui ne le sont plus. Ce nouveau droit pour la personne concernée

corrobore l'obligation faite au responsable du traitement de maintenir les données exactes et tenues à jour (art. 5-1-d). La mise en œuvre de cette obligation nécessite pour le fabricant d'objet connecté de pouvoir suivre les destinataires des données qu'il a collectées, traitées et transférées.

1.5.3 - DROITS DE RECTIFICATION ET À LA LIMITATION DU TRAITEMENT, DROIT D'OPPOSITION ET DE REFUS DE DÉCISION FONDÉE SUR UN TRAITEMENT AUTOMATISÉ

Une fois les données collectées identifiées, la personne concernée peut exercer un droit de rectification faisant obligation au responsable du traitement de corriger les données inexactes, y compris en les complétant pour les rendre exactes - la personne concernée est autorisée à fournir des informations complémentaires.

Elle est également en droit d'exiger, dans 4 cas (contestation de l'exactitude des données, illicéité du traitement mais refus de leur effacement par la personne concernée, données devenues inutiles pour le responsable du traitement mais pas pour la personne concernée et enfin, opposition au traitement) que les données ne soient plus utilisées par le responsable du traitement bien qu'il puisse les conserver. Cette interdiction de traiter disparaît néanmoins (i) lorsque la personne concernée accepte le traitement, (ii) dans le cadre de procédure judiciaires ou administratives, (iii)

pour protéger les droits d'une autre personne et enfin (iv) pour des motifs importants d'intérêts publics.

Le droit d'opposition au traitement, qui doit être notifié à la personne concernée lors de la première communication, permet à toute personne de s'opposer à ce que ces données fassent l'objet d'un traitement automatisé. Dans certains cas liés aux intérêts légitimes et impérieux du responsable du traitement, celui-ci ne traite plus les données.

Par ailleurs, le droit de s'opposer à la prospection est absolu et ne connaît aucune dérogation : des prospections issues de données générées par des objets connectés - y compris au travers d'un profilage - sont, par nature, temporaires et éphémères c'est-à-dire jusqu'à ce que la personne s'y oppose.

La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

1.5.4 - DROIT À LA PORTABILITÉ DES DONNÉES (DROIT NOUVEAU)

La personne physique reste propriétaire de ses données ; l'entreprise n'en est que l'utilisateur, de façon temporaire.

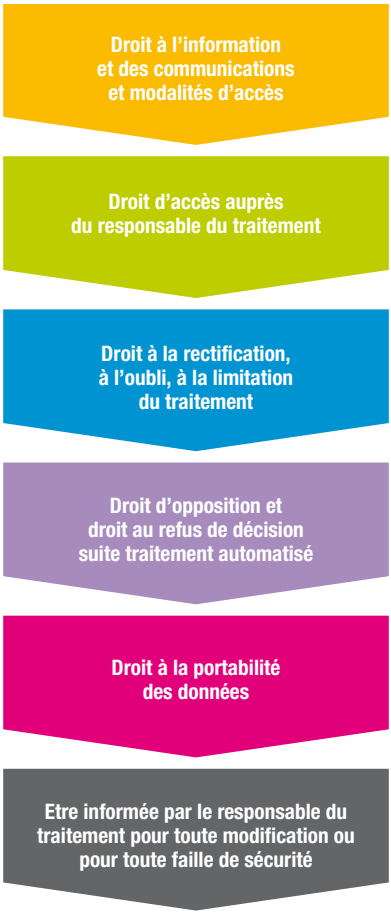
À ce titre, la personne physique peut exiger que ses données - traitées avec son consentement ou en exécution d'un contrat ; et à l'aide d'un procédé automatisé - lui soient restituées ou transmises à un tiers de son choix qui sera seul autorisé à les exploiter.

1.5.5 - DROIT À L'EFFACEMENT (DROIT À L'OUBLI)

Les données ne doivent être conservées que le temps nécessaire à l'accomplissement de l'objectif qui était poursuivi lors de leur collecte : à l'issu de cette durée, elles doivent être effacées. Les personnes concernées peuvent exiger leur effacement, dans les meilleurs délais, s'il n'y est pas procédé spontanément par le responsable du traitement. Néanmoins, ce droit est encadré par les dispositions de l'article 17 du Règlement.

Cela pose, en parallèle des conditions de cet effacement sur requête de la personne concernée, la question de la durée de conservation légitime des données générées par les objets connectés. Il est probable que des données de

géolocalisation « brutes » ont des durées de conservation relativement courtes, ce qui ne sera pas le cas pour des données relatives au bien-être de la personne et qui conduisent à l'exécution d'un contrat (balances connectées et livraison de repas hypoglycémiques).



1.6 - DEVOIRS DU RESPONSABLE DE TRAITEMENT ET DES SOUS-TRAITANTS

Le R.G.P.D. définit des rôles spécifiques pour délimiter plus clairement les responsabilités des organisations, à la fois directement envers leurs clients mais aussi envers les vendeurs ou partenaires tiers qui sont impliqués dans des transferts et exploitations de données personnelles. A la qualité de responsable de traitement, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ;

Exemples de responsable de traitement : Responsable Juridique, Responsable Marketing, Directeur Métiers / Directeur de processus, Directeur des Opérations, Directeur Général, etc...

Est un sous-traitant, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

Exemples de sous-traitants externes à l'entreprise : société tierce, opérant pour le compte du responsable du traitement tout ou partie des activités du responsable de traitement ou ayant en charge le traitement informatique de données pour le compte du responsable de traitement (infogérance, hébergeur...)

1.6.1 LE RESPONSABLE DE TRAITEMENT

De façon générale, le responsable du traitement assure le respect du Règlement Général sur la Protection des Données Personnelles, tant au regard des obligations qui lui sont fixés personnellement par le règlement, mais il assure encore que les droits de la personne concernée sont respectés par la personne pour laquelle il intervient.

Lorsqu'il sous-traite un traitement, il assume conjointement les risques et responsabilités du traitement avec le

sous-traitant qu'il a choisi : la personne concernée peut demander des comptes à l'un, à l'autre voire aux deux, le plus souvent au plus solvable.

Il met en œuvre des mesures techniques et organisationnelles appropriées - qu'il réexamine et actualise si nécessaire - pour s'assurer et être en mesure de prouver que les traitements dont il est responsable sont effectués conformément au Règlement. A cet égard, il tient à jour le registre des activités de traitement effectuées sous sa responsabilité[14] (dont le contenu est énuméré par le Règlement à l'article 30 : le sous-traitant en sus de son propre registre doit tenir aussi un registre pour chaque traitement dont il assume la sous-traitance) et coopère avec l'autorité de contrôle dont il relève (art. 31), qu'il informe des violations de données à caractère personnel et consulte préalablement lorsque les études d'impact font ressortir des risques.

Il tient, toujours au nom du principe de traçabilité, l'inventaire des violations des données à caractère personnel qu'il notifie à l'autorité de contrôle et aux personnes concernées, outre un inventaire de la bonne gestion des demandes des utilisateurs (demandes d'accès, droit à l'effacement, droit de modification, portabilité) même si l'inventaire est anonymisé ou pseudonymisé.

Il s'assure de la protection des données dès la conception et de la protection des données par défaut (Privacy by design and by default). Il met en œuvre, dès la phase de conception des projets informatiques et des outils IoT puis lors de leur mise en œuvre et de toute évolution (adaptative et corrective) des mesures techniques et organisationnelles appropriées de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du Règlement et de protéger les droits de la personne concernée.

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent 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.

Il met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour les traitements de données à caractère personnel. En cas de violation de données à caractère personnel, il notifie celle-ci à l'autorité de contrôle et la communique à la personne concernée.

Il réalise, avant la mise en œuvre du traitement, les études d'impact relatives à la protection des données lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Lorsqu'une analyse d'impact indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque il consulte l'Autorité de Contrôle préalablement à la mise en œuvre du traitement.

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Ils peuvent se partager les responsabilités qui pèsent sur le responsable du traitement, mais cette répartition est inopposable à la personne concernée qui peut faire valoir ses droits auprès de l'un ou de l'autre.

1.6.2 LE SOUS-TRAITANT

Agissant pour le compte d'un responsable du traitement, celui-ci doit présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisation-

[14] https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx

nelles appropriées de manière à ce que les traitements répondent aux exigences du Règlement et garantissent la protection des droits de la personne concernée.

Les modalités d'intervention du sous-traitant doivent impérativement être précisées danss un contrat dont le contenu minimum est énuméré par le règlement, y compris par des références à des clauses types, qui doivent néanmoins faire l'objet d'adaptation aux cas de l'espèce.

Le recours à des mécanismes de certification ou à un code de conduite approuvé peuvent servir à démontrer l'existence des garanties suffisantes chez le sous-traitant.

Les instructions du responsable du traitement définissent le spectre de l'intervention du sous-traitant qui ne peut agir que dans ce cadre et dans cette limite, sauf à devenir lui-même responsable du traitement.

1.6.3 LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPD) OU DATA PRIVACY OFFICER (DPO)

Obligatoire dans certaines hypothèses (notamment celles des traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées), la nomination d'un DPO par le responsable du traitement est néanmoins recommandée dans de nombreux autres cas.

Présentant des garanties de compétences professionnelles et, en particulier, des connaissances spécialisées du droit et des pratiques en matière de protection des données, il dispose de ressources utiles à sa mission mais ne reçoit aucune instruction dans l'exercice de sa mission, faisant directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant, dont il tire sa légitimité.

Le DPO doit également posséder une connaissance éprouvée en matière organisationnelle puisqu'il peut quasiment assumer le rôle de chef de projet lors de la mise en place du R.G.P.D. dans les départements concernés au sein de l'entreprise (notamment la DSI, les RH et le marketing). Des connaissances informatiques sont aussi requises puisqu'il doit pouvoir, a minima, comprendre les enjeux et les solutions techniques existantes dont il pourra, le cas échéant, recommander les évolutions et superviser celles-ci.

Véritable conseil indépendant, il recommande et assiste l'entreprise sans porter toutes les responsabilités - qui restent à la charge du conseil d'administration dont il est le superviseur et l'observateur impartial. Il est associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, il est le point de contact des personnes concernées au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le Règlement.

Par ailleurs, il a la responsabilité (et doit disposer des compétences en adéquation) :

a) d'informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent

b) de contrôler le respect du Règlement et des autres règles légales ou internes en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

c) de dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 ;

d) de coopérer avec l'autorité de contrôle ;

e) de faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.

Il est important de noter que les compétences qui sont exigées du DPO (compétences techniques, organisationnelles et juridiques) justifient que le DPO puisse être externalisé - notamment dans les structures de tailles modestes ou moyennes qui ne disposent pas de salariés dotés de ces trois compétences - renforçant par là même son impartialité et son indépendance.

Un groupe d'entreprises peut partager un même DPO à partir du moment où ce dernier demeure « facilement accessible à partir de chaque établissement ». Ainsi les structures qui peuvent manquer de moyens, sont également en mesure d'assurer leur conformité au R.G.P.D. par le biais d'un système de DPO collaboratif.

Privacy by Design (dès la conception)

Déterminer la Criticité
- **PIA : pour tout risque élevé et soumission à la CNIL**
- **Analyse simplifiée pour tous les autres risques**

Mise en place de sécurité de traitement

Registre des activités de traitements et conserver les preuves du respect du R.G.P.D.

Coopération avec l'autorité de contrôle : la CNIL

Obligations de notification à la personne concernée et à la CNIL pour toute violation du R.G.P.D. dans les 72h

1.7 - SANCTIONS ET IMPACTS

Le Règlement augmente substantiellement les risques pour le responsable du traitement défaillant.

1.7.1 DES RISQUES D'AMENDES ADMINISTRATIVES

Alors que les amendes records prononcées par la CNIL ont atteints 150.000 euros, le Règlement porte l'amende administrative maximale à 4 % du chiffre d'affaires mondial ou 20 millions d'euros d'amende - montant le plus élevé des deux - pour les manquements les plus graves (violation des principes de base du traitement, y compris le consentement, violations des droits des personnes concernées, etc.).

Néanmoins toutes les infractions n'exposent pas à de telles amendes qui dans certains cas sont plafonnés à 2 % du chiffre d'affaires mondial et 10 millions (violation des obligations de sécurité du traitement, analyse d'impact, DPD).

1.7.2 DES RISQUES DE DOMMAGES-INTÉRÊTS EN RÉPARATION DU PRÉJUDICE DE LA VICTIME

Les personnes concernées se voient reconnaître un droit personnel à réparation de son préjudice, sous forme de dommages-intérêts, qui vient en application du droit personnel d'introduire un recours juridictionnel effectif contre le responsable du traitement, si elle considère que ses droits ont été violés et que cela lui a causé un préjudice, qu'il soit matériel et/ou moral.

Ces dernières peuvent se faire assister ou représenter par des associations.

Notons que des actions de groupes sont également envisageables, les organismes habilités pouvant prendre l'initiative d'intenter des actions sans être mandatés par ceux dont ils défendent, statutairement, les intérêts. Néanmoins ces dernières n'agissent que pour obtenir la cessation du trouble (dommage consécutif à un manquement à la loi Informatique et Libertés, tel qu'une faille de sécurité chez un opérateur ou l'un de ses sous-traitants) et non pas pour la réparation du préjudice individuel des victimes.

1.7.3 DES RISQUES POUR L'IMAGE DE MARQUE DE L'ENTREPRISE

Les sanctions prononcées par l'Autorité de contrôle peuvent être rendues publiques par mention dans des publications et journaux.

1.7.4 UN RISQUE PÉNAL

Enfin, il est à rappeler que le défaut de prise de mesures de protections pour préserver la sécurité des données expose également le contrevenant à cinq ans d'emprisonnement et à 300 000 euros d'amende (Art. 226-17 code pénal).

1.7.5 DES SANCTIONS COMPLÉMENTAIRES À VENIR

Enfin le Règlement octroie aux États membres la possibilité de fixer d'autres sanctions que les amendes pour les violations.

Le projet préparatoire présenté en conseil des ministres les 13 décembre 2017[15] fait usage de cette faculté, prévoyant notamment des amendes pénales ou des injonctions de mise en conformité sous astreinte pouvant atteindre 100.000 euros par jour.

[14] https://www.legifrance.gouv.fr/affichLoiPreparation.do ; jsessionid=AD5660270AD9F70B94275AC823321680.tplgfr22s_3 ? idDocument=JORFDOLE000036195293&type=contenu&id=2&typeLoi=proj&legislature=15

1.7.6 D'UNE RESPONSABILITÉ PERSONNELLE VERS UNE RESPONSABILITÉ IN-SOLIDUM DU RESPONSABLE DU TRAITEMENT ET DE SON SOUS-TRAITANT

Le responsable du traitement est responsable des dommages causés par les violations du Règlement.

Le sous-traitant est responsable des manquements aux obligations spécifiques que lui impose le règlement ainsi que de ne pas avoir respecté les instructions du responsable du traitement.

Lorsqu'ils ont concourus ensemble à la réalisation d'un dommage, la victime peut demander réparation à l'un d'entre eux pour la totalité du dommage, charge à ce dernier de se retourner contre son cocontractant. La même règle vaut s'il y a plusieurs responsables d'un même traitement.

2

MISE EN PLACE DU R.G.P.D. : SIX ÉTAPES CLÉS

Dans cette partie, nous proposons une méthodologie permettant à votre projet de répondre aux exigences du règlement sur la protection des données personnelles en vue d'asseoir votre conformité règlementaire. Elle s'inspire des recommandations de la Commission Nationale Informatique et Libertés (CNIL[16]) et est illustrée par des exemples dédiés aux projets pour appliquer le principe de « privacy by design ». Elle prend en compte le contexte de l'Internet des Objets et le principe d'amélioration continue. Ce sujet, en pleine évolution, conduira, si nécessaire, à des mises à jour de ce document, d'où la nécessité d'utiliser la version du Guide la plus récente.

6 étapes ? Oui, mais lesquelles…

- **Etape 1** : S'appuyer en interne sur la gouvernance et identifier les acteurs clés

- **Etape 2** : Cartographier mon traitement de données personnelles

- **Etape 3** : Prioriser les actions à mener au regard des obligations légales en matière de droits et de libertés des personnes concernées.

- **Etape 4** : Gérer les risques. Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener une analyse d'impact sur la protection des données (PIA).

- **Etape 5** : Suivre les procédures internes pour traiter des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

- **Etape 6** : Documenter la conformité. Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés, révisés et actualisés régulièrement pour assurer une protection des données en continu.

Tout au long de ce chapitre, nous vous amènerons à répondre à un certain nombre de questions qui vous permettront d'obtenir les réponses nécessaires au respect des exigences du Règlement Général sur la Protection des Données Personnelles.

Il conviendra de les exploiter dans le cadre du processus de mise en conformité.

2.1 - ETAPE 1 : IDENTIFIER LES RÔLES ET RESPONSABILITÉS, LES ACTEURS CLÉS ET LÉGAUX DU PROJET

Action : j'identifie chacun de mes traitements

Action : j'identifie l'entité juridique qui le met en place et/ou l'exploite, en sa qualité de « responsable de traitement » ou « sous-traitant » au niveau de :
- La « Business Unit » de l'entité juridique ;
- La filiale ;
- Le client, l'entreprise externe ;
- …

Action : si mon entreprise ou le groupe de mon entreprise, possède une gouvernance établie pour le R.G.P.D., je

m'appuie sur les règles établies par cette gouvernance. J'identifie le DPD/DPO ou le correspondant référent avec les autorités.

Précaution : attention aux contraintes légales et aux spécificités propres qui s'appliquent au RT ainsi qu'aux dispositions légales et réglementaires du territoire dans lequel le traitement est opéré. Un traitement réalisé aux USA en application des directives du RT situé en France sera soumis au Règlement Général sur la Protection des Données Personnelles et au droit américain.

Réflexe 1
Je m'assure du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de mon traitement de données dès sa conception. Je m'assure du soutien de la direction dans ma démarche de conformité au règlement.

- [Q1] Qui est le DPO ? Quels sont les acteurs du traitement ? Quelles autres ressources juridiques, techniques, métier sont associées au projet pour garantir la protection des données personnelles ?

2.2 - ETAPE 2 : CARTOGRAPHIER MON TRAITEMENT DE DONNÉES PERSONNELLES

Réflexe 2
Pour mon traitement de données personnelles, je me pose les bonnes questions et en cas de doute, je contacte mon DPO et/ou mon service support juridique et/ou sécurité habituel.

Action : j'identifie :

- **Qui ?**
  - [Q2] Nom et coordonnées du délégué à la protection des données, Nom et coordonnées du responsable du traitement (et de son représentant légal)
  - [Q3] Responsables des services opérationnels (destinataires) traitant les données au sein de mon projet
  - [Q4] Liste de mes sous-traitants
  - [Q5] Personnes concernées par le traitement de leurs données personnelles
- **Quoi ?**
  - [Q6] **Source des données** (origine primaire et secondaire)
  - [Q6bis] Parcours et flux des données de la source à la destruction des données, décrivant les traitements et les systèmes d'information utilisateurs
  - [Q7] **Catégories de données** traitées
  - [Q7 bis] Données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé). Si les données sont identifiées comme sensibles ou les traitements sont à haut risque, je me rapproche de mon DPO ou à défaut de mon service juridique ou à défaut je consulte le guideline du G29[17] sur le PIA pour voir si je procède à une analyse d'impact (PIA). Dans de nombreux cas de figures, même sans obligation légale, un PIA est fortement recommandé et pourra servir de base de document initial pour la documentation de conformité R.G.P.D.

[17] *http://ec.europa.eu/newsroom/document.cfm?doc_id=44137*

- **Pourquoi ?**

  - [Q8] **Finalités** pour lesquelles les données sont collectées ou traitées. Quel est le but de mon fichier ? (à quoi va-t-il servir ?)

Rappel : l'utilisation et le traitement de données personnelles doivent s'inscrire dans un but précis et déterminé.

Exemples de finalités :

- Gestion de la carrière et de la mobilité des salariés
- Fichier client-prospect de vente en ligne
- Suivi des véhicules utilisés par les salariés pour maintenance et assurances
- Suivi du temps de travail/contrôle des horaires du salarié pour gestion de la paie

  - [Q9] **Qui définit la finalité** ?

  - [Q10] Est-ce **légitime**, notamment au regard de mes missions et des droits et libertés des personnes (base légale du traitement) et au regard des autres textes législatifs s'appliquant à mon domaine d'activité ?

Exemples d'autres textes législatifs à prendre en compte :

- Code du travail
- Loi Programmation Militaire[18] pour OIV
- Code des postes et des communications électroniques
- Code de commerce
- Procédure d'agrément des hébergeurs de données de santé à caractère personnel précisée par le décret du 4 janvier 2006
- Code de la santé modifié au 26 janvier 2016 et décret NIR du 27 mars 2017
- La Loi pour une république numérique
- Avis et délibérations de la CNIL
- Jurisprudence de la CJUE (Cour de Justice Union Européennes) en termes de protection de données personnelles (ex une donnée IP statique est une donnée personnelle mais aussi une donnée IP dynamique dans un contexte permettant l'identification avec d'autres données disponibles[19]

  - [Q11] Comment présenter cette finalité pour la rendre compréhensible par tous ?

  - [Q12] Comment présenter cette finalité pour la rendre compréhensible par tous ?
  - [Q12bis] Je vérifie si j'ai vraiment besoin de toutes les données personnelles envisagées pour le projet de traitement et si je peux obtenir le même résultat en les anonymisant ou en les pseudonymisant.

  - [Q13] Combien de temps les données doivent-elles être disponibles pour atteindre ce but ?

- **Où ?**

  - [Q14] Dans quel lieu et dans quel pays les données sont-elles collectées, traitées et hébergées ?

  - [Q15] Existe-t-il des transferts de données entre pays ?
  - [Q15bis] Des données collectées ou traitées dans l'UE sont-elles transférées hors UE ?

Réflexe 3
Je contrôle les transferts hors UE.

[18] http://www.defense.gouv.fr/portail/enjeux2/politique-de-defense/la-loi-de-programmation-militaire-lpm-2014-2019/actualisation-de-la-loi-de-programmation-militaire-lpm-2014-2019/lpm
[19] Ref Judgment in Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland

Les règles relatives aux transferts de données personnelles sont très contraignantes, notamment pour des groupes d'entreprises mondiaux. Il est très important de s'appuyer sur le DPO, ou à défaut son service juridique et les experts sécurité et métier associés au projet pour vérifier les conditions du transfert (techniques et contractuelles) :

- [Q16] Quelles sont les mesures de protection garanties pour ce transfert ? Existe-t-il des Règles Contraignantes d'Entreprises (Binding Corporate Rules) ? Les clauses contractuelles relatives au transfert s'appuient-elle sur les modèles de clauses contractuelles types adoptées par la Commission européenne ?

- [Q17] Le service juridique est-il informé de ce transfert ?

Illustration : Transfert de données au départ de l'UE vers les USA

Les entreprises établies en France souhaitant transférer des données vers les USA doivent vérifier que l'entreprise destinataire des données est effectivement enregistrée parmi la liste « Privacy shield » de l'administration américaine.

Cette inscription pouvant aisément être vérifiée à partir du site internet https://www.privacyshield.gov/

- **Jusqu'à quand ?**

- [Q19] Pour chaque catégorie de données, combien de temps les données sont-elles conservées ? (Se mettre en cohérence avec la question Q13)

Réflexe 4
La durée de conservation des données est définie et tient compte du contexte juridique. Une purge ou une anonymisation définitive est prévue à la fin du traitement, sauf pour les cas où des règles légales justifient de la conservation.

Le projet doit s'appuyer sur le DPO et/ou le service juridique pour définir une durée de conservation, à l'issue de laquelle les données seront détruites ou archivées.

Dans tous les cas, les données personnelles doivent être conservées uniquement le temps nécessaire à l'accomplissement de l'objectif qui était poursuivi lors de leur collecte. Ce principe a pour conséquence de faire obstacle à une durée illimitée des données collectées et de poser le principe d'une durée de conservation proportionnée par rapport à la finalité du traitement. La durée de conservation proportionnée repose souvent sur un fondement juridique (obligation légale ou réglementation spécifique) lorsqu'il est prévu ou sur la durée de la relation avec la personne physique fichée.

Illustration : Exemples de fondements juridiques pour les durées de conservation

Finalité du traitement	Durée de conservation maximale (à titre indicatif)	Fondement juridique (lorsqu'il est prévu)
Gestion du personnel	5 ans (en archivage intermédiaire) à compter du départ du salarié	Norme simplifiée n° 46
Dispositif de vidéo surveillance des lieux dont l'accès est strictement limité et non ouvert au public (zone de marchandises, entrée/sortie bâtiment, parking entreprise, ...)	1 mois	Loi 95-73 du 21-01-1995
Dossier médical dans les cabinets médicaux libéraux	Conservation du dossier médical pendant 10 ans.	Article L.1142-28 Code de la santé publique
La gestion de la facturation	10 ans	Article L123-22 alinéa 2 du Code de commerce Norme simplifiée n°48
Documents et informations relatives aux opérations faites par les clients (dépôts, retraits, virements, prélèvements, cartes)	5 ans à compter de l'exécution de l'opération	Article L561-12 du Code monétaire et financier Lutte contre le blanchiment et le financement du terrorisme AU 003
Contrôle des horaires des salariés	5 ans	Article L. 3171-3 et D317-16 du Code du travailde commerce
Géolocalisation des véhicules des employés	De 2 mois à 5 ans	Si rentre exactement dans le cadre de la norme simplifiée 51, si hors cadre de règlement, PIA et avis de la CNIL si besoin

- **Comment ?**

  - [Q20] Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées (chiffrement, contrôle d'accès, ...) ?

Réflexe 5
Dès la conception du traitement, je m'assure de la prise en compte des mesures adéquates pour protéger les données personnelles et respecter les droits des personnes.

Techniquement, les solutions opérationnelles adéquates à chaque contexte devront être élaborées. Les projets doivent s'appuyer à la fois sur le service de l'entreprise qui collecte et traite la donnée, l'équipe juridique et sur l'expertise en sécurité informatique (SSI).

2.3 - ETAPE 3 : PRIORISER LES ACTIONS À MENER

Après avoir identifié mon traitement de données personnelles mis en œuvre au sein du projet, je dois identifier les actions à mener pour me conformer aux obligations actuelles et à venir.

Cette priorisation peut être menée au regard des risques que font peser mon traitement sur les libertés des personnes concernées. Certaines tâches seront faciles à mettre en œuvre et permettront de progresser rapidement.

Je suis vigilant sur le respect des libertés individuelles. Je vérifie :

- que seules les données strictement nécessaires à la poursuite de mes objectifs sont collectées et traitées ;
- la base juridique sur laquelle se fonde mon traitement (par exemples : consentement de la personne, intérêt légitime, contrat, obligation légale) ;
- que mes sous-traitants sont informés de leurs obligations et responsabilités en matière de sécurité, de confidentialité et de protection des données personnelles traitées, notamment au travers des clauses contractuelles adéquates
- que mes mentions d'information auprès de la personne concernée par le traitement (client final ou salarié) existent et soient conformes aux exigences du règlement ;
- que je suis en mesure d'informer les personnes concernées de leurs droits et des modalités de leur exercice et que je suis personnellement en mesure de répondre effectivement à ces demandes
- que les mesures de sécurité sont mises en place

Attention : de manière générale, je documente et je conserve ces vérifications et des preuves (cf. Etape 6 Documentation).

2.4 - ETAPE 4 : GÉRER LES RISQUES

Je suis vigilant sur le niveau de risques que comportent les données personnelles que je collecte et détiens et/ou sur mon traitement.

Je vérifie l'existence d'un risque inhérent au traitement.

Lors d'une phase d'évaluation préalable, je fais une première analyse de risque et j'identifie si je rentre dans le cadre d'une obligation de PIA.

En effet selon la finalité du traitement, la nature des données, le niveau de criticité, je peux être dans l'obligation de mener une analyse d'impact sur la protection des données (PIA) (cf. critères définis par le G29 dans son guideline PIA[20] présent également sur le site de la CNIL[21]), de fournir une information renforcée, de recueillir le consentement, d'obtenir une autorisation préalable des autorités, d'encadrer par des clauses contractuelles spécifiques. Une analyse approfondie avec mon DPO ou mon service juridique et mes experts sécurité est nécessaire pour déterminer les mesures à mettre en œuvre.

Par ailleurs, je suis soumis à l'obligation[22] de PIA si :

- Il s'agit d'un le traitement à grande échelle d'informations concernant la santé, la vie sexuelle, la race ou l'origine ethnique (données sensibles Art.9) ;

[20] ec.europa.eu/newsroom/document.cfm?doc_id=44137
[21] https://www.cnil.fr/fr/gerer-les-risques
[22] A noter que la CNIL recommande un PIA si le traitement rencontre au moins 2 des critères parmi les 9 définis dans les lignes directrices du G29

- Il s'agit d'une surveillance systématique à grande échelle d'une zone accessible au public[23].
- le traitement concerne des données sur les enfants, des données biométriques ou des données génétiques dans des systèmes d'archivage à grande échelle.
- le traitement concerne une évaluation systématique d'aspects personnels y compris le profilage[24]

La CNIL peut enrichir cette liste d'obligation de PIA.

Réflexe 6
Dès la conception du traitement, je m'assure de la prise en compte des mesures adéquates pour protéger lesdonnées personnelles et respecter les droits des personnes.

De façon opérationnelle, les solutions de sécurité adéquates à chaque contexte devront être élaborées à partir d'une analyse de risque plus ou moins approfondie selon la sensibilité du traitement.
Pour cela, j'utilise les outils préconisés par mon entité et/ou mon DPO ou à défaut par :

- la CNIL[25] et/ou
- le G29[26] et/ou
- une méthodologie conforme à la norme EN 16571[27] qui sera présentée au dernier chapitre

Quelle que soit la méthode choisie, je m'appuie sur les principes de l'annexe 2 du guideline du G29.

Je vérifie l'existence d'un risque inhérent au transfert des données hors de l'UE.

Si des données sont transférées hors de l'Union européenne, le pays vers lequel je transfère les données doit être reconnu comme adéquat par la Commission européenne. Dans le cas contraire, j'encadre les transferts (Cf. Etape 2, Réflexe 3).

Je vérifie que les risques liés à la sécurité des données sont pris en compte et traités
Pour le management de la sécurité, je m'appuie sur :

- les guides de sécurité proposés par la CNIL[28]
- le guide d'hygiène informatique 2017 de l'ANSSI[29]
- le tableau d'évaluation check liste sécurité[30]
- la fiche sécurité des locaux[31]

[23] En droit français, on parle de vidéoprotection quand il s'agit d'une zone accessible au public et de vidéosurveillance quand l'accès est strictement limité et non ouvert au public. Dans le cas de la vidéoprotection, la loi française, en sus du PIA, impose une déclaration en préfecture. Dans les deux cas, je dois m'assurer qu'il ne porte pas atteinte à la vie privée des personnes filmées (et qu'en particulier la caméra ne cible pas une personne en particulier, tel qu'un employé)
[24] Lorsqu'il s'agit d'un logiciel aboutissant à un profilage, il doit respecter les règles de collecte, de stockage, d'échange et d'utilisation des données personnelles (intimité des gens) et permettre aux personnes concernées d'utiliser leurs droits d'accès (y compris du scoring du profilage, s'il y en a un), de communication, de modification et d'opposition. Dans le cadre de toute évaluation systématique et approfondie d'aspects personnels, y compris le profilage, vous devez informer la personne de la légitimité de finalité du traitement et la base sur laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative. Pour la décision automatique (avec ou sans profilage) le R.G.P.D. donne le droit à la personne concernée de s'y opposer, exceptées des conditions d'exception particulières (Article 22 : la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire).
[25] https://www.cnil.fr/fr/PIA-privacy-impact-assessment
[26] ec.europa.eu/newsroom/document.cfm?doc_id=44137
[27] https://www.boutique.afnor.org/norme/nf-en-16571/technologies-de-l-information-processus-d-evaluation-d-impact-sur-la-vie-privee-des-applications-rfid-/article/813483/fa178856
[28] http://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf
[29] http://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
[30] http://www.cnil.fr/sites/default/files/atoms/files/check_list.pdf
[31] http://www.cnil.fr/sites/default/files/atoms/files/check_list.pdf

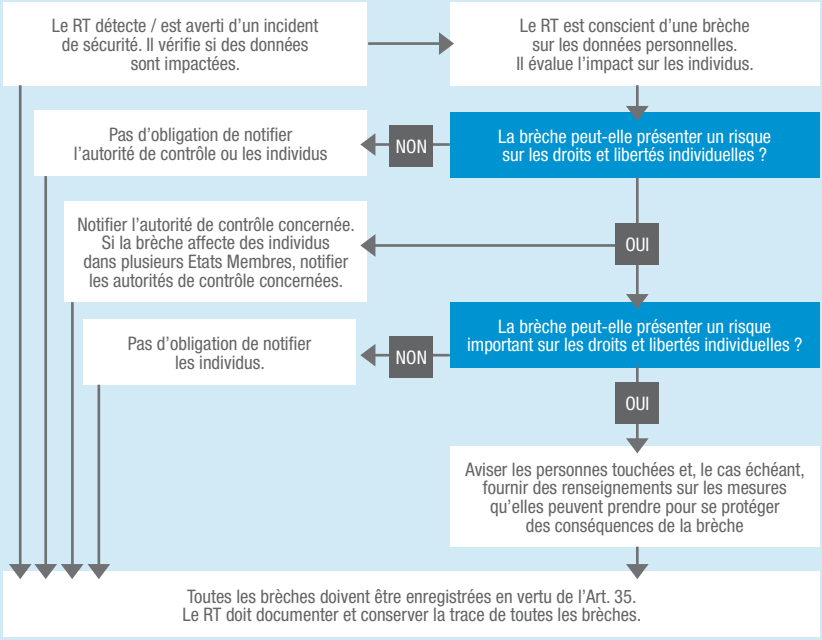
La sécurité nécessite de recenser les traitements de données à caractère personnel, automatisés ou non, les données traitées (ex. : fichiers client, contrats) et les 4 types de supports sur lesquels elles reposent :

- les matériels (ex : serveurs, ordinateurs portables, disques durs) ;
- les logiciels (ex : système d'exploitation, logiciel métier) ;
- les canaux de communication (ex : fibre optique, Wi-Fi, Internet) ;
- les supports papier (ex : document imprimé, photocopie).

Je vérifie avoir mis en place une procédure de notification à l'autorité de contrôle et d'information des personnes concernées en cas de violation de données à caractère personnelsont pris en compte et traités.

Réflexe 7
Je prévois une procédure de notification des failles et violations de données personnelles

La procédure de notification doit suivre le flow chart suivant :



2.5 - ETAPE 5 : PRENDRE EN COMPTE LES PROCÉDURES INTERNES

Le projet doit également prendre en compte les procédures internes, notamment pour :

- sensibiliser et organiser la diffusion d'information en construisant notamment un plan de formation et de communication auprès de vos collaborateurs ;
- intégrer, si nécessaire, la prise en compte du traitement des réclamations et des demandes des personnes concernées quant à l'exercice de leurs droits (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen) ;
- anticiper les violations de données en prévoyant, dans certains cas, la gestion de la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais par l'intermédiaire des entités compétentes.

Pour cela, je m'appuie sur mon DPO, le service juridique et l'entité en charge de la sécurité du système d'information. Je fais éventuellement appel à un spécialiste de la communication de crise.

2.6 - ETAPE 6 : DOCUMENTER LA CONFORMITÉ

Mon projet doit documenter les mesures prises pour protéger les données personnelles tout au long du cycle de vie du traitement.

Mon dossier devra notamment comporter les éléments suivants :

- Les informations utiles pour les registres des traitements (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants) ;
- Les analyses d'impact sur la protection des données (PIA) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes ;
- l'encadrement des transferts de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications) ;
- les mentions d'information des personnes concernées (mention dans l'application, mention dans les CGU/CGV ou les modes d'emploi…) ;
- les modèles de recueil du consentement des personnes concernées et je m'assure de pouvoir collecter les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.
- les procédures mises en place pour l'exercice des droits des personnes concernées
- les contrats avec les parties prenantes et les clauses de protection des données personnelles ; en cas de sous-traitance, je m'assure que le contrat qui me lie à mon sous-traitant respecte les dispositions impératives fixées par le Règlement. Je n'oublie pas que, même en cas de sous-traitance, je reste responsable - en tant que RT - de la violation des dispositions légales.
- les procédures internes en cas de violations de données

Lorsque j'y suis soumis ou que je m'y soumets volontairement, je tiens à jour mon Registre des Traitements.

Le responsable de traitement mais aussi le sous-traitant et, le cas échéant, le représentant du sous-traitant, doivent (sauf dérogation liée à la taille de l'entreprise) tenir un registre des activités de traitement dont les rubriques sont fixées par le règlement.

Ce registre doit impérativement être tenu à jour et doit pouvoir être présenté en cas de requête d'une Autorité de Contrôle.

Le registre doit impérativement contenir un certain nombre de mentions et doit revêtir une forme écrite (manuscrite ou électronique).

Selon que le registre est tenu par le RT ou un sous-traitant, ce registre doit contenir les rubriques suivantes :

- Pour le responsable de traitement :

  - le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
  - les finalités du traitement ;
  - une description des catégories de personnes concernées et des catégories de données à caractère personnel ;
  - les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
  - le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;
  - dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
  - dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

- Pour le sous-traitant :

  - le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;
  - les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
  - le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;
  - dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

Un modèle de registre est disponible sur le site de la CNIL[32].

Il est intéressant de noter que ce registre permet aussi de procéder à une revue d'implémentation du Règlement en fin de processus.

Le registre de traitements doit être actualisé et révisé à chaque modification ou changement d'une opération dans le traitement des données qui a un impact sur le respect de la réglementation.

Une modification de l'objet ou du flux d'information issus d'un objet connecté peut entraîner des changements dans la définition du traitement des données ; le registre pourra donc aussi être impacté et à actualiser lors d'un changement du matériel utilisé, que ce changement soit au niveau de l'électronique, du logiciel embarqué ou du flux de communication contenant les données personnelles.

En sus, le responsable de traitement doit tenir un registre de toutes les failles, notifiées ou non, avec le détail :

- des causes, de l'évènement, et du type de données personnelles concernées par la faille
- des effets et des conséquences de la faille
- du plan d'action mis en place pour traiter le problème

[32] *http://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles*

Le G29 recommande que l'entreprise documente aussi les mesures prises en réponse à une faille, et en particulier les justifications pour ne pas avoir notifié ou avoir pris du retard dans la notification.

Réflexe 8
Je documente tout le processus et les étapes 1 à 6 pour apporter les preuves de conformité nécessaires tout au long du cycle de vie du traitement.

2.7 - CONCLUSION SUR LES 6 ÉTAPES : LES 8 RÉFLEXES À AVOIR

Les principes du « privacy by design » (cf. chapitre 3) ou de « protection des données dès la conception et par défaut » deviennent obligatoires avec le règlement européen 2016/679 applicable dès le 25 mai 2018.

Les mesures sont à la fois organisationnelles, techniques et juridiques (contrats de sous-traitance, fournisseurs, ...).

Elles concernent des solutions à mettre en œuvre de façon opérationnelle dans les projets.

Les chefs de projet ont des responsabilités dans cette mise en œuvre.

Cependant, leur application opérationnelle pose encore de nombreuses questions auxquelles la gouvernance interne comme les autorités de contrôle devraient encore apporter des réponses. Il est donc important d'être vigilant sur les évolutions et de vérifier les mises à jour de préconisations, avis ou décisions de la CNIL et du G29.

Les risques de sanction, beaucoup plus importants, conduisent à faire un diagnostic des mesures actuelles de traitement des données et à préparer les organisations pour 2018.

Des réflexes appropriés facilitent cette transformation à travers une méthodologie recommandée par la CNIL pour se préparer en six étapes.

Parmi les réflexes à adopter, nous en avons retenu huit essentiels dans ce guide :

- **Réflexe 1** : Je m'assure du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de mon traitement de données dès sa conception, et je nomme un DPO si besoin (interne ou externe).
- **Réflexe 2** : Pour mon traitement de données personnelles, je me pose les bonnes questions et en cas de doute, je contacte mon DPO ou service juridique et sécurité habituel.
- **Réflexe 3** : Je suis vigilant sur les transferts hors UE.
- **Réflexe 4** : La durée de conservation des données est définie et tient compte du contexte juridique. Une purge est prévue à la fin du traitement.
- **Réflexe 5** : Dès la conception du traitement, je m'assure de la prise en compte des mesures adéquates pour protéger les données personnelles et respecter les droits des personnes.
- **Réflexe 6** : Je mène une analyse de risque adaptée à la sensibilité de mon traitement afin de garantir des mesures adéquates.
- **Réflexe 7** : Je prévois une procédure de notification des failles et violations de données personnelles.
- **Réflexe 8** : Je documente tout le processus et les étapes 1 à 6 pour apporter les preuves de conformité nécessaires tout au long du cycle de vie du traitement.

2.8 - CODES DE CONDUITE, LABELLISATION ET NORMALISATION

Au-delà de l'application de cette méthodologie, il est également possible de s'astreindre au respect de codes de conduites approuvés ou d'un mécanisme de certification qui peuvent servir à démontrer le respect des obligations incombant au responsable du traitement.

Des mécanismes de certification ainsi que des labels et des marques en matière de protection des données seront probablement mis en place afin de permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.

Un guide de l'AFNOR[33] intitulé « Protection des données personnelles : l'apport des normes volontaires » a été publié en début d'année 2017 dans le but d'informer sur l'état de la technique en rapport avec les procédures de protection des données à caractère personnel ayant pour vocation de pointer les normes pertinentes et d'en expliciter les usages.

Ce guide AFNOR apporte un éclairage sur les normes dédiées à la protection des données personnelles issues de l'ISO/IEC[34]. Les normes produites ont plusieurs objectifs. Par exemples, la norme ISO/IEC 29100[35] (Privacy Framework) définit les principes et la terminologie relatifs à la protection de la vie privée. Elle constitue le socle des autres normes. L'ISO/IEC 29134 (Privacy Impact Assessment - Methodology) a pour objectif de fournir un cadre pour mener des analyses d'impact sur la vie privée. La norme ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds) concerne les sous-traitants chargés des traitements de données personnelles pour le compte d'un responsable de traitements. Pour l'avenir, les priorités sont d'établir :

- une norme d'exigences afin de réaliser des certifications de systèmes de management intégrant la protection de la vie privée. C'est l'objectif du projet ISO/IEC 27552. (Extension to ISO/IEC 27001 for privacy management - Requirements).

- une norme sur une pratique d'ingénierie privacy-by-design. C'est l'objectif du projet ISO/IEC 27550

- une norme fournissant un guide spécifique pour la sécurité et la protection de la vie privée pour l'IdO.

En ce qui concerne les mesures techniques normalisées, elles reposent essentiellement sur la cryptographie dont le rôle est central dans la mise en place de solutions respectueuses de la vie privée. Ainsi, des primitives cryptographiques ont été créées et sont regroupées dans ce que l'on désigne couramment aujourd'hui sous l'appellation anglaise de Privacy Enhancing Technologies (PETs). On peut citer les signa-tures de groupe, objet de la norme ISO/IEC 29191 publiée en 2012, ou les signatures aveugles avec la norme ISO/IEC 18370.

[33] Afin de rendre accessible ce guide à tout utilisateur, notez que sa mise à disposition est gratuite : http://normalisation.afnor.org/actualites/protection-donnees-personnelles-guide-afnor-recense-normes-incontournables/ (url vers le guide en fin d'article).
[34] ISO/IEC JTC 1/SC 27/WG5 Information technology - Security techniques - Identity management and privacy technologies
[35] http://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip

3

PRIVACY BY DESIGN : DU CONCEPT À LA MISE EN PRATIQUE

3.1 - RÉFÉRENCE AU RÈGLEMENT R.G.P.D.

La prise en compte de la protection des données personnelles dès la conception d'un nouveau produit ou service est au centre du nouveau règlement européen. Le « considérant n°78 » présente les principes de protection des données dès la conception (Privacy by design) et de protection des données par défaut (Privacy by Default) comme essentiels pour permettre au responsable de traitement de garantir la conformité au règlement. La mise en pratique de ces principes exige l'adoption de mesures techniques et organisationnelles, mesures qui ne sont que très peu détaillées dans le « considérant n°78 » ou même dans l'article 25. A titre d'exemple, il est proposé de :

- réduire à un minimum le traitement des données à caractère personnel,
- pseudonymiser les données à caractère personnel dès que possible,
- garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel,
- permettre à la personne concernée de contrôler le traitement des données,
- permettre au responsable du traitement de mettre en place des dispositifs de sécurité et de les améliorer de façon continue,

sans que cette liste soit exhaustive.

L'article 25 indique également que l'étendue de ces mesures dépend de certains critères tels que :

- l'état des connaissances,
- les coûts de mise en œuvre
- la nature, la portée, le contexte et les finalités du traitement
- les risques, définis par un degré de probabilité et de gravité

Ce dernier point est intéressant puisqu'il indique que les risques doivent être évalués afin de mettre en place des mesures adaptées. Cette évaluation, appelée généralement évaluation d'impact sur la vie privée (EIVP) ou encore Privacy Impact Assessment (PIA) en anglais, est, suivant certains critères, rendue obligatoire selon les termes de l'article 35.

Dans son dernier paragraphe, l'article 25 indique qu'un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect de ces exigences. Néanmoins, avant de pouvoir certifier quoi que ce soit, et garantir que les principes de Privacy by Design et Privacy by Default ont été respectés, il faut savoir :

- Quels sont les droits fondamentaux qui doivent être respectés
- Quels sont les bases du concept de Privacy by Design
- Quelles sont les mesures techniques ou organisationnelles qui peuvent être mise en place
- Comment évaluer les risques

3.2 - PRINCIPES DU « PRIVACY BY DESIGN » (PBD)

L'origine du concept de « Privacy by design » vient de l'initiative de la préposée à la protection des données

de l'Etat d'Ontario au Canada, Ann Cavoukian. Il est intéressant de se pencher sur les sept principes fondamentaux qui s'appliquent à toutes les catégories de données à caractère personnel comme à tout type de mesures mises en place pour protéger la vie privée. Ces principes sont à mettre en perspective avec les droits fondamentaux énumérés précédemment.

- **Des mesures proactives et préventives**

Ce premier principe montre qu'une approche PbD ne peut se concevoir que dès la conception d'un projet. Inutile de chercher, parmi les autres principes, des mesures correctives en cas d'atteinte à la vie privée. Une telle proactivité ne peut donc se concevoir que si toutes les parties prenantes à un projet sont réellement engagées dans la démarche.

- **Une protection implicite et automatique**

Si la protection de la vie privée est implicite, cela implique que les personnes concernées n'ont aucune action à réaliser pour être protégées. Ce principe, repris spécifiquement dans le règlement européen au second paragraphe de l'article 25, est connu sous le nom de « Privacy by Default ».

- **Une intégration de la vie privée dans la conception des systèmes et au cœur des pratiques**

Ce troisième principe renforce le premier en indiquant clairement que la protection de la vie privée doit se concevoir dès la conception du projet. Cela doit être une composante à part entière du produit ou de la solution.

- **Une protection intégrale**

L'idée de ce principe est d'éviter les discussions stériles qui opposent la protection de la vie privée et certains impératifs de business ou de sécurité. Il peut se résumer au fait que protéger la vie privée est la seule valeur ajoutée qui permette réellement d'instaurer la confiance avec les utilisateurs.

- **Une sécurité de bout en bout, durant toute la durée de la conservation des données**

Ce principe met l'accent sur le fait que la protection des données personnelles doit être assurée jusqu'à la fin de la durée de conservation, durée qui doit être en adéquation avec les finalités du traitement. Le processus de destruction de ces données doit être sécurisé.

- **La garantie de la visibilité et de la transparence**

Ce principe vise clairement à faire en sorte que la confiance puisse être garantie (et vérifiable) à tout moment et pas uniquement à la mise sur le marché du produit ou service. Le règlement européen reprend ce principe aux articles 12, 13 et 14.

- **Le respect de la vie privée des utilisateurs (en privilégiant les intérêts des particuliers)**

Ce dernier principe est très général puisqu'il demande aux concepteurs et fournisseurs de produits ou services,

de toujours privilégier les intérêts des individus. Le corollaire de ce principe est que le respect de la vie privée ne peut se résumer à la mise en place de mesures de sécurité et protection des données personnelles.

La prise en compte et le respect des sept principes fondamentaux de la « Privacy by Design » ont pour objectif de rendre à la personne concernée le contrôle de ses données à caractère personnel. C'est la raison pour laquelle, le règlement européen est fortement basé sur ce concept.

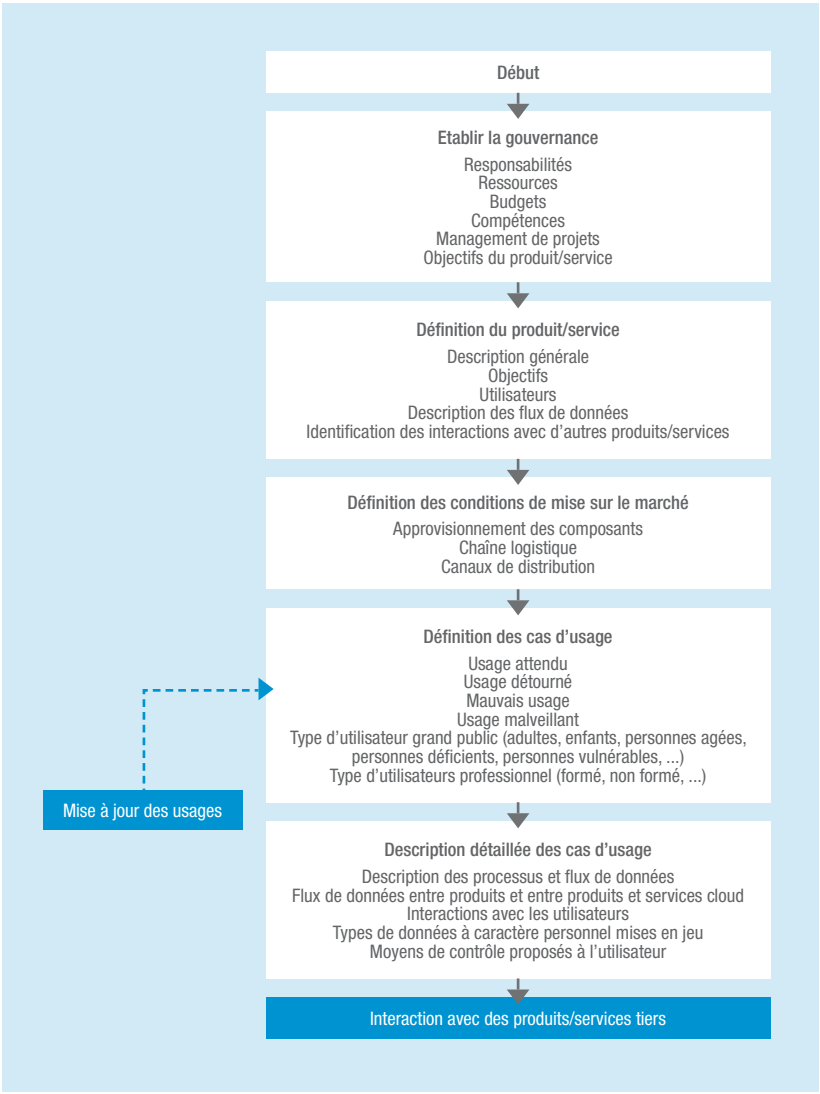
Cela implique de penser la protection des données personnelles dès la conception :

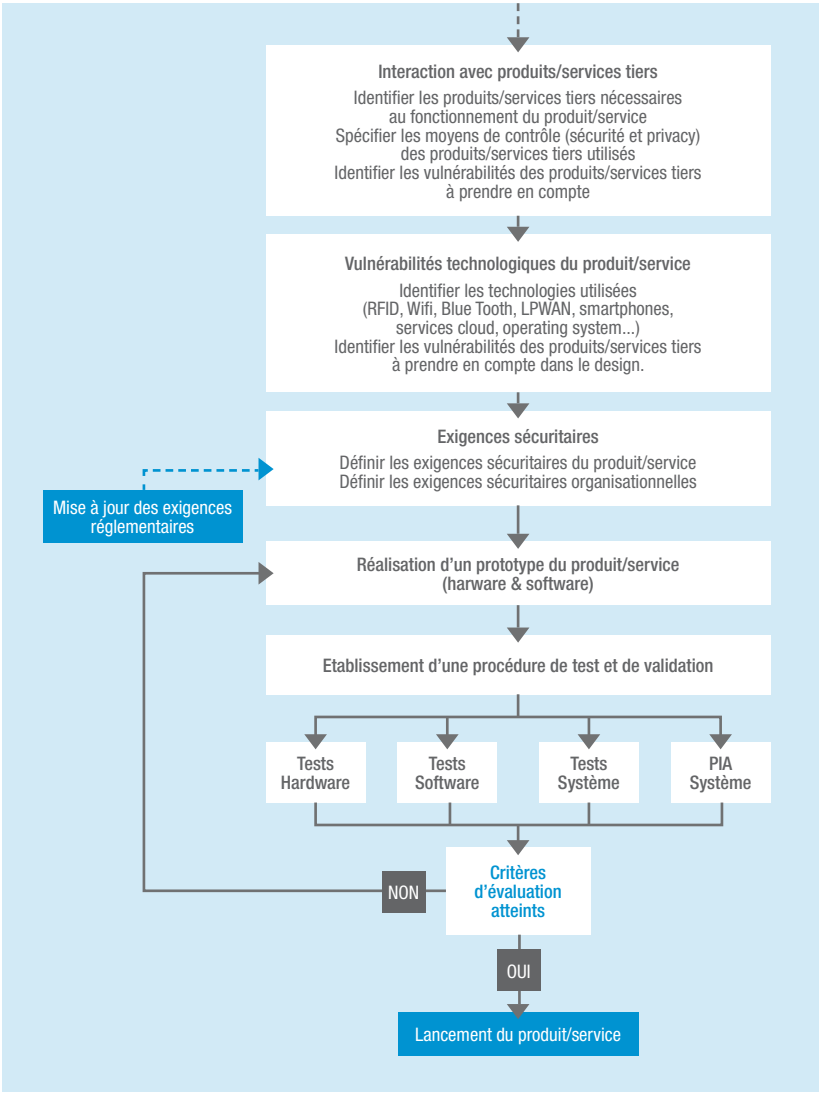
- des objets connectés, tant au niveau du matériel que du logiciel embarqué,
- de la communication et des échanges des données vers des systèmes d'information
- des systèmes d'information qui traiteront et exploiteront ces données
- des processus et des activités et de l'organisation des Métiers utilisant ces données

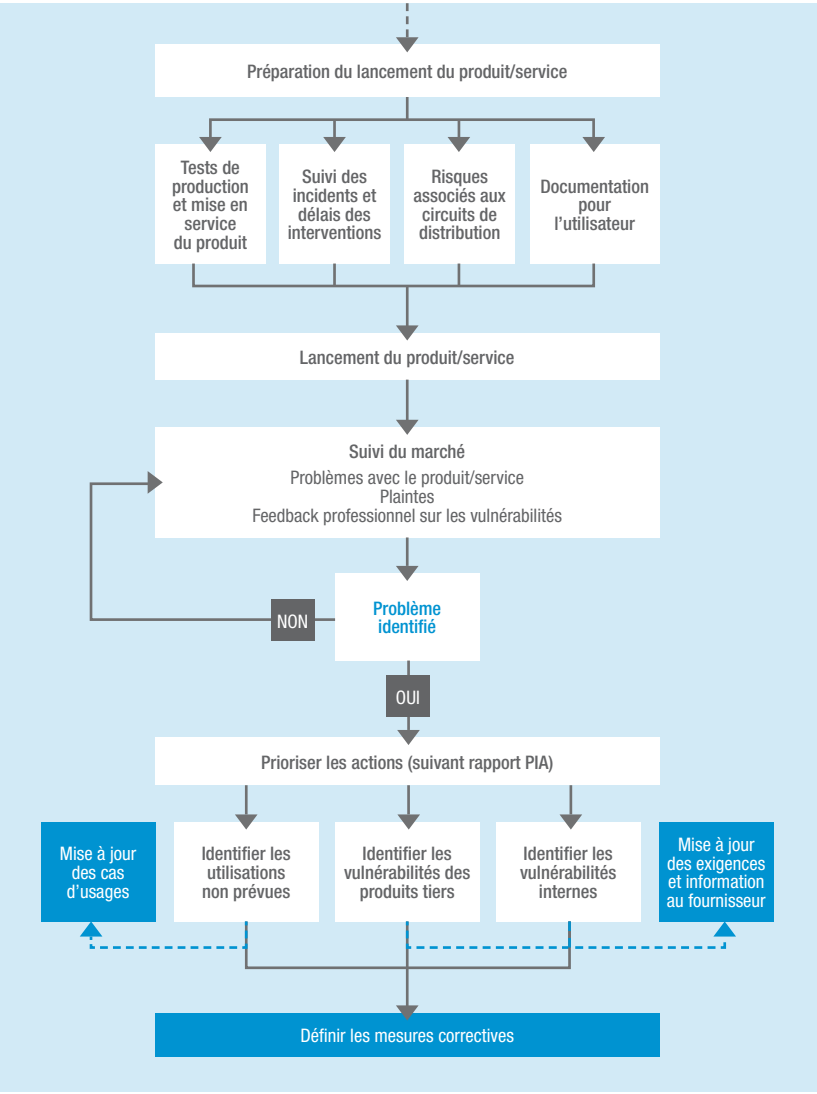
Le paragraphe suivant propose une méthodologie permettant de mettre en place le concept de « Privacy by Design ». Cette méthodologie peut s'apparenter à celle à mettre en œuvre dans une démarche qualité. Dans ce cadre, il peut être intéressant de regarder les mesures proposées par la CNIL dans son guide des « mesures pour traiter les risques sur les libertés et la vie privée ». Comme indiqué précédemment, ces mesures doivent être en adéquation avec le niveau de risque encouru. Il est donc nécessaire de présenter une méthode simple mais efficace permettant d'évaluer ce risque. Il est, dans tous les cas, obligatoire que le cahier des charges de tout nouveau produit ou service impose aux développeurs internes et aux sous-traitants de respecter les principes fondamentaux du R.G.P.D. (cf. chapitre 1) tout au long de la vie du projet (de la conception à la fin de vie du produit).

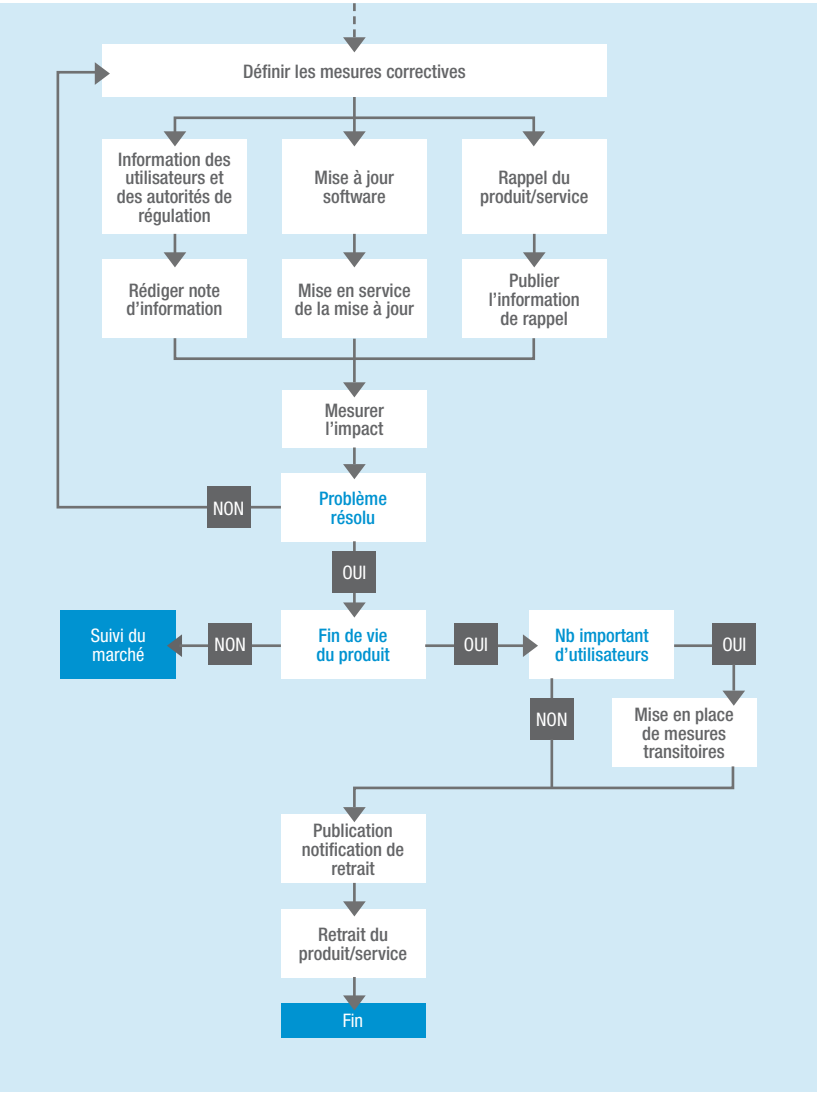
3.3 - PROCESSUS « PRIVACY BY DESIGN »

Plutôt qu'avec un long discours, nous avons choisi dans ce document de présenter le processus sous la forme d'un logigramme, présentant les étapes et les actions à réaliser.


Début
Etablir la gouvernance
Responsabilités
Ressources
Budgets
Compétences
Management de projets
Objectifs du produit/service
Définition du produit/service
Description générale
Objectifs
Utilisateurs
Description des flux de données
Identification des interactions avec d'autres produits/services
Définition des conditions de mise sur le marché
Approvisionnement des composants
Chaîne logistique
Canaux de distribution
Définition des cas d'usage
Usage attendu
Usage détourné
Mauvais usage
Usage malveillant
Type d'utilisateur grand public (adultes, enfants, personnes agées, personnes déficients, personnes vulnérables, ...)
Type d'utilisateurs professionnel (formé, non formé, ...)
Mise à jour des usages
Description détaillée des cas d'usage
Description des processus et flux de données
Flux de données entre produits et entre produits et services cloud
Interactions avec les utilisateurs
Types de données à caractère personnel mises en jeu
Moyens de contrôle proposés à l'utilisateur
Interaction avec des produits/services tiers


Interaction avec produits/services tiers
Identifier les produits/services tiers nécessaires au fonctionnement du produit/service
Spécifier les moyens de contrôle (sécurité et privacy) des produits/services tiers utilisés
Identifier les vulnérabilités des produits/services tiers à prendre en compte
Vulnérabilités technologiques du produit/service
Identifier les technologies utilisées (RFID, Wifi, Blue Tooth, LPWAN, smartphones, services cloud, operating system...)
Identifier les vulnérabilités des produits/services tiers à prendre en compte dans le design.
Exigences sécuritaires
Définir les exigences sécuritaires du produit/service
Définir les exigences sécuritaires organisationnelles
Mise à jour des exigences réglementaires
Réalisation d'un prototype du produit/service (harware & software)
Etablissement d'une procédure de test et de validation
Tests Hardware
Tests Software
Tests Système
PIA Système
Critères d'évaluation atteints
NON
OUI
Lancement du produit/service


Préparation du lancement du produit/service
Tests de production et mise en service du produit
Suivi des incidents et délais des interventions
Risques associés aux circuits de distribution
Documentation pour l'utilisateur
Lancement du produit/service
Suivi du marché
Problèmes avec le produit/service
Plaintes
Feedback professionnel sur les vulnérabilités
NON
Problème identifié
OUI
Prioriser les actions (suivant rapport PIA)
Mise à jour des cas d'usages
Identifier les utilisations non prévues
Identifier les vulnérabilités des produits tiers
Identifier les vulnérabilités internes
Mise à jour des exigences et information au fournisseur
Définir les mesures correctives


Définir les mesures correctives
Information des utilisateurs et des autorités de régulation
Mise à jour software
Rappel du produit/service
Rédiger note d'information
Mise en service de la mise à jour
Publier l'information de rappel
Mesurer l'impact
Problème résolu
NON
OUI
Suivi du marché
NON
Fin de vie du produit
OUI
Nb important d'utilisateurs
OUI
NON
Mise en place de mesures transitoires
Publication notification de retrait
Retrait du produit/service
Fin

3.4 - EVALUATION DE L'IMPACT SUR LA VIE PRIVÉE : COMMENT LA RÉALISER ?

Le règlement prévoit des cas spécifiques de traitements pour lesquels une analyse d'impact est obligatoire. Dans le cadre de ce guide, nous préconisons de réaliser cette analyse quel que soit le traitement afin de s'assurer que les risques[37] sont bien identifiés et maîtrisés.

Il existe plusieurs approches pour réaliser une EIVP. Toutes ces approches présentent des similitudes quant au processus lui-même. Les différences résident généralement dans la manière d'évaluer le risque. Certaines méthodes proposent une échelle unique (chaque risque à une valeur particulière), d'autres proposent une vision suivant les deux axes de définition d'un risque : gravité et vraisemblance.

A défaut d'outils préconisés par mon entité et/ou mon DPO je peux mener une analyse de risques et une EIVP en suivant les guides :

- de la CNIL [38] (https://www.cnil.fr/fr/PIA-privacy-impact-assessment) et/ou
- du G29 (ec.europa.eu/newsroom/document.cfm?doc_id=44137).
- de l'association internationale des professionnels de la vie privée (IAPP)[39]

Dans tous les cas, quelle que soit la méthode utilisée, cette dernière doit satisfaire les obligations citées dans l'annexe 2 « critères d'acceptabilité » du guide du G29 sur le PIA[40].

Dans ce chapitre, nous présenterons également une méthodologie proposée dans la norme EN 16571 spécialement dédiée aux applications RFID[41].

Aujourd'hui, plusieurs outils informatiques sont disponibles. Ils permettent de simplifier la réalisation d'une EIVP. Connectwave a mis en place un logiciel spécialement dédié aux applications RFID . La CNIL, quant à elle, propose un outil plus général[42].

3.4.1 PROCESSUS

Lorsque le responsable de traitement souhaite réaliser une évaluation de l'impact sur la vie privée, il doit globalement suivre les 9 étapes suivantes :

ÉTAPE 1 : Préparer une description détaillée de l'application. Cette description doit délimiter et décrire le périmètre de l'application. Quelles sont les DCP concernées ? Qui peut y avoir accès ? Quelle est la durée de conservation ? Comment les DCP sont-elles collectées ? Comment les DCP sont-elles gérées lors de la fin de vie de l'application ?...

ÉTAPE 2 : Identifier et attribuer une valeur aux données à caractère personnel utilisées dans l'application. Il faut veiller à bien prendre en compte :

- Les données à caractère personnel d'un individu utilisées par l'application et pouvant être utilisées au-delà du périmètre d'utilisation prévu pour l'application.

[37] Le concept de risque, tel que défini par la Commission européenne, prend en compte deux éléments : La probabilité que survienne un évènement et la sévérité de ses conséquences. Le risque attaché à un événement particulier se caractérise par sa probabilité et par la gravité de ses effets.
[38] La CNIL vient de publier un document dédié à la réalisation d'EIVP pour les applications d'objets connectés : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-fr.pdf
[39] https://iapp.org/lang/fr/#
[40] https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf
[41] http://rfid-pia-en16571.eu/why-use-the-software/how-it-works/
[42] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

- Les dispositifs pouvant être à l'origine d'une violation ou d'une perte de données à caractère personnel dans le cadre d'un traitement de données.

Cette étape permet de mesurer la gravité de l'évènement lorsque celui-ci survient. Ces évènements (redoutés) sont généralement de trois types :

- un accès illégitime aux DCP
- une modification non désirée des DCP
- une disparition des DCP

ÉTAPE 3 : Identifier et évaluer les menaces sur la vie privée. Cette étape concerne toutes les menaces possibles y compris celles pouvant intervenir au-delà du périmètre d'utilisation prévu pour l'application.

Pour évaluer ces menaces, le vecteur d'attaque doit être identifié (interne ou externe) ainsi que les moyens à mettre en œuvre.

Exemples :

- Un responsable des ressources humaines lit à distance les badges RFID des employés à proximité de la salle de repos.
- Un industriel logisticien modifie les données de localisation de la flotte de camion de son concurrent.
- Un employé distrait supprime les droits d'accès de ses collègues en créant un nouveau badge.

ÉTAPE 4 : Identifier les vulnérabilités associées aux menaces et aux données.

Une menace pourra être mise à exécution d'autant plus facilement que la donnée est vulnérable. Combinée à la volonté de nuire et aux capacités de l'attaquant, cela donne une mesure de la vraisemblance de l'évènement.

ÉTAPE 5 : Réaliser une évaluation des risques, dans laquelle le risque est une fonction de la donnée, de la menace et de la vulnérabilité. Certaines méthodes donnent une valeur de risque entre 0 et 8 (EN 16571, ISO/IEC 27005[43]), d'autres présentent le risque sur deux axes : gravité vs. vraisemblance (ISO/IEC 29134[44]).

ÉTAPE 6 : Identifier les mesures de contrôle (techniques ou organisationnelles) à mettre en place afin de limiter les risques.

Lorsque les risques sont jugés trop importants en regard des bénéfices de l'application, il est du devoir du responsable de traitement de mettre en place des mesures permettant de réduire le risque. Ces mesures peuvent être techniques (authentification des personnes ayant accès aux DCP, chiffrement des données encodées sur un support nomade, pseudonymisation des données, etc.) ou organisationnelles (suivi des incidents, gestion des crises, etc.)

ÉTAPE 7 : Déterminer les risques résiduels.

Après application des mesures de contrôle, les risques doivent être réévalués. Si, grâce à ces mesures, la probabilité peut être réduite, elle ne peut jamais complètement disparaitre. On dit généralement que la risque zéro n'existe pas. Le responsable de traitement doit décider de l'acceptabilité ou non des risques résiduels et ce, de manière argumentée, notamment au regard des enjeux préalablement identifiés de l'application.

ÉTAPE 8 : Remplir et signer le rapport d'évaluation de l'impact sur la vie privée.

ÉTAPE 9 : Remplir et signer un résumé d'évaluation de l'impact sur la vie privée à destination des utilisateurs.
Les étapes 2 à 7 font partie d'un processus d'évaluation des risques. Les responsables de traitement doivent faire attention à ce qu'ils considèrent comme données à caractère personnel et doivent être en mesure de prouver qu'ils n'ont pas fait d'impasse.

[43] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742
[44] https://www.iso.org/standard/62289.html

3.4.2 - IDENTIFICATION DES TRAITEMENTS ET CLASSEMENT DES DONNÉES

En considérant les différents aspects de la vie privée (vie privéephysique,comportementale,communications,etc.), l'identification des données à caractère personnel et de leur traitement n'est pas une tâche aussi simple qu'il y paraît. Toutes les données traitées par le système back-end, transférées par canaux de communication ou stockées et/ou traitées directement dans un objet connecté doivent être prises en compte. Le responsable de traitement doit ensuite classer les données et les trier selon leur importance.

Il faut recenser les traitements de données à caractère personnel, automatisés ou non, les données traitées (ex : fichiers client, contrats) et les supports sur lesquels elles reposent :

- les matériels (ex : serveurs, ordinateurs portables, disques durs, objets connectés) ;
- les logiciels (ex : système d'exploitation, logiciel métier) ;
- les canaux de communication (ex : fibre optique, Wi-Fi, Internet) ;
- les supports papier (ex : document imprimé, photocopie).

3.4.3 - IDENTIFICATION ET CLASSEMENT DES MENACES

Les menaces sont intimement liées à ce qu'on appelle les « évènements redoutés ».

Pour la vie privée, il s'agit d'identifier les impacts potentiels sur les droits et libertés des personnes concernées, pour les trois types d'évènements redoutés suivants :

- accès illégitime à des données (ex : usurpations d'identités consécutives à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise) ;
- modification non désirée de données (ex : accusation à tort d'une personne d'une faute ou d'un délit suite à la modification de journaux d'accès) ;
- disparition de données (ex : non détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient).

Il existe de nombreuses définitions d'une menace en fonction de l'agent (vecteur), de ses motivations et parfois d'une partie de vulnérabilité du système. La définition proposée dans le présent document provient d'une version adaptée de celle de l'ENISA :

> *des mécanismes physiques ou de type matériel informatique et logiciel pouvant potentiellement avoir un impact négatif sur un actif par le biais d'un accès non autorisé, d'une destruction, d'une diffusion, d'une modification de données et/ou d'un déni de service.*

Il s'agit d'identifier les menaces réalisables (qu'est-ce qui pourrait permettre qu'un évènement redouté survienne ?). Ces menaces se réalisent via les supports des données (matériels, logiciels, canaux de communication, supports papier, etc.), qui peuvent être :

- utilisés de manière inadaptée (ex : abus de droits, erreur de manipulation) ;
- modifiés (ex : piégeage logiciel ou matériel - keylogger, installation d'un logiciel malveillant) ;
- perdus (ex : vol d'un ordinateur portable, perte d'une clé USB) ;
- observés (ex : observation d'un écran dans un train, géolocalisation d'un matériel) ;
- détériorés (ex : vandalisme, dégradation du fait de l'usure naturelle) ;
- surchargés (ex : unité de stockage pleine, attaque par dénis de service).

Bien entendu, le processus d'identification des menaces pour une application IoT doit considérer les éléments suivants :

- les aspects technologiques : données stockées dans l'objet connecté nomade, protocole d'interface radio hertzienne, couche réseau télécoms, services cloud et couche applicative ;
- les aspects sécuritaires : confidentialité, intégrité et disponibilité des données

Comme pour les données à caractère personnel, toutes les menaces identifiées et concernées par l'évaluation doivent être classées en fonction de leur importance. A titre d'exemple, les menaces les plus connues sont : clonage d'objet connecté, écoute clandestine, « attaque man in the middle », déni de service, code malveillant, etc.

Dans le cadre de l'évaluation des menaces, il est important de prendre en compte les motivations de la personne (ou de l'organisation) à l'origine de l'attaque et des compétences requises pour réaliser ces attaques.

3.4.4 - IDENTIFICATION ET CLASSEMENT DES VULNÉRABILITÉS

Comme pour les menaces, il est important de définir ce qu'est une vulnérabilité. Voici, entre autres, une définition proposée par la norme ITSEC[45] (Information Technology Security Eva-luation Criteria) :

L'existence d'une faiblesse, d'une erreur de conception ou de mise en œuvre pouvant entraîner un événement inattendu ou indésirable nuisible pour la sécurité du système informatique, du réseau, de l'application ou du protocole concerné.

Pour le classement des vulnérabilités, le responsable de traitement peut faire appel aux règles suivantes :

- S'il est impossible de mettre en œuvre une menace, le niveau de risque de vulnérabilité peut être considéré comme « faible ». Par exemple, une attaque par force brute sur un algorithme de cryptographie AES 128.
- Si une menace est identifiée et s'il est possible de l'appliquer au produit/service, alors le niveau de vulnérabilité est considéré comme « moyen ». Il s'agit de menaces principalement mises en œuvre dans le cadre d'un laboratoire de recherche.

- Le niveau de vulnérabilité « élevé » ne s'applique que lorsque des failles connues ont été identifiées dans des cas de figure réels.

3.4.5 - EVALUATION DES RISQUES

Lorsque les données, les menaces et les vulnérabilités (ou autrement dit la gravité et la vraisemblance d'un risque) ont été identifiées et classées, la dernière étape est l'évaluation des risques.

Cette démarche peut être réalisée :

- Suivant la norme EN16571 qui propose une méthode basée sur la norme ISO/IEC 27005. Avec cette approche, les données peuvent avoir une valeur entre 0 et 4. Pour les menaces et les vulnérabilités, les valeurs peuvent être « faible », « moyen » ou « élevé ». L'équation permettant de calculer la valeur de risque est basée sur l'addition des valeurs des données, de menace et de vulnérabilité. Elle est synthétisée dans le tableau ci-dessous. Dans ce tableau, plus le chiffre est élevé, plus le risque est élevé.

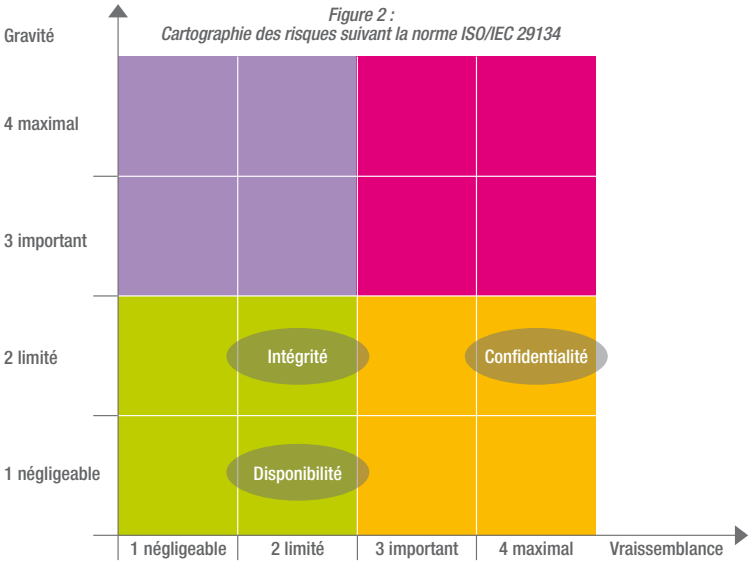
[45] *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile*

	Probabilité de la menace	Faible			Moyen			Elevée		
	Facilité d'exploitation de faille - vulnérabilité	F	M	E	F	M	E	F	M	E
Valeur de la donnée	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	0	3	4	5	4	5	6	5	6	7
	0	4	5	6	5	6	7	6	7	8

Tableau 1 : Matrice d'évaluation des risques basée sur la norme ISO/IEC 27005

- Suivant la norme ISO/IEC 29134 qui représente le risque suivant deux axes : la gravité (impact sur la personne) vs. la vraisemblance (probabilité de l'évènement redouté). Reste à savoir s'il faut traiter les risques les plus graves avec une probabilité faible ou des risques moins graves mais ayant une probabilité plus forte...

Figure 2 :
Cartographie des risques suivant la norme ISO/IEC 29134



3.4.6 - RISQUES RÉSIDUELS

Tous les spécialistes de l'analyse de risques s'accordent à dire que le risque zéro n'existe pas en matière de vie privée. En fonction du seuil défini par le responsable de traitement, certains risques restent non résolus. Ces risques sont appelés « risques résiduels ». Ce concept est défini dans le Guide ISO 73:2009[46].

Bien entendu, plus la valeur des risques résiduels est faible, plus les individus utilisant l'application peuvent être assurés que leur vie privée est protégée. Le responsable de traitement doit calculer le retour sur investissement de la mise en place de mesures de contrôle et de contre-mesures supplémentaires.

3.4.7 - RAPPORT ET RÉSUMÉ DE L'ÉVALUATION DE L'IMPACT SUR LA VIE PRIVÉE

Une fois l'évaluation des risques terminée, la prise de décision finale de mise en place de l'application devra être documentée dans le rapport d'évaluation de l'impact sur la vie privée, accompagnée d'éventuelles remarques concernant les risques, les mesures de contrôle et les risques résiduels.

Les signataires du rapport d'évaluation de l'impact sur la vie privée devront disposer des compétences nécessaires pour comprendre le fonctionnement de l'application et/ou l'autorité requise pour exiger une modification du système, le cas échéant.

Un rapport d'évaluation de l'impact sur la vie privée peut contenir des informations confidentielles concernant la mise en place du produit/service. Le responsable de traitement devra rédiger un résumé d'évaluation de l'impact sur la vie privée s'il désire communiquer les résultats de l'évaluation aux acteurs concernés externes à la société. Ce résumé devra contenir au moins les éléments suivants : la date du rapport d'évaluation de l'impact sur la vie privée, le nom du responsable de traitement, les généralités concernant l'application IoT, les données collectées communiquées, et traitées, le score d'évaluation de l'impact sur la vie privée (calculé grâce au Tableau 1), les limitations des risques et les mesures de contrôle.

Comme indiqué précédemment, l'évaluation de l'impact sur la vie privée est un processus continu qui doit être renouvelé à chaque nouvelle étape de projet ou nouvelle configuration. Les critères de renouvellement du processus pourront être, notamment :

- Des modifications importantes de l'application, comme l'extension du champ d'application.
- Des modifications au niveau du traitement des données à caractère personnel.
- Des signalements de violations de la vie privée identifiées dans des applications similaires.
- La disponibilité d'un nouveau modèle sectoriel, ou d'une mise à jour du modèle utilisé.
- La disponibilité d'une technologie plus avancée. Il est tout de même recommandé de prendre en compte la valeur résiduelle des investissements en cours et la migration vers de nouvelles technologies.
- La réévaluation périodique, au moins une fois par an si possible, de l'évaluation de l'impact sur la vie privée. Si aucun changement important ne s'est produit, il suffit simplement de mettre à jour la date de publication de l'évaluation de l'impact sur la vie privée.

3.4.8 - EXEMPLE D'EIVP

Une évaluation d'impact sur la vie privée a été menée en collaboration avec la CNIL sur une application de badge NFC pour les participants à un congrès professionnel sur la RFID. Ce document est disponible sur le site de Connectwave. Une version équivalente mise en place avec le logiciel de la CNIL est également disponible[47].

[46] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651
[47] http://www.connectwave.fr

3.5 - QUELLES TECHNOLOGIES UTILISER POUR RENFORCER LA PROTECTION DE LA VIE PRIVÉE ?

De nombreux travaux de recherche sont menés depuis plusieurs années sur les technologies permettant d'améliorer la protection de la vie privée, les PETs (Privacy Enhancing Technologies), et un symposium leur est même dédié depuis 2000. Cependant, la transposition de ces travaux dans des produits opérationnels n'est pas immédiate et le niveau de maturité de ces technologies est très variable. Un guide est en préparation par l'ENISA (European Union Agency For Network And Information Security) au niveau européen pour évaluer précisément la maturité des PETs disponibles selon une méthodologie qui a été validée[48]. Lorsque ce guide sera publié, nous y ferons référence dans une prochaine version de ce document.

Nous discutons dans cette section les technologies permettant d'améliorer le respect de la vie privée dans le cadre des activités liées aux objets connectés. Nous identifions trois grandes familles de technologies pertinentes pour la protection de la vie privée dans l'IoT à partir de la catégorisation proposée par[49] :

- protection de la vie privée par confidentialité,
- protection de la vie privée par contrôle,
- protection de la vie privée par transparence.

3.5.1 - APPROCHES PAR CONFIDENTIALITÉ

Les approches par confidentialité recouvrent les solutions pour anonymiser les communications, anonymiser les données et également minimiser la quantité de données collectées.

Notions d'anonymat, pseudonymat, risques de réidentification.

Anonymiser les communications

- Protéger le contenu des communications ainsi que les méta-données de communication (identité, localisation, date, durée, fréquence, volume…).
- Protocoles spécifiques : Mix-Net protocol[50], TOR (The Onion Router)[51], IP 2[52], Turfnet[53] or Blind[54]

Anonymiser les données

- k-anonymat
- l-diversité
- t-closeness
- differential privacy

Minimiser la collecte de données

- méthodes d'agrégation avec chiffrement des données
- perturbation des données ou altération systématique des données par projection, sélection, ajout de données, ajout de bruit, permutation
- obfuscation de données ou modification aléatoire des données par remplacement de valeurs,

[48] *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan, version 1.0, Dec. 2015*
[49] *Danezis, G. and Gürses, S. (2010). A Critical Review of 10 Years of Privacy Technology. In Surveillance Cultures : A Global Surveillance Society?, UK.*
[50] *Chaum D (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. Commun ACM 24(2):84-88*
[51] *Dingledine R, Mathewson N, Syverson PF (2004) Tor: the second-generation onion router. In: 13th USENIX security symposium, San Diego*
[52] *Okagawa T, Nishida K, Miura A (2003) A proposed routing procedure in IP2. In: IEEE 58th VTC, vol 3*
[53] *Schmid S, Eggert L, Brunner M, Quittek J (2005) TurfNet: an architecture for dynamically composable networks. In: Autonomic communication. Lecture notes in computer science, vol 3457. Springer, Berlin*
[54] *Ylitalo J, Nikander P (2006) BLIND: a complete identity protection framework for end-points. In: Security protocols. Lecture notes in computer science, vol 3957. Springer, Berlin*

3.5.2 APPROCHES PAR CONTRÔLE

Méthodes de contrôle d'accès

- Évolution du contrôle d'accès : identity-based access control models, mandatory access control models, role-based access control (RBAC)
- Prise en compte du contexte : Attribute-based access control (ABAC), Enterprise Privacy Authorization Language (EPAL), Extensible Access Control Markup Language (XACML)

Méthodes de contrôle d'usage

- Notion d'obligation
- Notion de « sticky policy »
- Langages pour définir des politiques d'usage : Usage Control (UCON)[55], XACML[56], Ponder2[57]

3.5.3 APPROCHES PAR TRANSPARENCE

Des outils offrant de la transparence aux utilisateurs sont nécessaires pour améliorer la compréhension de quelles données de leur profil sont exposées et offrir aux utilisateurs les moyens pour contrôler ces données. Ces outils doivent répondre à quatre besoins[58] :

- fournir l'information sur l'objet de la collecte, quelles données seront traitées et stockées
- fournir une vue globale de quelles données ont été divulguées, à qui et selon quelle politique
- fournir un accès en ligne direct aux données collectées et comment elles ont été traitées
- fournir aux utilisateurs des moyens de contre-profilage leur permettant de déterminer quelles données sont pertinentes du point de vue du collecteur de données pour identifier des risques potentiels sur leur vie privée.

3.5.4 CHOIX DES MÉTHODES

Nous indiquons ci-dessous quelles techniques peuvent être utilisées au cours du cycle de vie des données issues des objets connectés.

Au moment de la collecte de données de contexte, des techniques de confidentialité et d'anonymisation telles que la k-anonymisation peuvent être utilisées pour protéger des données et empêcher qu'elles soient reliées à l'utilisateur. Cependant, les attaques d'anonymisation ont démontré que ces techniques ne sont pas encore assez sûres [Narayanan and Shmatikov, 2008]. L'approche de vie privée différentielle (differential privacy) a donc proposé d'utiliser plutôt des techniques de perturbation afin de rendre des ensembles de données indiscernables les uns des autres [Dwork, 2006].

Lors du traitement des données de contexte, l'anonymisation peut également être utilisée, ainsi que des techniques de contrôle pour la gestion de l'identité, pour limiter la divulgation des données. Comme indiqué dans [Danezis and Gürses, 2010], des solutions monolithiques et traditionnelles de gestion d'identités ont tendance à freiner une capacité d'auto-émancipation des informations préconisée dans une approche par transparence de la vie privée. Sur cette question, OpenID [OpenID, 2013] et le principe FOAF (Friend-of-a-Friend) des réseaux sociaux sont des approches prometteuses et devraient être approfondies [Danezis and Mittal, 2009].

[55] Lazouski A, Martinelli F, Mori P (2010) Usage control in computer security: a survey. Else-vier Comput Sci Rev 4(2):81–99
[56] OASIS (2012) Extensible access control markup langage (XACML). http://www.oasis-open.org/committees/xacml/
[57] Twidle K, Dulay N, Lupu E, Sloman M (2009) Ponder2: a policy system for autonomous pervasive environments. In: IEEE workshop on policies for distributed systems and networks
[58] Castellucia C, Druschel P, Fischer Hübner S et al. (2011) Privacy, accountability and trust - Challenges and opportunities. Technical report MSU-CSE-00-2, ENISA

De plus, les techniques de minimisation de l'exposition des données telles que la perturbation et l'obfuscation[59] peuvent limiter les violations de la vie privée causées par l'agrégation de données et l'inférence [Agrawal and Srikant, 2000]. Une difficulté rencontrée par les techniques actuelles de protection de la vie privée est de faire face à la variété des mécanismes d'anonymisation et de protection des données pouvant être utilisés tout le long de la chaîne de traitement. Cela nécessite de nouveaux langages de définition et manipulation de politiques.

Dans la dernière étape de présentation des données de contexte et de leur diffusion vers les applications, des risques plus élevés de préjudices à la vie privée existent comme indiqué par Solove [Solove, 2006]. Plusieurs techniques doivent alors être associées comprenant des techniques de confidentialité, de gestion des identités et des politiques de contrôle d'accès et d'usage.

Enfin, des solutions de protection par transparence de la vie privée sont utiles dans toutes les phases de la gestion données collectées. Les utilisateurs doivent avoir le choix des données collectées et traitées et être informés de la façon dont elles seront utilisées et dans quel but. Il y a une tendance claire dans les solutions de protection par transparence de la vie privée pour offrir plus de contrôle aux utilisateurs.

[59] *Stratégie de protection de la vie privée sur internet qui consiste à publier des informations fausses ou imprécises de manière à dissimuler les informations pertinentes.*

En savoir plus sur : www.connectwave.fr

5 avenue de Manéou - 13790 Rousset - France
Tél : +33 (0)4 42 37 09 37 - contact@connectwave.fr
www.connectwave.fr

AVEC LE SOUTIEN DE :