Cahier

n° 35

l'Academie
SCIENCES TECHNIQUES COMPTABLES FINANCIERES

GOUVERNANCE DES DONNEES PERSONNELLES ET ANALYSE D'IMPACT DANS LE CADRE DU RGPD

#RGPD (REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES)
#DPIA (DATA PROTECTION IMPACT ASSESSMENT)
#EIVP (ETUDE D'IMPACT SUR LA VIE PRIVEE)
#ANALYSE DE RISQUE

DECEMBRE 2018

sage

Toute reproduction de la présente publication, partielle ou totale, par quelque procédé que ce soit, destinée à une utilisation collective est interdite sans l'autorisation de l'Académie et constitue une infraction sanctionnée par le code de la propriété intellectuelle. Les auteurs nommés ayant participé à ce guide sont propriétaires et responsables de leurs écrits. Et, à ce titre, ils peuvent faire usage de leurs écrits sans autorisation préalable de l'Académie ou de toute autre personne.

© Tous droits réservés.

EDITO

Ce Cahier de l'Académie est le 2ème sur le sujet de la protection des données personnelles, enjeu majeur pour le respect des libertés de chacun. L'Académie a par ailleurs souhaité poursuivre ses travaux et faire un point d'étape à la lueur de l'entrée en vigueur du RGPD, en mai 2018.

Les technologies numériques de mobilité, de géolocalisation, d'Internet des objets et autre vidéosurveillance font que nous sommes pistés en permanence et que nos données personnelles permettent de tout connaître de chacun.

Et vous l'aurez compris, d'importants enjeux économiques sont derrière ces considérations.

L'Europe a décidé de renforcer les dispositions déjà anciennes sur le traitement des données pour aller plus loin en mettant en cause la responsabilité de ceux qui procèdent à ces traitements mais aussi en simplifiant les démarches administratives. Ainsi le RGPD est entré en application le 25 mai 2018 pour « *renforcer les droits des personnes, responsabiliser les acteurs traitant des données et crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données* ». Le cadre est défini et les entreprises doivent se confronter à cette mise en conformité.

Il s'agit là de s'interroger sur son contrôle interne et l'analyse de risques, des sujets bien connus de l'Académie. Le zoom particulier de ce Cahier de l'Académie sur l'analyse d'impact montre une évolution importante dans le degré de maturité de la gouvernance en matière de données personnelles. Point plutôt positif dans un contexte où la plupart des entreprises n'étaient pas complétement prêtes à l'après 25 mai.

Je salue les membres du groupe de travail de l'Académie, en particulier Alain Bensoussan et Serge Yablonsky ainsi que les représentants des nombreux organismes qui ont apporté leurs expériences et leurs contributions à la réalisation de cet ouvrage.

William NAHUM
Président fondateur de l'Académie des Sciences et Techniques Comptables et Financières

EDITO SAGE

Les groupes de travail thématiques de l'Académie contribuent de façon décisive à enrichir les pratiques de l'ensemble des acteurs dans les entreprises mais aussi de l'économie. Né des métiers du chiffre, Sage est aux côtés de l'Académie depuis sa création pour soutenir ce travail de réflexion, référence majeure pour ses propres développements.

La thématique de ce 35ème Cahier de l'Académie, « Gouvernance des données personnelles et analyse d'impact dans le cadre du RGPD », fait écho à plusieurs titres aux travaux conduits par Sage.

Je voudrais d'abord souligner ici l'importance que nous accordons à ce sujet, central en termes d'équilibre entre l'innovation que nous devons à nos clients et la responsabilité qui est la nôtre en tant qu'acteur économique. La richesse de la production du groupe de travail animé par Alain Bensoussan et Serge Yablonsky en donne de remarquables illustrations.

Pour définir et accompagner sa stratégie de mise en œuvre du RGPD, Sage a réuni une équipe dédiée, validée au niveau de notre Direction Générale et a mis en place une organisation interne et des procédures de gouvernance lui permettant de prendre en compte, au quotidien et au sein de chaque fonction, les obligations découlant du RGPD.

Comme toute organisation, quelle que soit sa taille (TPE ou grande entreprise) et son activité, Sage s'est organisé pour être en conformité avec les nouvelles obligations issues du RGPD. Les solutions logicielles de Sage et les services associés peuvent faire partie des contrôles et des traitements spécifiques que les entreprises clientes de Sage doivent mettre en œuvre pour le suivi de leurs propres obligations relatives au RGPD. A ce titre, Sage a réalisé une action de révision de l'ensemble de ses solutions et de leurs documentations utilisateurs respectives. Des mises à jour ont ainsi été proposées à nos clients afin que ceux-ci puissent intégrer les solutions logicielles de Sage à leurs propres plans de conformité.

Enfin, Sage a à cœur, au-delà de ses produits, d'accompagner les entreprises dans la mise en place du RGPD. Articles de notre blog, livres blancs ou tutoriels apportent aux professionnels du chiffre et aux entreprises un accompagnement pratique, complémentaire, je le crois, aux débats experts dont l'objet du présent numéro des Cahiers de l'Académie est de rendre compte.

Bonne lecture !

Laurence VERITÉ
Directrice juridique Southern Europe, Sage

AVANT PROPOS

A l'heure où nous finalisons la seconde édition de ce Cahier de l'Académie « Gouvernance des données personnelles et analyse d'impact dans le cadre du RGPD », le Règlement général sur la protection des données (RGPD) vient d'entrer en application, et dans son prolongement la loi du 20 juin 2018 relative à la protection des données personnelles[1].

Nul besoin de rappeler que cette réforme majeure impacte en profondeur l'environnement digital des entreprises, même si force est de constater qu'au 25 mai dernier, la prise de conscience de toutes les implications, notamment juridiques et opérationnelles, des changements induits par ce règlement n'était pas, loin s'en faut, générale au sein des entreprises et organisations.

De toute évidence, pour beaucoup d'entre elles, les chantiers de mise en conformité n'avaient débuté que depuis trop peu de temps pour atteindre un niveau de conformité correct à la date fatidique[2].

Pour autant, la mise en conformité au RGPD est un travail au long cours, et l'enjeu réside maintenant, pour ceux déjà en conformité, dans le maintien en condition opérationnelle, qui sous-tend l'idée d'une continuité de la protection au-delà du 25 mai.

Il est question maintenant de la réalisation d'analyses d'impact, au cœur des travaux menés par le groupe de l'Académie, même si la CNIL a dès février 2018 décidé de repousser de trois ans leurs réalisations, pourtant obligatoires au titre du RGPD pour tous les traitements pouvant présenter un risque pour les données à caractère personnel.

Ainsi, en l'état, les études d'impact ne pas sont exigées pour une période de trois ans pour :

- les traitements ayant fait l'objet d'une formalité préalable auprès de la CNIL avant le 25 mai 2018 ;
- les traitements ayant été consignés au registre d'un correspondant Informatique et libertés.

Cette dispense d'obligation d'analyses d'impact pour les traitements en cours régulièrement mis en œuvre, sera limitée dans le temps, comme l'a précisé la CNIL : à l'issue de ce délai de trois ans à compter du 25/05/2018, les responsables de traitement devront avoir effectué une telle étude si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes.

En revanche, l'étude d'impact doit être réalisée, sans attendre l'issue de ce délai de trois ans, dans tous les autres cas, dès lors que le traitement présente un risque élevé :

- pour tout nouveau traitement mis en œuvre après le 25 mai 2018 ;
- pour les traitements antérieurs n'ayant pas fait l'objet de formalités préalables auprès de la CNIL ;
- pour les traitements, antérieurs au 25 mai et qui ont été dispensés d'étude d'impact en raison de l'accomplissement d'une formalité préalable auprès de la CNIL, mais qui font l'objet d'une modification significative.

[1] JO du 21 juin 2018, Loi n°2018-493, loi relative à la protection des données personnelles
[2] F. Forster, RGPD : l'heure H a sonné, EDI Magazine, Juin 2018

Les obligations de procéder à ces études d'impact, celle dite *d'accountability* ou obligation de « rendre des comptes », sont au cœur du RGPD et plus que jamais essentielles.

C'est dans ce sens, à jour de l'évolution des textes et en se confrontant aux retours d'expériences, que les travaux du groupe de l'Académie ont été menés.

Car plus que jamais, au-delà du seul RGPD, l'analyse de risques et l'analyse d'impact relative à la protection des données sont primordiales pour les organismes concernés qui ont tout intérêt à démontrer, comme nous l'avions déjà souligné dans le premier Cahier, que leur écosystème respecte le nouveau cadre juridique de la protection des données à caractère personnel.

Rappelons en effet que le RGPD représente aussi, pour l'entreprise, un facteur de transparence et de confiance vis-à-vis de son environnement avec lequel il faudra compter dans les prochains mois : sa mise en application devrait aussi et surtout avoir un effet positif puisqu'il renforce les obligations de sécurité des entreprises, donnant ainsi à leurs clients l'assurance d'un niveau de protection accru pour le traitement de leurs données à caractère personnel.

Bonne lecture !

Alain Bensoussan

Avocat à la Cour d'appel de Paris

Serge Yablonsky

Expert-comptable Commissaire aux comptes

SOMMAIRE

EDITO 2

EDITO SAGE 3

AVANT PROPOS 4

1 APPROCHE GÉNÉRALE 9

1.1 Préambule 9

1.2 Contexte 9

1.2.1 Le Règlement général sur la protection des données 9

1.2.2 Vers un principe de responsabilité des organismes 10

1.2.3 L'introduction de l'analyse d'impact réalisée à la suite d'une analyse de risque 13

1.2.4 Les problématiques majeures : Quoi ? Qui ? Quand ? 14

1.2.5 Terminologie 15

1.3 Plan 16

2 PÉRIMÈTRE DE L'ANALYSE D'IMPACT 17

2.1 Les traitements présentant un risque élevéc17

2.1.1 La notion de traitement 18

2.1.2 La référence aux droits et libertés des personnes physiques 18

2.1.3 La notion de risque élevé 19

2.1.4 L'évaluation systématique et approfondie d'aspects personnels en vue d'une décision 22

2.1.5 Les traitements à grande échelle de données particulières 24

2.1.6 Les traitements de surveillance 27

2.2 Les listes publiées par les autorités de contrôle 27

2.3 Les dérogations 28

2.4 La liste de la CNIL des traitements soumis obligatoirement à analyse d'impact 30

2.5 Synthèse 31

3 CONDUITE DE L'ANALYSE D'IMPACT 33

3.1 Le déclenchement de l'analyse d'impact 33

3.1.1 Cadre légal 33

3.1.2 La détermination du moment opportun 33

3.1.3 Les risques juridiques d'une analyse d'impact tardive 34

3.2 Une approche continue 36

SOMMAIRE

3.3 Le contenu de l'analyse d'impact **37**

3.4 Les personnes impliquées dans l'analyse d'impact **38**

3.4.1 Le débiteur de l'obligation 38

3.4.2 Le sous-traitant 38

3.4.3 Le délégué à la protection des données 39

3.4.4 Les personnes concernées par le traitement 40

3.5 Le rôle du comité européen et des autorités de contrôle **41**

3.5.1 Les autorités de contrôle 41

3.5.2 Le Comité européen à la protection des données (CEPD) 42

4 CADRE MÉTHODOLOGIQUE ***43***

4.1 Les aspects méthodologiques **43**

4.1.1 Panorama rapide des référentiels ou bonnes pratiques 43

4.1.2 Objectifs et principes clés de l'analyse d'impact relative à la protection des données 45

4.2 Description d'une méthodologie d'analyse d'impact relative à la protection des données à caractère personnel **46**

4.2.1 Présentation d'ensemble 46

4.2.2 Description détaillée 50

4.2.2.1 Impliquer et consulter les acteurs internes et externes pertinents de manière continue 50

4.2.2.2 Identifier le périmètre, documenter le contexte et cartographier les données et les flux de données de façon globale 52

4.2.2.3 Analyser les traitements et données au regard des critères susceptibles d'engendrer un risque élevé 54

4.2.2.4 Détailler le contexte et cartographier précisément les données et les flux de données 57

4.2.2.5 Identifier les mesures de conformité et de suppression ou de réduction des risques 60

4.2.2.6 Cartographier et décrire les risques résiduels et leurs impacts potentiels 63

4.2.2.7 Décrire les risques résiduels acceptés et prévoir la mise en œuvre des actions correctives 66

4.2.2.8 Réaliser une revue générale, constater les risques résiduels, définir les modalités de la revue périodique ou sur événements déclencheurs et rédiger le rapport de PIA et valider 69

4.2.2.9 Revue périodique ou à la suite d'événements déclencheurs, mise à jour et, le cas échéant, correction(s) 70

SOMMAIRE

5 ÉTUDE DE CAS « APPLICATION PROGRAMME DE FIDÉLITÉ » 73

5.1 Présentation générale 73

5.2 Analyse du contexte et cartographie des traitements mis en œuvre 74

5.3 Arbre de décision 79

5.4 Analyse d'impact via le logiciel PIA Cnil 80

6 GLOSSAIRE 95

6.1 Traitement 95

6.2 Finalité 95

6.3 Risque 95

6.4 Responsable du traitemen 96

6.5 Données à caractère personnel 96

6.6 Délégué à la protection des données 96

6.7 Traitement automatisé 97

6.8 Profilage 97

6.9 Autorité de contrôle 97

6.10 Données génétiques 97

6.11 Données biométriques 98

6.12 Données concernant la santé 98

6.13 Proportionnalité 98

6.14 Personne concernée 99

6.15 Sécurité du traitement 99

6.16 Preuve 100

6.17 Sous-traitant 100

6.18 Représentants des personnes concernées 100

7 BIBLIOGRAPHIE INDICATIVE 101

7.1 Textes européens 101

7.2 Travaux du groupe de travail « Article 29 » sur la protection des données 101

7.3 Travaux des autorités de protection des données 102

7.4 Autres 102

COMPOSITION DU GROUPE DE TRAVAIL 103

APPROCHE GÉNÉRALE

CHAPITRE 1

1.1 Préambule

Le présent Cahier de l'Académie a pour objet de définir les grands axes de la méthodologie applicable à l'analyse d'impact relative à la protection des données à caractère personnel. Cette analyse d'impact a été introduite dans le Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, applicable depuis le 25 mai 2018, et abrogeant la directive 95/46/CE (ci-après Règlement général sur la protection des données).

1.2 Contexte

La gouvernance des données fait aujourd'hui partie intégrante de la stratégie d'entreprise et se traduit notamment par la mise en place d'une organisation spécifique et le développement d'outils dédiés.

La mise en place d'une telle stratégie suppose l'adoption par les organismes d'une démarche d'analyse des risques juridiques, techniques et économiques.

Cette démarche est appelée à se généraliser, dans la mesure où elle correspond à l'esprit du Règlement général sur la protection des données, qui vise à réformer la directive n°95/46/CE relative à la protection des données à caractère personnel et à la libre circulation de ces données (ci-après directive 95/46/CE).

1.2.1 Le Règlement général sur la protection des données

Pendant longtemps, la directive 95/46/CE du 24 octobre 1995 a constitué le socle de base relatif à la protection des données à caractère personnel au sein de l'Union Européenne. Composé de 34 articles, ce texte, rédigé sous la forme d'une directive adressée aux Etats membres, visait tout à la fois à introduire un droit à la protection des données à caractère personnel et à garantir la libre circulation de ces données entre les Etats membres[3].

Près de 20 ans après l'adoption de la directive 95/46/CE, les institutions européennes ont réformé ce texte fondateur. Considérant que le cadre juridique posé par la directive 95/46/CE au sein de l'Union européenne apparaissait « satisfaisant en ce qui concerne ses principes et ses objectifs », les institutions européennes n'en ont pas moins relevé « une fragmentation de la mise en œuvre de la protection des données dans l'Union, une insécurité juridique ou le sentiment, largement répandu dans le public, que des risques

[3] Dir. 95/46/CE du 24-10-1995 relative à la protection des données à caractère personnel et à la libre circulation de ces données, JOCE 23-11-1995 L 281 p. 0031 – 0050, considérant (3).

importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne »[4].

En effet, depuis l'adoption de ce texte en 1995, les technologies ont évolué, la place d'Internet dans la vie quotidienne des individus a considérablement grandi et l'utilisation des réseaux sociaux et des objets connectés s'est développée, permettant une augmentation exponentielle du partage des données à caractère personnel. En outre, ces données sont aujourd'hui au centre de l'activité et du modèle économique de nombreux organismes.

Ces évolutions ont créé de nouveaux enjeux pour la protection des données à caractère personnel. La révision du cadre légal de leur protection au sein de l'Union européenne a ainsi eu pour objectifs principaux de mettre en place une harmonisation plus poussée sur le territoire de l'Union, ainsi qu'un cadre juridique plus cohérent. A cela s'est également ajoutée la volonté d'assurer une application rigoureuse des règles.

Dans ce contexte, la Commission européenne a publié, le 25 janvier 2012, une proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Ce texte a fait l'objet de très nombreux amendements de la part du Parlement européen et du Conseil de l'Union européenne. A l'issue d'une phase dite de « trilogue », la Commission, le Parlement et le Conseil se sont accordés sur un texte commun.

Ainsi, le Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, publié au journal officiel de l'Union européenne le 4 mai 2016 est applicable depuis le 25 mai 2018.

S'agissant d'un Règlement et non plus d'une directive, ce texte est d'application directe au sein des différents Etats-membres et vise à plus d'harmonisation et de cohérence dans le corpus de règles applicables à la protection des données à caractère personnel au sein de l'Union européenne. Depuis le 25 mai 2018, les organismes doivent désormais respecter les différentes obligations posées par le Règlement général sur la protection des données et sont susceptibles d'être sanctionnés par les autorités de contrôle nationales en cas de non-conformité.

1.2.2 Vers un principe de responsabilité des organismes

Le Règlement général sur la protection des données introduit de nouvelles obligations pour les responsables de traitements et les sous-traitants, ainsi que de nouveaux droits pour les individus, parmi lesquels notamment :

[4] Règl. 2016/679 du 27-4-2016 considérant 9.

- l'obligation, sous certaines conditions tenant à l'organisme ou aux traitements mis en œuvre, de désigner un délégué à la protection des données[5] ;
- la consécration d'un droit à l'oubli numérique pour les personnes concernées ainsi qu'un droit à la portabilité des données[6] ;
- la création de l'obligation de mettre en œuvre la protection des données dès la conception d'un projet et par défaut[7] ;
- l'introduction de l'obligation de notification des violations de données à caractère personnel[8] ;
- la prise en compte du principe de responsabilité (« accountability[9] »).

Le principe de responsabilité, qui est l'obligation pour un responsable de traitement de rendre des comptes, consiste en un processus permanent et dynamique de mise en conformité d'un organisme à la réglementation sur la protection des données personnelles, grâce à un ensemble de règles contraignantes, d'outils et de bonnes pratiques correspondantes.

Concrètement, cela implique, pour le responsable du traitement :

- de prendre des mesures efficaces et appropriées afin de se conformer au Règlement ;
- d'apporter la preuve, si nécessaire, que les mesures appropriées ont été prises.

Les mesures techniques et organisationnelles attendues de la part des organismes doivent tenir compte de différents facteurs incluant :

- la nature ;
- la portée ;
- le contexte ;
- les finalités du traitement, ainsi que ;
- les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques.

Le principe d'accountability s'accompagne donc d'une approche par les risques. Cette démarche est d'ailleurs directement évoquée dans d'autres articles du Règlement général sur la protection des données concernant :

[5] Règl. (UE) 2016/679 du 27-4-2016 art. 37.
[6] Règl. (UE) 2016/679 du 27-4-2016 art. 17 et 20.
[7] Règl. (UE) 2016/679 du 27-4-2016 art. 25.
[8] Règl. (UE) 2016/679 du 27-4-2016 art. 33.
[9] Règl. (UE) 2016/679 du 27-4-2016 art. 24.

- la protection des données dès la conception :

« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent Règlement et de protéger les droits de la personne concernée. »[10]

- l'obligation d'assurer la sécurité du traitement :

« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. »[11]

- l'obligation de réaliser des analyses d'impact relatives à la protection des données :

« Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. »[12]

Concernant plus particulièrement l'analyse d'impact sur la protection des données, elle est intrinsèquement liée :

- à l'obligation d'assurer la sécurité du traitement, dans la mesure où l'évaluation des risques et l'identification des mesures permettant de faire face aux risques en matière de sécurité constituent l'une des composantes de l'analyse d'impact relative à la protection des données ;
- au principe d'accountability, la réalisation d'une analyse d'impact relative à la protection des données constituant l'une des mesures prises par l'organisme pour se conformer au Règlement général sur la protection des données, et permettant de créer une documentation ayant valeur de preuve juridique de la conformité d'un traitement aux dispositions du Règlement.

[10] Règl. 2016/679 du 27-4-2016 art. 25 § 1.
[11] Règl. 2016/679 du 27-4-2016 art. 32.
[12] Règl. 2016/679 du 27-4-2016 art. 35.

1.2.3 L'introduction de l'analyse d'impact réalisée à la suite d'une analyse de risque

Au titre des mesures qui s'imposent aux responsables du traitement, l'article 35 du Règlement général sur la protection des données rend ainsi obligatoire la réalisation d'une analyse de l'impact de certains traitements envisagés par un organisme sur la protection des données à caractère personnel.

L'article 35 du Règlement fait référence à une terminologie nouvelle en matière de protection des données à caractère personnel, avec notamment l'introduction des notions de « grande échelle », d'« aspects personnels » et surtout de « risque élevé ». L'identification d'un niveau de risque élevé pour les droits et libertés des personnes physiques constitue en effet un préalable nécessaire pour déterminer si une analyse d'impact relative à la protection des données est nécessaire au regard de l'article 35 du Règlement général sur la protection des données.

D'une manière générale, l'obligation de mener des analyses d'impact relatives à la protection des données s'inscrit dans le cadre d'une tendance toujours croissante encourageant l'adoption de règles d'organisation internes plus respectueuses de la vie privée des personnes concernées.

Plusieurs documents à ce sujet ont d'ailleurs été publiés par la Cnil et le Groupe de l'article 29 (ci-après G29)[13], au cours des dernières années[14].

Ainsi, avant même que cette nouvelle obligation ne repose sur un texte juridiquement contraignant, certains organismes avaient déjà entrepris de développer des procédures de gouvernance interne visant à améliorer la maîtrise de leurs traitements complexes, et à gérer les risques que ces traitements peuvent faire peser sur les personnes concernées. Désormais, l'ensemble des organismes visés par le Règlement général sur la protection des données doit mettre en place ce type de procédure, et notamment intégrer dans leurs processus internes la réalisation d'analyses d'impact sur la protection des données.

1.2.4 Les problématiques majeures : Quoi ? Qui ? Quand ?

La mise en place d'analyses d'impact relatives à la protection des données a des conséquences économiques et organisationnelles certaines sur les organismes. L'adoption d'une politique générale de conduite des analyses d'impact au sein d'un organisme nécessite ainsi de répondre aux questions suivantes : Quoi ? Qui ? Quand ? Comment ?

En premier lieu, la définition du périmètre de l'analyse d'impact relative à la protection des données (le « Quoi ? ») apparait déterminante. Elle permet tout d'abord d'identifier les situations susceptibles de présenter le plus de risques pour les droits et libertés des personnes concernées.

En outre, elle présente des enjeux importants en matière de responsabilité des organismes, à travers l'identification des cas dans lesquels l'absence de réalisation d'une analyse d'impact pourra être sanctionnée.

La désignation des acteurs de l'analyse d'impact relative à la protection des données (le « Qui ? ») est également essentielle. Elle répond à des impératifs majeurs tels que la complétude de l'analyse menée ou encore l'acceptation en interne de ses résultats et des actions identifiées comme nécessaires.

De nombreux acteurs peuvent être impliqués dans une analyse d'impact relative à la protection des données. Par exemple, les métiers, le Data Protection Officer (« DPO »), les départements juridiques, informatiques ou les équipes chargées de l'audit au sein de l'organisme peuvent être associés à l'étude. Le rôle de chacun des intervenants doit alors être défini avec soin, afin de permettre une analyse fine, objective et complète des traitements en cause.

[13] Le G29 rassemble les autorités de protection des données au sein de l'Union européenne. Le comité européen de la protection des données (CEPD) instauré par le Règlement général sur la protection des données a remplacé le G29 le 25 mai 2018.
[14] PIA-1, la méthode : Comment mener une étude d'impact sur la vie privée 2-2018 ; PIA-2, les modèles, 2-2018 ; PIA-3, les bases de connaissances, 2-2018 ; Comment réaliser une évaluation d'impact sur la vie privée (EIVP) pour les dispositifs RFID ? Cnil 9-2013 ; L'évaluation d'impact sur la vie privée pour les dispositifs RFID : questions-réponses, Cnil, 26-9-2013.

Le recours à la sous-traitance peut également être envisagé. Par exemple, l'identification et la description de l'ensemble des flux de données à caractère personnel pourraient être confiées à une entreprise tierce, en vue d'obtenir un relevé exhaustif et granulaire des caractéristiques des traitements.

Le recours à la sous-traitance dès la phase de conception d'un produit ou service peut toutefois soulever quelques inquiétudes au sein des organismes, au regard de l'impératif de protection des informations confidentielles. Il apparaît alors essentiel d'encadrer strictement, au sein d'un contrat, l'intervention du prestataire choisi.

Enfin, le moment auquel l'analyse d'impact relative à la protection des données sera déclenchée (le « Quand ? ») doit être clairement défini, afin que cette dernière s'intègre facilement dans les différentes phases de l'avancée d'un projet et de ses évolutions.

Ce moment doit être choisi par l'organisme en prenant en compte différents paramètres essentiels tels que notamment :

- l'importance d'effectuer une analyse d'impact sur un produit suffisamment défini ;
- les risques financiers et juridiques liés à la réalisation d'une analyse d'impact tardive.

La Cnil est venue préciser les traitements pour lesquels une étude d'impact n'est pas exigée. Ainsi une étude d'impact ne sera pas exigée pour :

- les traitements qui ont fait l'objet d'une formalité préalable auprès de la CNIL avant le 25 mai 2018 ;
- les traitements qui ont été consignés au registre d'un correspondant « informatique et libertés ».

Cependant, cette dispense est limitée à une période de 3 ans. Ce délai épuisé, les responsables de traitement devront effectuer une analyse d'impact pour les traitements susceptibles d'engendrer un « risque élevé » pour les droits et libertés des personnes.

Dans ce contexte, un groupe de travail, co-présidé par Serge Yablonsky et Alain Bensoussan, a décidé de se réunir avec pour objectif de définir, sous forme d'un Cahier de l'Académie, les grands axes de la méthodologie applicable à l'analyse d'impact relative à la protection des données.

Le partage de réflexions et d'expériences au sein du groupe de travail a fourni la matière pour la mise à jour du Cahier de l'Académie paru en octobre 2014, suite à l'adoption du Règlement général sur la protection des données.

1.2.5 Terminologie

A ce stade de la présentation, il convient de préciser la terminologie.

En effet, « l'analyse d'impact relative à la protection des données » introduite par l'article 35 du Règlement général sur la protection des données n'est pas un concept complètement nouveau. De nombreux pays – généralement anglo-saxons – comme la Nouvelle-Zélande, l'Australie, le Canada, les États-Unis d'Amérique ou encore le Royaume-Uni l'ont déjà adopté, certains même depuis la fin des années 90. Dans tous ces pays, il apparaît sous la dénomination « Data Privacy Impact Assessment » ou PIA. Dans la version anglaise du Règlement général sur la protection des données, le concept a reçu une autre appellation « Data Protection Impact Assessment » ou DPIA.

Enfin, concernant la traduction française de l'expression « Privacy Impact Assessment », il faut noter que le Canada, dont une des langues officielles est le français, utilise comme traduction l'expression « étude d'impact relative à la vie privée » ou EIVP. Cette dernière expression est parfois aussi utilisée dans des documents français publiés par la CNIL.

Dans un souci de cohérence par rapport au texte du Règlement général sur la protection des données, le groupe de travail a fait le choix d'utiliser en français l'expression « analyse d'impact relative à la protection des données ».

1.3 Plan

Le présent Cahier de l'Académie a pour objet de présenter les résultats des réflexions des membres du groupe de travail, concernant :

- le périmètre de l'analyse d'impact ;
- la conduite de l'analyse d'impact ;
- la mise en œuvre pratique d'une méthodologie d'analyse d'impact ;
- deux cas pratiques.

PÉRIMÈTRE DE L'ANALYSE D'IMPACT

CHAPITRE 2

Les réflexions du groupe de travail ont tout d'abord porté sur la détermination des traitements concernés par « l'analyse d'impact », en application de l'article 35 du Règlement général sur la protection des données.

Il s'est d'abord agi de délimiter le périmètre de cette analyse, en tentant de définir ce qui est inclus et ce qui est exclu de son périmètre.

Le texte précise que l'analyse d'impact s'applique aux traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et définit plusieurs éléments permettant de déterminer les situations correspondantes.

Ces éléments ont été étudiés par le groupe de travail et organisés sous la forme d'un « arbre de décision », permettant aux responsables de traitement, à travers une série de questions, de déterminer si un traitement donné entre ou non dans le champ de l'analyse d'impact. Cet arbre de décision a été conçu comme un outil fonctionnel à la disposition des organismes et son utilisation est illustrée à travers une étude de cas présentée au chapitre 5.

Enfin, concernant la terminologie employée dans l'article 35, les membres du groupe de travail ont considéré que tous les mots utilisés devaient être entendus de manière restrictive, et non énonciative. Une telle interprétation permet de mieux définir le périmètre de l'analyse d'impact et d'augmenter ainsi la sécurité juridique pour les organismes soumis à cette obligation.

2.1 Les traitements présentant un risque élevé

L'article 35 § (1) du Règlement général sur la protection des données dispose que :

- « Lorsqu'un type de traitement, en particulier par le recours à des nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. »

Les « traitements » concernés par l'analyse d'impact sont donc ceux présentant un ou plusieurs « risques élevés » pour « les droits et libertés des personnes physiques ». La nature, la portée, le contexte ou encore la finalité des traitements envisagés sont autant de critères permettant de déterminer si ceux-ci présentent des risques particuliers au regard des droits et libertés des personnes.

CHAPITRE 2

2.1.1 La notion de traitement

Le groupe de travail a noté que la notion de « traitement », reprise dans l'article 35, avait fait l'objet de plusieurs modifications par rapport à la directive 95/46/CE.

Ainsi, la directive 95/46/CE définissait les traitements de données à caractère personnel comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel »[15].

La directive 95/46/CE et l'article 4 §(2) du Règlement général sur la protection des données listent différents types d'opérations devant être considérées comme des traitements de données à caractère personnel.

Deux modifications ont été apportées par le Règlement pour qualifier un traitement de données à caractère personnel :

- l'ajout de la notion de « structuration » et de « limitation » ;
- la suppression de la notion de « verrouillage ».

Dans ce contexte, il est permis de s'interroger sur la question de savoir si l'énumération des différents types d'« opérations » dans le Règlement général sur la protection des données[16] doit être comprise comme étant exhaustive ou non.

Enfin, concernant les traitements inclus dans le périmètre de l'analyse d'impact, il semble que l'article 35 soit susceptible de s'appliquer aussi bien aux traitements automatisés qu'aux traitements non automatisés de données y compris les traitements papier.

2.1.2 La référence aux droits et libertés des personnes physiques

L'article 35 §(1) du Règlement général sur la protection des données énonce que les « traitements » concernés par l'analyse d'impact sont ceux susceptibles d'engendrer un « risque élevé » pour « les droits et libertés des personnes physiques ».

La formulation employée semble suggérer que les traitements inclus dans le périmètre de l'analyse d'impact ne sont pas uniquement ceux qui présentent des risques liés à la protection des données à caractère personnel ou à la protection de la vie privée. En effet, sont concernés tous les traitements présentant des risques pour les « droits et libertés des personnes physiques », cette notion

[15] Dir. 95/46/CE du 24-10-1995 art. 2 b).

[16] L'article 4 §(2) du Règlement général sur la protection des données liste les opérations suivantes : 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 ainsi que l'effacement ou la destruction des données.

apparaissant plus large.

A cet égard, le groupe de travail souligne l'importance d'adopter une approche « multi-droits » de l'analyse d'impact, prenant en compte les différentes règles juridiques applicables aux traitements soumis à l'analyse (droit de la protection des données à caractère personnel mais également droit pénal, droit du travail, droit de la santé...).

Une telle approche permettrait de prendre en compte les incidences globales d'un traitement sur les droits et libertés des individus et d'intégrer l'analyse d'impact dans un processus général de recherche de conformité légale d'un organisme.

La nécessité d'adopter une telle approche est confirmée par le G29, dans ses lignes directrices[17] concernant l'analyse d'impact relative à la protection des données, qui précise que si la référence aux « droits et libertés » des personnes concernées vise principalement les droits à la protection des données et à la vie privée, cette référence doit s'étendre à d'autres droits fondamentaux, tels que la liberté d'expression, la liberté de pensée, la liberté de circulation, la liberté de conscience et de religion ainsi que l'interdiction de toute discrimination.

Il semble toutefois ressortir des exemples du G29 que le caractère « fondamental » des droits et libertés en question soit d'une particulière importance alors même que ce critère ne figure pas au sein du Règlement général sur la protection des données.

2.1.3 La notion de risque élevé

La notion de « risque élevé » ne fait l'objet d'aucune définition dans le Règlement général sur la protection des données. Il est seulement indiqué que ce risque concerne les droits et libertés des personnes physiques.

Au titre de l'article 35 §(1) les éléments devant être pris en compte pour déterminer si des traitements sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques sont :

- la nature du traitement ;
- sa portée ;
- son contexte ;
- ses finalités ;
- le recours à de nouvelles technologies.

[17] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 : Groupe « Article 29 » WP 248 rev.01 du 4-4-2017 et révisées le 4-10-2017

Quelques critères d'appréciation ressortent également du considérant (75) du Règlement général sur la protection des données, qui indique que les risques pour les droits et libertés des personnes physiques peuvent résulter du traitement de données susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral. Ces situations incluent les cas dans lesquels :

- le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important ;
- les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel ;
- le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes ;
- des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels ;
- le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants, ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.

Bien que la terminologie employée soit légèrement différente, il est intéressant de noter que la notion de traitement présentant des « risques particuliers » au regard « des droits et libertés des personnes concernées » figurait dans le Règlement n°45/2001 du 18 décembre 2000[18]. Ce texte dresse une liste des traitements « susceptibles » d'entrer dans cette définition. Ces traitements incluent[19] :

- « les traitements de données relatives à la santé et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté » ;
- « les traitements destinés à évaluer des aspects de la personnalité des personnes concernées, tels que leur compétence, leur rendement ou leur comportement » ;
- « les traitements permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire entre des données traitées pour des finalités différentes » ;
- « les traitements visant à exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat ».

[18] Règl. CE 45/2001 du 18-12-2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JOCE 12-1-2001 L8.
[19] Règl. CE 45/2001 du 18-12-2000, art. 27.

De la même manière, l'article 35 §(3) liste plusieurs types de traitements devant être considérés comme susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, en prenant soin toutefois d'indiquer que cette liste n'est pas limitative (grâce à l'utilisation de l'expression « en particulier »).

Il est important de comprendre que l'analyse d'impact s'accompagne nécessairement d'une analyse préalable de risque. Cette analyse permettra de déterminer le niveau de risque présenté par le traitement, en identifiant les éventuels risques élevés et donc la nécessité ou non de réaliser une analyse d'impact.

Cette idée ressortait d'ailleurs clairement de la proposition du Parlement européen sur le texte du Règlement général sur la protection des données, qui faisait toutefois référence aux traitements susceptibles de présenter des risques « spécifiques ». Le Parlement européen appuyait le principe d'une approche en trois temps, consistant à[20] :

- réaliser une « analyse du risque en ce qui concerne les répercussions potentielles du traitement de données prévu sur les droits et les libertés des personnes concernées, tout en évaluant si les traitements sont susceptibles de présenter des risques spécifiques » ;
- procéder à une analyse d'impact relative à la protection des données en cas de mise en œuvre d'un traitement susceptible de présenter des risques spécifiques listés dans le texte ;
- effectuer régulièrement des examens de la conformité de la protection des données, afin de s'assurer que les actions identifiées lors de l'analyse d'impact sont mises en œuvre.

Le G29 est également venu préciser les éléments pouvant être pris en compte pour déterminer si un risque est élevé[21] en proposant les neuf critères suivants :

- traitement consistant ou aboutissant à une évaluation ou une notation, y compris les activités de profilage et de prédiction, portant notamment sur des «aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements» ;
- l'existence d'une prise de décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;
- traitement utilisé pour observer, surveiller ou contrôler les personnes, y compris la collecte de données via des réseaux ou par la surveillance systématique d'une zone accessible au public ;

[20] Résolution législative du Parlement européen du 12-3-2014, art. 32bis.

[21] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 : Groupe « Article 29 » WP 248 rev.01 du 4-4-2017 et révisées le 4-10-2017

- traitement de catégories particulières de données à caractère personnel ainsi que des données à caractère personnel relatives aux condamnations pénales ou aux infractions ou de données à caractère hautement personnel ;
- traitement de données à grande échelle ;
- croisement ou combinaison d'ensembles de données ;
- traitement de données concernant des personnes vulnérables ;
- utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
- traitements qui, en eux-mêmes, empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Pour le G29, dès lors que le traitement satisfait à deux critères, il nécessitera une analyse d'impact relative à la protection des données. Et, plus le traitement remplira de critères, plus il sera susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une analyse d'impact.

Le G29 ajoute, malgré tout que, dans certains cas, un traitement ne satisfaisant qu'à un seul de ces critères pourrait requérir la réalisation d'une analyse d'impact.

Les critères proposés par le G29 constituent indéniablement un référentiel d'intérêt pour l'évaluation du niveau de risque présenté par un traitement. L'approche proposée par le G29 ne constitue pas pour autant une règle figée, chaque organisme étant libre de mettre en place sa propre grille d'analyse et d'identification du niveau de risque susceptible d'être engendré par un traitement sous réserve que ces critères incluent a minima à ceux recommandés par le G29.Liste indicative des traitements susceptibles d'engendrer un risque élevé

Les réflexions du groupe de travail ont notamment porté sur les trois types de traitements considérés comme susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes physiques, tels que listés à l'article 35§(3) du Règlement général sur la protection des données

2.1.4 L'évaluation systématique et approfondie d'aspects personnels en vue d'une décision

Aux termes de l'article 35 §(3) a) du Règlement général sur la protection des données, l'analyse d'impact est tout d'abord requise en cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques et lorsque cette évaluation est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.

En conséquence, une analyse d'impact relative à la protection des données doit également être effectuée lorsque des données à caractère personnel sont traitées en vue de prendre des décisions relatives à des personnes physiques spécifiques à la suite d'une évaluation systématique et approfondie d'aspects personnels propres à des personnes physiques sur la base du profilage desdites données.

Pour déterminer si l'analyse d'impact sera nécessaire, il convient donc de caractériser l'existence d'une évaluation :

- systématique et approfondie ;
- portant sur les aspects personnels d'une personne physique ;
- fondée sur un traitement automatisé sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.

Se pose la question de savoir ce qu'il faut entendre par « produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ». Dans la version anglaise, il est indiqué « based that produce legal effects concerning the natural person or similarly significantly affect the natural person ».

Selon l'interprétation du groupe de travail, l'atteinte peut recouvrir 2 aspects :

- produire des effets juridiques pour la personne concernée. A cet égard, à titre d'exemple, il est généralement admis que l'exclusion du bénéfice d'un droit, d'une prestation ou d'un contrat est considérée comme produisant des effets juridiques ;
- sans produire des effets juridiques, avoir des conséquences significatives pour la personne concernée.

Le G29 a défini les termes « effets juridiques » ainsi qu'« affectant de manière significative » de façon similaire[22].

Une décision produit des effets juridiques lorsqu'une activité de traitement a un impact sur les droits d'une personne physique tels que sa liberté d'association, son droit de vote ou son droit d'ester en justice. Le G29 précise qu'un effet juridique peut également correspondre à un évènement qui affecte le statut juridique d'une personne physique ou ses droits contractuels.

Une décision affectant de manière significative de façon similaire renvoie, quant à elle, aux situations dans lesquelles les droits et les obligations ne sont pas spécifiquement affectés mais les personnes concernées peuvent tout de même être suffisamment impactées pour que cela requiert une protection particulière.

[22] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 : Groupe « Article 29 » WP 251 rev.01 du 3-10-2017, p. 10 à 11.

Pour que le traitement de données affecte de manière significative une personne physique, son effet ne doit pas être anodin et doit être suffisamment important pour être digne d'attention. En d'autres termes, la décision doit influencer de manière significative les circonstances, le comportement ou les choix de la personne concernée. Dans les cas les plus extrêmes, la décision peut conduire à l'exclusion ou la discrimination de certaines personnes.

Le G29 ajoute que le traitement de données qui n'a qu'un léger impact sur une personne physique peut avoir des conséquences significatives sur une catégorie d'individus telles que les minorités ou les personnes vulnérables. Par exemple, une personne qui a des difficultés financières, et à qui des publicités pour des jeux en ligne sont soumises, pourrait y succomber et potentiellement aggraver sa situation financière.

A titre d'illustration, entreront dans le champ des traitements soumis à analyse d'impact sur ce fondement les traitements de score d'octroi de crédit. Ces traitements sont en général mis en œuvre pour l'ensemble des demandes de crédit adressé à l'établissement bancaire (dès lors qu'il dispose d'un score) et sont donc bien systématiques.

Les traitements de score ont pour objectif d'évaluer, de manière statistique, le risque de défaut de paiement du demandeur, ils sont en général basés sur des données extrêmement précises touchant à la vie personnelle du demandeur. Au-delà de l'analyse de sa situation financière, il peut s'agir d'informations relatives à la situation de son logement, à sa situation maritale. Il y a donc bien une évaluation portant sur les aspects personnels d'une personne physique.

Enfin, le traitement de score d'octroi de crédit peut permettre d'accorder ou de refuser, de manière automatique, le crédit, à tout le moins il s'agit d'un traitement d'aide à la décision. Dès lors, un score de crédit fonde une décision produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.

De même, il pourrait produire des effets non juridiques significatifs par exemple en ayant un impact sur les modalités financières de l'offre de crédit fonction de l'appréciation du risque global par l'établissement bancaire.

2.1.5 Les traitements à grande échelle de données particulières

Aux termes de l'article 35 § (3) b) du Règlement général sur la protection des données, l'analyse d'impact relative à la protection des données est également requise en cas de traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Le spectre des données concernées ne pose pas de difficultés d'interprétation. La notion de « catégorie particulière de données » est définie à l'article 9 du Règlement et correspond aux données révélant l'origine raciale ou ethnique, les opinions politiques, les

convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Concernant la notion de données relatives aux condamnations pénales et aux infractions, le groupe de travail relève la difficulté d'interprétation de cette notion notamment en raison de la position doctrinale de la Cnil qui a une interprétation totalement extensive de cette notion d'infraction qui inclut la donnée « susceptible » de révéler une infraction.

La notion « à grande échelle » pose encore plus de difficultés d'interprétation, malgré les explications du G29.

Dans son considérant 91, le Règlement général sur la protection des données considère que l'analyse d'impact devrait en particulier être réalisée lorsqu'il s'agit d'opérations de traitement « à grande échelle ».

Il apporte quelques premières précisions sur ce qu'il faut entendre par « à grande échelle ».

Doivent être pris en compte :

- le volume de données à caractère personnel ;
- le périmètre de cette collecte (niveau régional, national ou supranational)
- le nombre de personnes concernées.

Le considérant 91 précise que le traitement de données à caractère personnel de patients ou de clients traités par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel ne devrait pas être considéré comme étant à grande échelle.

Dans de tels cas, une analyse d'impact relative à la protection des données ne devrait pas être obligatoire.

Au-delà de ces quelques indications, le Règlement général sur la protection des données ne définit pas le terme de « grande échelle ».

Pourtant, ce terme est particulièrement important, notamment en ce qu'il intervient non seulement pour déterminer la nécessité de réaliser une analyse d'impact mais aussi pour déterminer s'il est ou non nécessaire de désigner un délégué à la protection des données ce qui est particulièrement structurant.

Relevant cette lacune du texte, le G29 recommande de prendre en compte, en particulier, les facteurs suivants :

Il est regrettable de ne pas disposer de seuils afin de disposer de critères objectifs pour déterminer si l'on est, ou non, dans un traitement de données à grande échelle.

Le G29, s'il relève que les traitements de « données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel » concernent des données sensibles ou des données à caractère hautement personnel et des données concernant des personnes vulnérables, considère que la réalisation d'une analyse d'impact n'est pas nécessaire.

Le groupe de travail s'étonne d'une telle position s'agissant de données hautement personnelles et/ou sensibles et susceptibles de concerner des personnes vulnérables.

2.1.6 Les traitements de surveillance

Aux termes de l'article 35 § (3) c) du Règlement général sur la protection des données, l'analyse d'impact relative à la protection des données est encore requise en cas de surveillance systématique à grande échelle d'une zone accessible au public.

Le G29 précise qu'il s'agit des traitements utilisés pour observer, surveiller ou contrôler les personnes concernées, y compris la collecte de données à caractère personnel via des réseaux ou par la surveillance systématique d'une zone accessible au public.

Pour le G29, s'entend comme « systématique » toute surveillance qui remplit un ou plusieurs des critères suivants :

- se déroule selon un système ;
- préparée, organisée ou méthodique ;
- se déroule dans le cadre d'un plan général de collecte de données ;
- réalisée dans le cadre d'une stratégie.

Une « zone accessible au public » doit, toujours selon le G29, s'entendre comme tout lieu, quel qu'il soit, ouvert à tout un chacun, tel qu'une place, un centre commercial, une rue, un marché, une gare ou encore une bibliothèque publique, par exemple.

Ce type de surveillance présente un niveau de risque élevé dans la mesure où elle est susceptible d'intervenir dans des circonstances telles que les personnes concernées ne savent pas qui collecte leurs données et la manière dont elles seront utilisées. En outre, le risque réside également dans le fait qu'il peut être impossible pour les personnes de se soustraire à un tel traitement dans l'espace considéré.

Dans son considérant 91, le Règlement général sur la protection des données précise que c'est en particulier le cas lorsque des dispositifs optoélectroniques sont utilisés.

Concernant la notion de « à grande échelle », elle a été développée dans le paragraphe précédent[23].

2.2 Les listes publiées par les autorités de contrôle

Le Règlement général sur la protection des données prévoit que l'autorité de contrôle doit établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

[23] Cf. 2.2.2

Elle a également la possibilité d'établir et de publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

La Cnil devrait donc publier de telles listes en application du règlement général sur la protection des données.

Il convient de souligner qu'elle a l'obligation de publier une liste des opérations de traitement nécessitant une analyse d'impact. En revanche, ça n'est pas une obligation de publier une liste pour les opérations ne nécessitant pas une telle analyse.

En France, la Cnil devrait donc publier, à tout le moins, une liste des opérations de traitements nécessitant une analyse d'impact.

A cet égard, le G29 indique que lorsque le traitement figure dans la liste facultative des opérations de traitement qui ne requièrent pas d'analyse d'impact, cette liste peut recenser les activités de traitement conformes aux conditions fixées par l'autorité en question, en particulier par l'intermédiaire de lignes directrices, de décisions ou autorisations spécifiques, de règles de conformité, etc.

Aussi, il semble que les dispenses, normes simplifiées, autorisations uniques et les packs de conformité faisant l'objet de délibérations de la Cnil vont demeurer particulièrement structurants pour guider les responsables de traitement dans la manière de réaliser leurs traitements. Dès lors que ce cadre de référence de la Cnil est strictement respecté en tous points, il ne sera pas nécessaire d'effectuer une analyse d'impact.

2.3 Les dérogations

L'analyse d'impact n'est pas nécessaire dans les cas suivants :

- quand le traitement ne présente pas de risque élevé pour les droits et libertés des personnes concernées ;
- lorsque la nature, la portée, le contexte et les finalités du traitement envisagé sont très similaires à un traitement pour lequel une analyse d'impact a déjà été menée ;
- quand le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public (art 6.1.c 6.1.e), sous réserve que les conditions suivantes soient remplies :
  - qu'il ait une base juridique dans le droit de l'UE ou le droit de l'État membre ;
  - que ce droit réglemente cette opération ou l'ensemble d'opérations de traitement considéré ;
  - et qu'une analyse d'impact ait déjà été menée lors de l'adoption de cette base juridique.

Toutefois, l'article 35 §(10) du règlement général sur la protection des données prévoit que les États membres peuvent considérer qu'une analyse d'impact est nécessaire avant de commencer les activités de traitement. Les réglementations nationales devront donc le spécifier.

PÉRIMETRE DE L'ANALYSE D'IMPACT

CHAPITRE 2

Une particularité est admise par l'article 35 §(1) qui ajoute qu'« une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

Sur cette possibilité de procéder à une analyse d'impact unique, le considérant 92 du Règlement général sur la protection des données précise qu'il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou encore lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée.

Si les opérations de traitement sont similaires en termes de nature, de portée, de contexte, de finalités et de risques, une seule analyse d'impact suffit pour évaluer les risques. Devrait également être prises en compte la nature des données collectées et traitées.

En effet, une analyse d'impact vise à assurer l'étude systématique des nouvelles situations susceptibles d'entraîner des risques élevés pour les droits et libertés des personnes physiques. Il n'est donc pas nécessaire de procéder à une analyse d'impact dans les cas qui ont déjà fait l'objet d'une étude spécifique.

A titre d'illustration, tel peut être le cas lorsque des technologies similaires sont utilisées pour collecter le même type de données pour les mêmes finalités

Une analyse d'impact unique peut valoir pour des opérations de traitements similaires mises en œuvre par un seul responsable de traitement mais également par différents responsables du traitement.

Par exemple, un groupe d'autorités municipales mettant chacune en place un système similaire de vidéosurveillance pourrait se contenter d'une seule analyse d'impact unique couvrant le traitement envisagé par chacun de ces responsables distincts. Ou encore un opérateur ferroviaire (un seul responsable de traitement) pourrait couvrir la vidéosurveillance de l'ensemble de ses gares au moyen d'une seule et même analyse d'impact si les modalités sont identiques.

Dans ce cas, une analyse d'impact dite « de référence » devra être partagée ou être « publiquement » accessible selon le G29.

A cet égard, le groupe de travail suggère que l'analyse d'impact soit mise à disposition sur demande ou en fonction d'habilitations, afin de préserver la confidentialité et le secret des affaires.

Les mesures décrites dans l'analyse d'impact devront être mises en œuvre et une justification de la réalisation d'une analyse d'impact unique devra être fournie.

Enfin, lorsque l'opération de traitement implique des responsables conjoints du traitement, ils doivent définir précisément leurs obligations respectives. L'analyse d'impact devra déterminer la charge de la responsabilité des différentes mesures pour faire face aux risques et pour protéger les droits et libertés des personnes concernées. Chaque responsable du traitement devra exprimer ses besoins et partager les informations utiles en veillant à ne pas porter atteinte aux informations (secrets d'affaires, propriété intellectuelle, informations commerciales confidentielles etc.) et à ne pas divulguer de vulnérabilités.

2.4 La liste de la CNIL des traitements soumis obligatoirement à analyse d'impact

Conformément à ce que prévoit l'article 35.4 du RGPD, il faut faire une analyse d'impact si le traitement envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de réaliser une analyse d'impact relative à la protection des données.

La CNIL a soumis son projet de liste au Comité Européen de la Protection des données, qui a rendu son avis le 25 septembre 2018, à la suite duquel la CNIL a publié au Journal Officiel n°0256 le 6 novembre 2018[24] les quatorze types d'opérations de traitement soumis à analyse d'impact obligatoire :

- Traitements de données de santé mis en oeuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes ;
- Traitements portant sur des données génétiques de personnes dites « vulnérables » (patients, employés, enfants, etc.) ;
- Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines ;
- Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés ;
- Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire ;
- Traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle ;
- Traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre ;
- Traitements impliquant le profilage des personnes pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci ;
- Traitements mutualisés de manquements contractuels constatés, susceptibles d'aboutir à une décision d'exclusion ou de suspension du bénéfice d'un contrat ;
- Traitements de profilage faisant appel à des données provenant de sources externes ;

[24] Délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD)

- Traitement de données biométriques de reconnaissance des personnes dites « vulnérables » (élèves, personnes âgées, patients, demandeurs d'asile, etc.) ;
- Instruction des demandes et gestion des logements sociaux ;
- Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes ;
- Traitements de données de localisation à large échelle.

Cette liste n'est pas exhaustive et sera régulièrement revue par la commission selon son appréciation des « risques élevés » que peuvent présenter certains traitements.

La CNIL doit encore diffuser une liste des traitements pour lesquels aucune analyse d'impact n'est à effectuer conformément à ce que prévoit l'article 35.5 du RGPD.

2.5 Synthèse

En conclusion de ce premier chapitre, il apparaît que les traitements entrant dans le périmètre de l'analyse d'impact sont tous des traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques du fait de leur nature, de leur portée, de leur contexte, de leurs finalités ou encore en raison du recours à une nouvelle technologie.

Si la notion de risque élevé n'est pas définie, certains critères ont été énoncés dans les lignes directrices du G29 afin d'identifier un éventuel risque élevé, à savoir :

- le nombre de personnes concernées (en valeur absolue ou en proportion de la population considérée) ;
- le volume de données traitées ;
- l'éventail des différents éléments de données traitées ;
- la durée ou la permanence de l'activité de traitement de données ;
- l'étendue géographique de l'activité de traitement ;
- le risque présenté par la technologie utilisée.

Le périmètre de l'analyse d'impact pourra également être précisé par les autorités de contrôle, ce qui permettra d'augmenter la sécurité juridique des opérations.

Le schéma ci-dessous tente de représenter, sous la forme d'un algorithme juridique, les critères retenus à l'article 35 du Règlement général sur la protection des données ou proposés par le G29 pour déterminer si un traitement doit faire l'objet d'une analyse d'impact.

* Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a higt risk » for the purposes of Regulation 2016/679 du 4-4-2017 : WP248

Oui
Non

CONDUITE DE L'ANALYSE D'IMPACT

CHAPITRE 3

Après avoir étudié les aspects réglementaires relatifs à la conduite de l'analyse d'impact relative à la protection des données, décrite par l'article 35 du Règlement général sur la protection des données, les membres du groupe de travail se sont interrogés sur la méthode pouvant être suivie par les organismes afin de réaliser une analyse de l'impact des traitements qu'ils envisagent sur la protection des données à caractère personnel.

3.1 Le déclenchement de l'analyse d'impact

Les participants du groupe de travail se sont interrogés sur le moment auquel l'analyse d'impact relative à la protection des données devait être effectuée.

3.1.1 Cadre légal

L'article 35 §(1) du Règlement général sur la protection des données prévoit que le responsable du traitement « effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ».

L'analyse d'impact relative à la protection des données doit donc être conduite avant la mise en œuvre du traitement, voire dès sa phase de conception.

L'impératif de protection des données dès la conception implique au préalable une analyse des risques pour les droits et libertés des personnes physiques dès le moment de la détermination des moyens du traitement (soit dès la phase de conception du traitement). En effet, l'article 25 du Règlement général sur la protection des données impose aux responsables du traitement de mettre en œuvre, dès ce moment, des mesures techniques et organisationnelles appropriées pour mettre en œuvre les principes relatifs à la protection des données, cela en tenant compte notamment des risques du traitement sur les droits et libertés des personnes physiques.

Ainsi à tout le moins, l'identification d'un niveau élevé de risques et donc de la nécessité de réaliser une analyse d'impact relative à la protection des données doit avoir lieu dès la phase de conception d'un traitement.

3.1.2 La détermination du moment opportun

Il ressort de l'ensemble des dispositions précitées que l'analyse d'impact relative à la protection des données doit être menée préalablement au traitement ou plus précisément à sa mise en œuvre, afin de permettre aux organismes d'être conscients très tôt des conséquences du traitement qu'ils envisagent.

S'il est clair que l'analyse d'impact doit être menée avant la mise en œuvre du traitement, soit par exemple avant qu'un produit ou service soit mis sur le marché, la question se pose de savoir dans quel délai précédant la mise en œuvre du traitement le niveau de risque doit être évalué et le dossier d'analyse d'impact rédigé.

L'analyse d'impact relative à la protection des données et l'analyse de risques permettant d'identifier la nécessité de réaliser une analyse d'impact doivent être menées sur un traitement suffisamment abouti dans l'expression des besoins pour que ses caractéristiques principales et notamment les données collectées soient correctement définies.

En outre, il convient de ne pas négliger les ressources nécessaires en temps et en personnel pour rédiger un dossier d'analyse d'impact relative à la protection des données.

Une fois menée à bien, l'analyse d'impact permettra d'identifier les actions et mesures à mettre en œuvre pour que le traitement envisagé soit conforme au Règlement général sur la protection des données.

Pour que ces mesures puissent être effectivement mises en œuvre, il est cependant primordial qu'elles soient proposées à un moment où le traitement peut être facilement modifié, sans engendrer de coût financier et/ou de lourdeur administrative difficilement surmontables.

Ce moment pourra différer d'un projet à l'autre. Ainsi par exemple, lorsqu'une entreprise aura recours à un prestataire pour développer un nouveau produit, il conviendra de s'assurer, dès la réalisation du cahier des charges, que le prestataire répondra aux exigences du Règlement européen et prendra en compte toute modification rendue nécessaire suite à la réalisation de l'analyse d'impact relative à la protection des données.

Pour s'assurer de l'efficacité de la démarche, l'organisme responsable du traitement devra donc veiller à ce que l'analyse d'impact relative à la protection des données soit déclenchée à un moment où toute modification du traitement est encore envisageable. Cela est d'autant plus important que la réalisation tardive d'une analyse d'impact pourra engendrer des coûts financiers importants et des risques en terme de responsabilité pour l'organisme au regard du Règlement général sur la protection des données.

3.1.3 Les risques juridiques d'une analyse d'impact tardive

Il convient de s'interroger sur le risque juridique lié à la réalisation d'une analyse d'impact tardive.

Les sanctions administratives sont détaillées à l'article 83 §(4) du Règlement général sur la protection des données. Cet article prévoit des amendes pouvant s'élever jusqu'à 10 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu en cas de violation des dispositions prévues aux articles 35 et 36 du Règlement.

De nombreux éléments doivent être pris en compte dans la détermination du montant de l'amende administrative parmi lesquels notamment[25] :

- le fait que la violation a été commise délibérément ou par négligence ;
- les mesures techniques et organisationnelles mises en œuvre conformément à l'article 25 (Protection des données dès la conception et protection des données par défaut) et à l'article 32 (Sécurité du traitement) du Règlement général sur la protection des données.

Dès lors, deux situations peuvent être envisagées :

- l'organisme, intentionnellement ou par négligence, n'a pas réalisé d'analyse d'impact alors qu'il y était tenu au titre du Règlement européen, peu important que le traitement lui-même soit conforme : il risque alors une amende pouvant aller jusqu'à 10 000 000 euros ou 2% du chiffre d'affaire annuel mondial total de l'exercice précédent[26] ;
- l'organisme a réalisé une analyse d'impact mais les mesures mises en œuvre à la suite de l'opération n'ont pas permis à l'organisme de mettre en œuvre un traitement conforme au Règlement européen : il risque alors la peine prévue pour la violation constatée (par exemple : traitement de données sensibles en dehors des cas autorisés).

A côté des risques de sanction administrative et en fonction des règles définies au sein de chaque pays, l'organisme qui n'aurait pas rempli ses obligations au titre du Règlement général sur la protection des données s'exposerait également à des risques pénaux.

Par ailleurs, le Règlement général sur la protection des données organise au profit des personnes concernées :

- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- le droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant et un droit à réparation (article 79).

Enfin, il convient de garder à l'esprit que toute sanction publique pourrait entraîner des conséquences très néfastes pour l'organisme concerné, en terme d'image.

Dans ce contexte, il apparaît donc déterminant, afin de prévenir tout risque de sanction, d'effectuer l'analyse d'impact à un moment où toute modification du traitement est encore envisageable.

[25] Règl. 2016/679 du 27-4-2016, art. 83 § (2).

[26] La question de la nature de la responsabilité liée à l'identification d'un risque « élevé » conduisant à une analyse d'impact relative à la protection des données se pose. S'agit-il d'une simple obligation de moyen, d'une obligation de moyen renforcée (à l'image de l'obligation d'assurer la sécurité du traitement) ou d'une obligation de résultat (à l'image de l'obligation de respecter le principe d'accountability) ?

3.2 Une approche continue

La lecture de l'article 35 du Règlement général sur la protection des données semble suggérer une action en trois parties :

Analyse de risque : l'étude d'un traitement débutera par une analyse des risques présentés par ce traitement pour les droits et libertés des personnes physiques.

Cette analyse de risque permettra d'identifier l'existence éventuelle de « risques élevés » qui impliqueront la réalisation d'une analyse d'impact relative à la protection des données.

A l'issue de l'analyse de risque :

- s'il apparaît que le traitement ne nécessite pas une analyse d'impact, l'analyse des risques documentée, sera conservée comme trace de l'analyse réalisée, pour son éventuelle future mise à jour, d'une part, et pour se ménager une preuve des mesures d'accountability mises en œuvre par le responsable du traitement, d'autre part ;
- s'il apparaît que le traitement nécessite une analyse d'impact, celle-ci devra être menée comme indiqué ci-dessous.

Analyse d'impact : s'il apparaît que les risques présentés par le traitement justifient la conduite d'une analyse d'impact, une telle analyse devra être menée, en prenant en compte l'ensemble des opérations de traitement envisagées[27]. Cela peut s'entendre de la totalité du cycle de vie des données à caractère personnel tel qu'il est envisagé, de la collecte à la suppression, en passant par le traitement.

Il conviendra ici encore de documenter l'analyse d'impact.

Examen de conformité : l'article 35 §(11) du Règlement général sur la protection des données indique que si nécessaire, le responsable du traitement doit procéder à un examen destiné à évaluer si le traitement est effectué conformément à l'analyse d'impact.

Aucune durée précise n'est mentionnée dans le texte qui indique toutefois qu'un examen devra être effectué au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Pour le G29, une modification du risque pourrait intervenir suite à l'utilisation d'une nouvelle technologie ou à l'introduction d'une nouvelle finalité par exemple, mais également en cas d'évolution du contexte organisationnel ou sociétal du traitement conduisant à donner plus de poids à certaines décisions automatisées ou à considérer certaines catégories de personnes comme

[27] Règl. 2016/679 du 27-4-2016, art. 35 §(1).

plus vulnérables et exposées aux discriminations[28].

Le G29 évoque également le cas dans lequel le risque présenté par un traitement deviendrait moins important. Par exemple, des décisions ne seraient plus prises de manière automatisée ou des opérations de surveillance ne seraient plus réalisées de manière systématique. Dans ces cas, un examen serait également nécessaire. Celui-ci pourrait toutefois conduire à considérer qu'aucune analyse d'impact n'est plus nécessaire[29].

D'une manière générale, dans une démarche d'accountability, il convient de prévoir une revue régulière du traitement et de sa conformité à l'analyse d'impact.

A l'issue de l'examen, si des lacunes sont identifiées, il conviendra de :

- proposer des recommandations pour remédier aux lacunes ;
- mettre à jour l'analyse d'impact.

L'examen de conformité et ses recommandations devraient également être documentés.

Ces différentes étapes et l'adoption d'une approche continue de l'analyse d'impact permettront d'assurer que le traitement continuera à être conforme tout au long de son existence.

3.3 Le contenu de l'analyse d'impact

L'article 35 §(7) du Règlement général sur la protection des données précise quelles sont les informations qui doivent au minimum figurer dans une analyse d'impact. Ces informations comprennent :

- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent Règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

[28] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purposes of Regulation 2016/679 : Groupe « Article 29 » WP 248 rev.01 du 4-4-2017 et révisées le 4-10-2017, p. 13 et 14.
[29] Ibid., p. 14.

Il ressort de ces éléments que l'analyse d'impact vise à disposer d'une documentation complète sur un traitement donné et à évaluer sa conformité au Règlement général sur la protection des données, tant en terme de sécurité qu'en termes de nécessité et proportionnalité.

3.4 Les personnes impliquées dans l'analyse d'impact

3.4.1 Le débiteur de l'obligation

L'article 35 §(1) du Règlement général sur la protection des données fait peser l'obligation d'effectuer une analyse d'impact sur les seuls responsables du traitement.

Au titre du principe d'accountability, c'est en effet le responsable du traitement qui doit s'assurer et être en mesure de démontrer qu'un traitement est conforme aux exigences du Règlement.

Le responsable du traitement a la possibilité de sous-traiter la réalisation de tout ou partie de l'analyse d'impact. Toutefois, il demeure pleinement responsable de la conformité du traitement au Règlement général sur la protection des données et du respect de l'article 35 portant sur les analyses d'impact relatives à la protection des données.

Par ailleurs, aucune dérogation n'est prévue pour les micro, petites et moyennes entreprises[30].

3.4.2 Le sous-traitant

Si l'idée de soumettre également les sous-traitants à cette obligation a été envisagée dans le cadre de l'adoption du Règlement général sur la protection des données, dans la version finale du Règlement, le sous-traitant est uniquement tenu d'aider le responsable du traitement à respecter son obligation d'effectuer une analyse d'impact, compte tenu notamment des informations à sa disposition[31].

[30] L'idée de prévoir de telles dérogations a été un temps discutée dans le cadre de l'adoption du règlement. Le G29 s'était clairement opposé à cette proposition, considérant notamment que « tout en tenant compte de l'attention spéciale portée aux micro, petites et moyennes entreprises, il ne semble pas y avoir de raison impérieuse de créer des conditions spéciales pour elles. En particulier, puisque l'objectif de cet article est d'établir des garanties supplémentaires dans le cas où une opération de traitement présente (ou est susceptible de présenter) des risques particuliers au regard des droits et libertés des personnes concernées, il ne convient pas d'exempter de cette obligation les entités responsables du traitement pour des raisons de taille » (Avis 08/2012 apportant des contributions supplémentaires au débat sur la réforme de la protection des données : Groupe « Article 29 » WP199 du 5-10-2012, p. 39).
[31] Règl. 2016/679 du 27-4-2016, art. 28 §(3) f).

En revanche, l'obligation de garantir un niveau de sécurité adapté au risque pèse tout à la fois sur le responsable du traitement et sur le sous-traitant. Or, le respect de cette obligation s'accompagne nécessairement d'une analyse préalable des risques pour les droits et libertés des personnes physiques, et de leur évaluation en termes de probabilité et de gravité.

Cette analyse de risques sera particulièrement utile pour permettre au responsable du traitement de respecter l'article 35 du Règlement général sur la protection des données.

Dans tous les cas, la relation entre un responsable du traitement et un sous-traitant doit être encadrée par un contrat ou un autre acte juridique permettant de définir les rôles et responsabilités de chacun[32]. Dans la mesure où la réalisation d'une analyse d'impact peut représenter des coûts financiers ou des investissements en temps et en ressources humaines, il peut être utile de prévoir par contrat les conditions dans lesquelles les deux parties réaliseront l'analyse d'impact éventuellement requise et procèderont aux examens ultérieurs.

3.4.3 Le délégué à la protection des données

Le rôle précis du délégué à la protection des données dans l'analyse d'impact prête à discussion.

L'article 35 §(2) du Règlement général sur la protection des données prévoit que le responsable du traitement « demande conseil au délégué à la protection des données, si un tel délégué a été désigné ». Dans la version anglaise du texte, le mot « shall » est utilisé, ce qui semble suggérer une obligation pour le responsable du traitement de demander conseil au délégué à la protection des données qui aurait été désigné. Les guidelines publiées par le G29 vont également dans le sens de cette interprétation[33].

Il n'en demeure pas moins que théoriquement, c'est le responsable du traitement qui doit être à l'origine de la demande de conseil : les missions du délégué au titre de l'article 39 du Règlement général sur la protection des données incluent en effet la dispense de conseils sur l'analyse d'impact, mais uniquement « sur demande ».

Dans les faits, le délégué à la protection des données sera bien souvent impliqué très en amont dans le déclenchement de l'analyse de risque préalable à l'analyse d'impact.

Le thème et la nature des conseils pouvant être apportés par le délégué à la protection des données peuvent être variés et porter notamment sur :

- la nécessité ou non de conduire une analyse d'impact ;

[32] Règl. 2016/679 du 27-4-2016, art. 28 §(3).
[33] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purposes of Regulation 2016/679 : Groupe « Article 29 » WP 248 rev.01 du 4-4-2017 et révisées le 4-10-2017, p. 15.

- la détermination de la méthodologie à suivre ;
- le choix de réaliser l'analyse d'impact en interne ou en externe.

Les conseils donnés par le délégué à la protection des données et les décisions prises par le responsable du traitement au regard de ces conseils devraient être documentés.

Enfin, le délégué à la protection des données ne dispose pas que d'un rôle de conseil en matière d'analyse d'impact. Ce dernier est également tenu de vérifier l'exécution des analyses d'impact telles qu'exigées à l'article 35 du Règlement. A minima, le délégué à la protection des données devra donc être tenu informé de l'avancement de toute analyse d'impact effectuée par le responsable du traitement.

3.4.4 Les personnes concernées par le traitement

La question de l'implication des personnes concernées dans l'analyse d'impact est également stratégique pour les responsables d'un traitement.

Sur ce point, l'article 35 §(9) du Règlement général sur la protection des données prévoit que le responsable du traitement peut « le cas échéant » demander « l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu ».

Cette consultation des personnes concernées par le traitement envisagé est toutefois assortie de plusieurs réserves, en ce qu'elle ne doit pas porter préjudice à « la protection des intérêts généraux ou commerciaux » ni à « la sécurité des traitements ». Ces réserves permettraient ainsi aux organismes de limiter le périmètre d'une consultation du public, afin que ces derniers ne soient pas obligés de dévoiler des informations confidentielles sur leurs projets les plus innovants.

En fonction du contexte donc, l'avis des personnes concernées pourrait être recueilli. La forme à retenir est libre : il pourrait s'agir d'une consultation en ligne, de l'organisation d'enquêtes, de sondages ou de groupes de discussion, de l'organisation de réunions avec des associations ciblées ou de la consultation d'instances représentatives du personnel.

Ici encore, la décision de consulter ou non les personnes concernées ou leurs représentants et les décisions prises par le responsable du traitement au regard des résultats d'une éventuelle consultation devraient être documentés.

3.5 Le rôle du comité européen et des autorités de contrôle

3.5.1 Les autorités de contrôle

Au-delà de la préparation et publication de listes de traitements soumis ou non à analyse d'impact, les autorités de contrôle doivent être consultées pour certains traitements.

La consultation préalable de l'autorité de contrôle est exigée par le Règlement général sur la protection des données 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 »[34].

Cependant, c'est uniquement si le responsable du traitement n'est pas en mesure d'atténuer les risques élevés présentés par les opérations de traitement par des mesures appropriées et des moyens raisonnables compte tenu des techniques disponibles et des coûts de mise en œuvre, qu'il devra consulter l'autorité de contrôle[35].

Un risque résiduel peut être considéré comme élevé et inacceptable dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par ex. : un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) et/ou lorsqu'il semble évident que le risque se concrétisera (par ex. : impossibilité de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée)[36].

Lorsque le responsable du traitement ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable (à savoir que les risques résiduels demeurent élevés), la consultation de l'autorité de contrôle devient obligatoire[37].

L'autorité de contrôle devra être également consultée dans lors que le droit de l'État membre exige que les responsables du traitement consultent l'autorité de contrôle et/ou obtiennent son autorisation préalable en ce qui concerne un traitement que le responsable du traitement envisage dans le cadre d'une mission d'intérêt public dont il est investi, notamment pour les traitements en rapport avec la protection sociale et la santé publique (article 36§5 du Règlement général sur la protection des données)[38].

[34] Règl. 2016/679 du 27-4-2016, art. 36 §(1).
[35] Règl. 2016/679 du 27-4-2016, considérants 84 et 94.
[36] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purposes of Regulation 2016/679 : Groupe « Article 29 » WP 248 rev.01 du 4-4-2017 et révisées le 4-10-2017, p. 22.
[37] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purposes of Regulation 2016/679 : Groupe « Article 29 » WP 248 rev.01 du 4-4-2017 et révisées le 4-10-2017, p. 22.
[38] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purposes of Regulation 2016/679 : Groupe « Article 29 » WP 248 rev.01 du 4-4-2017 et révisées le 4-10-2017, p. 22.

3.5.2 Le Comité européen à la protection des données (CEPD)

Remplaçant le G29, le Comité européen à la protection des données est un organe de l'Union européenne composé du chef de l'autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données[39].

Le Comité européen de la protection des données devrait contribuer à l'application cohérente du Règlement européen sur la protection des données dans l'ensemble de l'Union européenne[40]. Il pourra également publier des lignes directrices, recommandations et bonnes pratiques afin d'encourager une application cohérente du Règlement européen[41].

S'agissant plus particulièrement de l'analyse d'impact, les autorités de contrôle seront tenues d'établir, de publier et de communiquer au Comité européen de la protection des données une liste des opérations de traitement nécessitant une analyse d'impact[42] (article 35, paragraphe 4). Le Comité européen de la protection des données devra alors émettre un avis sur cette liste d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données doit être effectuée[43].

Les aspects réglementaires de l'analyse d'impact issus du Règlement général sur la protection des données étant posés, il convient désormais d'en étudier les aspects méthodologiques.

[39] Règl. 2016/679 du 27-4-2016, article 68.
[40] Règl. 2016/679 du 27-4-2016, considérant 139.
[41] Règl. 2016/679 du 27-4-2016, article 70.
[42] Règl. 2016/679 du 27-4-2016, article 35§4.
[43] Règl. 2016/679 du 27-4-2016, article 64§1.a.

CADRE MÉTHODOLOGIQUE

CHAPITRE 4

4.1 Les aspects méthodologiques

4.1.1 Panorama rapide des référentiels ou bonnes pratiques

La démarche d'analyse d'impact est basée sur une approche de gestion des risques en matière de respect de la vie privée et de la protection des données à caractère personnel.

S'agissant d'une approche de gestion de risques, de nombreux référentiels existent aujourd'hui. Il s'agit de référentiels génériques applicables à tous types de risques, de référentiels plus sectoriels, mais aussi de référentiels développés en interne par les organismes. A titre d'exemples, nous pouvons citer ISO 31000, Ebios, Mehari, Amrae.

En matière de gestion de risques relatifs à des données à caractère personnel et des risques relatifs à la vie privée, la méthodologie doit porter sur des scenarii susceptibles d'engendrer des impacts pour les personnes concernées indépendamment de la préservation des intérêts de l'organisation.

A ce titre, la Commission européenne a proposé une approche d'évaluation de l'impact des dispositifs RFID[44]. Ce cadre, qui a été approuvé par le G29[45], est aussi conforme aux attentes de la Cnil qui en a récemment précisé la méthodologie[46].

L'approche Cnil est basée sur la méthode Ebios qu'elle a d'ailleurs spécifiquement adaptée au cas particulier de la protection des données personnelles. Ce qui a donné lieu à la publication de cinq guides méthodologiques susceptibles d'être révisés :

- PIA 1 « La méthode », qui présente la méthode pour réaliser les PIA - février 2018 ;
- PIA 2 « Les modèles », qui inclut des modèles et bases de connaissance pour mettre en œuvre la méthode – février 2018 ;
- PIA 3 « Les bonnes pratiques », qui constitue un catalogue de mesures, destinées à respecter les exigences réglementaires et à traiter les risques appréciés avec cette méthode – février 2018.

[44] Cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données du 11-2-2011, mis à jour le 28-10-2015. Cette proposition faisait suite à la recommandation de la Commission européenne sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, en date du 12-5-2009, dans laquelle la Commission invitait les États membres à « veiller à ce que les entreprises, en collaboration avec les parties intéressées de la société civile, élaborent un cadre d'évaluation de l'impact sur la protection des données et de la vie privée ». Ce cadre devait ensuite être soumis pour approbation au G29.

[45] Avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) : Groupe « Article 29 » WP180 du 11-2-2011.

[46] L'évaluation d'impact sur la vie privée pour les dispositifs RFID : Questions/réponses Cnil 26-9-2013. Comment réaliser une évaluation d'impact sur la vie privée (EIVP) pour les dispositifs RFID ? Cnil 9-2013.

- PIA : Etude de cas Captoo - février 2018-, qui propose un exemple d'approche et de documentation d'un cas basé sur l'approche PIA de la Cnil ;
- PIA : Application aux objets connectés - février 2018-, qui décline le guide PIA de la Cnil au domaine des objets connectés.

Ainsi qu'à la mise en œuvre d'un outil aidant à la conduite et la formalisation des analyses d'impacts basé sur l'approche PIA de la Cnil, l'outil « PIA » (logiciel open source).

Et à la publication d'un guide « La sécurité des données personnelles » Edition 2018, susceptible d'être utilisé dans le cadre d'une gestion des risques qui rappelle les mesures de sécurité et précautions qui devraient être mises en œuvre pour des traitements de données à caractère personnel.

De son côté, le G29[47] a publié en avril 2017 un guide méthodologique sur l'analyse d'impact et l'évaluation du risque élevé au sens du Règlement européen « Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP28) »[48]. Ce guide a été amendé et ré-adopté le 4 octobre 2017.

Le G29 fait référence aux normes ISO 31000 (gestion des risques) et ISO 29134 (analyse d'impact sur la vie privée[49]). La méthode doit être adaptée au besoin et au contexte, et doit être intégrée aux processus de revue opérationnelle et de gestion des risques, de développement et de conception, en tenant compte du contexte et de la culture de l'entreprise. Le G29 propose une liste de critères que doit respecter la méthode d'analyse (annexe 2 de l'avis du G29) et laisse de la flexibilité dans le choix de la structure et de la forme du rapport d'analyse.

Il donne aussi des exemples

- de supports génériques
  - DE : Standard data Protection Model V1.0, 2016
  - ES : Guia para una Evaluacion de Impacto en la Proteccion de datos personales, AGPD- 2014
  - FR : PIA, CNIL-2015
  - UK : Conducting privacy impact assessment – code of practice, ICO 2014 (qui remplace son « Handbook » sur l'analyse d'impact relative à la protection des données publié en 2009)

[47] Le G29 ou Groupe de travail Article 29 sur la protection des données (en anglais Article 29 Data Protection Working Party) est un organe consultatif européen indépendant sur la protection des données et de la vie privée. Son organisation et ses missions sont définies par les articles 29 et 30 de la directive 95/46/CE

[48] Adopted on 4 April 2017 by the Data Protection Working Party which was set up under Article 29 of Directive 95/46/EC

[49] ISO/IEC 29134:2017 - Guidelines for privacy impact assessment – June 2017

- De supports sectoriels
  - Privacy and DPIA Framework for RFID Applications - 2011 ;
  - DPIA Template for Smart Grid and Smart Metering systems,- 2014.

Plus récemment, l'organisation internationale ISO a publié en juin 2017 la Norme ISO/IEC 29134 « Guidelines for privacy impact assessment » ou « lignes directrices pour mener des études d'impact sur la vie privée » qui fournit le cadre pour mener des analyses d'impact tel que définies dans le Règlement européen. Elle est proche des guides produits par la Cnil auxquels elle peut faire référence. Elle s'appuie sur la norme ISO/IEC 29100 (Privacy Framework) qui définit les principes et la terminologie relatifs à la protection de la vie privée et notamment le principe d'« accountability »

S'agissant d'apporter une réponse pragmatique à l'obligation liée à l'article 35 du Règlement européen, la démarche développée ci-après est fondée sur les approches ou bonnes pratiques préconisées par la Commission européenne et le G29, et les recommandations Cnil.

4.1.2 Objectifs et principes clés de l'analyse d'impact relative à la protection des données

Le Règlement européen ne rend pas obligatoire l'analyse d'impact relative aux données à caractère personnel pour tous les traitements. Celle-ci est requise si le risque est élevé (article 35-1), ce qui suppose de mener une analyse de risque préalablement à l'analyse d'impact.

L'objectif de l'analyse d'impact relative à la protection des données à caractère personnel est de s'assurer que les risques liés à la vie privée sont minimisés tout au long du traitement des données et que les principes fondamentaux du Règlement sont respectés. Il s'agit dans ce cadre de permettre une identification et une appréciation des risques le plus tôt possible en analysant, dès la phase de conception d'un projet informatique, d'une application ou d'un traitement de données (« privacy by design » en anglais), les modalités d'utilisation des données à caractère personnel et les finalités des traitements et en identifiant quelles mesures sont prises pour prévenir et pour limiter de manière proportionnée les impacts sur la vie privée.

Dans ce cadre, l'analyse d'impact permet :

- de mettre en évidence les risques liés aux traitements de données à caractère personnel ;
- d'apprécier leurs impacts potentiels ;
- de documenter les modalités et démarches de réduction de ces risques ;
- in fine, de décider d'accepter les risques résiduels.

Quels avantages et bénéfices pour les organisations ?

- une visibilité sur la conformité réglementaire de l'organisation ;
- une meilleure transparence à l'égard des personnes dont les données sont traitées et une confiance accrue ;
- une plus grande sensibilisation des intervenants internes et externes ;
- des gains financiers liés à la mise en œuvre d'une démarche d'analyse d'impact très tôt dès la conception des traitements ;
- une maturité plus forte dans la gouvernance des risques.

4.2 Description d'une méthodologie d'analyse d'impact relative à la protection des données à caractère personnel

4.2.1 Présentation d'ensemble

A titre liminaire, le G29 précise notamment que l'analyse d'impact[50]:

- doit au minimum adresser le contenu précisé dans le Règlement à l'article 35-7 et les considérants 84 et 90,
- doit être conforme au code de conduite (article 40 du Règlement) adopté si ce dernier est applicable au traitement sous revue,
- a pour but de gérer les risques sur les droits et liberté des personnes par :
  - la définition du contexte (nature, périmètre, contexte et finalité du traitement, et sources de risques)
  - l'évaluation des risques élevés basée sur leur probabilité d'occurrence et leur gravité
  - le traitement des risques (réduire les risques et assurer la protection des données à caractère personnel, et prouver la conformité avec le Règlement)
- a pour but d'évaluer les risques pour les droits des personnes et non les risques pour les entreprises ou autres organisations,
- donne toute flexibilité dans le choix de la structure et la forme de l'analyse d'impact,
- rappelle que la méthodologie doit s'intégrer dans les processus existants dans les organisations, prenant ainsi en compte les processus internes, le contexte et la culture de l'organisation, mais précise que la méthodologie retenue devra au minimum prendre en compte les critères (listés en annexe 2) pour être conforme au Règlement,
- encourage la création de cadres méthodologiques sectoriels,
- rappelle la nécessité de mettre à jour cette analyse dès lors que les risques évoluent,

[50] Guidelines on Data Protection Impact Assessment and determining whether processing is « likely to result in a high risk »for the purposes of Regulation 2016/679 – Revised and adopted on 4 October 2017

- et illustre la méthodologie d'analyse d'impact au travers du processus itératif ci-après.

Le schéma qui suit décrit les étapes « idéales » d'une analyse d'impact relative à la protection des données à caractère personnel, telles qu'elles ont pu être discutées dans le cadre du groupe de travail.

La description de chacune des étapes est présentée ci-après, et des exemples de formats de présentation sont illustrés dans les cas.

CHAPITRE 4

Phase 1 : Analyse de risque initiale
Phase 2 : Evaluation et limitation des risques
Phase 3 : Amélioration continue
Impliquer les acteurs internes et externes pertinents de manière continue
Etape 1 – Identifier le périmètre, documenter le contexte, cartographier les données et flux de données de façon globale
Etape 2 – Analyser les traitements et données au regard des critères susceptibles d'engendrer un risque élevé
La réalisation d'une analyse d'impact est-elle requise ?
Non
Oui
Rapport Initial
Etape 3 – Détailler le contexte et cartographier précisément les données et les flux de données
Etape 4 – Identifier les mesures de conformité et de suppression ou de réduction des risques
Etape 5 – Cartographier et décrire les risques résiduels et leurs impacts potentiels
Etape 6 – Décrire la mise en œuvre des actions correctives et les risques résiduels acceptés
Etape 7 – Réaliser une revue générale, Constater les risques résiduels, définir les modalités de la revue périodique ou sur évènements déclencheurs et rédiger le rapport d'analyse d'impact - Valider
Rapport principal
Etape 8 – Effectuer la revue périodique ou sur évènements déclencheurs, mises à jour, et le cas échéant, correction(s)
Rapport périodique

CADRE MÉTHODOLOGIQUE

CHAPITRE 4

Dans sa version complète, la démarche proposée est itérative. Elle s'articule autour de trois grandes phases qui regroupent huit étapes.

(1) Phase d'analyse de risque initiale :

- elle décrit « à grands traits » le contexte et le périmètre de l'application et propose une première cartographie des données et des flux de données ;
- elle documente les traitements et données au regard des critères susceptibles d'engendrer un risque élevé ;
- sur la base de ces informations, elle détermine le besoin de réaliser ou non une analyse d'impact sur la protection des données à caractère personnel et se conclut par la rédaction d'un rapport d'analyse de risque initial qui fait partie de la documentation du DPO.

(2) Phase d'évaluation et de limitation des risques :

- elle décrit de façon détaillée l'application, son contexte, son environnement et son fonctionnement, ainsi que les données et flux de données ;
- elle documente les mesures de conformité et les mesures de réduction ou suppression des risques mises en place ;
- elle identifie les menaces sur la vie privée, évalue leur probabilité d'occurrence et la gravité des événements redoutés avec mesure de l'impact sur la vie privée et elle décrit les risques résiduels, avec l'acceptation ou le refus de ces derniers ;
- elle prévoit la mise œuvre des actions correctives, définit les modalités de la revue périodique ou à la suite de l'apparition d'événements déclencheurs et se conclut par la rédaction du rapport principal.

(3) Phase d'amélioration continue :

- elle réalise la revue de l'application à intervalles réguliers ou à la suite de l'apparition d'événements déclencheurs ;
- elle met à jour les différentes analyses ;
- elle met en œuvre les corrections nécessaires ;
- et elle se conclut par la mise à jour du rapport initial d'analyse des risques ou de l'analyse d'impact pour la protection des données à caractère personnel.

La méthodologie proposée se veut suffisamment flexible pour s'insérer dans le cadre de processus de gestion des risques déjà opérationnels au sein des organisations (par exemples : Sox, LSF, 89-02...), mais aussi afin que son développement puisse être adapté aux risques potentiels sur la vie privée et la protection des données à caractère personnel.

Dans tous les cas, une attention particulière doit être portée :

- à la participation et à la consultation des acteurs pertinents tout au long du processus ;
- à la formalisation de la démarche ;
- à la mise à niveau périodique de l'analyse d'impact et de sa documentation.

4.2.2 Description détaillée

La suite de ce chapitre détaille les différentes étapes.

4.2.2.1 *Impliquer et consulter les acteurs internes et externes pertinents de manière continue*

Le responsable du traitement est responsable de la mise en œuvre de l'analyse d'impact même s'il délègue cette tâche. Il peut être assisté par le sous-traitant qui lui fournit les informations nécessaires. Leurs rôles et responsabilités sont définis contractuellement.

Il doit demander conseil au Délégué à la Protection des Données (DPO) (art. 35-2) et documenter les conseils émis par le DPO et les décisions prises in fine.

L'analyse d'impact ne doit pas être un exercice solitaire. Elle devrait être un exercice collectif qui implique toutes les parties concernées par un traitement, qu'elles soient internes ou externes à l'organisme. Dans cet exercice, la phase de consultation vise à faire émerger des points de vue suffisamment différents pour éclairer tous les contextes possibles du traitement. Ainsi, toutes les parties concernées devraient pouvoir, d'une part, exprimer leurs propres préoccupations en s'appuyant sur leur expérience, leur expertise, leurs besoins, etc. et, d'autre part, contribuer à l'identification de solutions visant à supprimer ou, sinon, à réduire les risques identifiés.

Sur ce point, le Règlement européen prévoit que le responsable de traitement demande, le cas échéant, l'avis des personnes concernées, et le G29 précise que cette consultation doit être réalisée, et que les avis des personnes concernées doivent être documentés, tout comme la décision de ne pas suivre les avis recueillis. Il convient ainsi de documenter la décision de ne pas consulter les personnes concernées.

D'une manière générale, il est recommandé d'impliquer les « sachants » internes comme externes, et de faire intervenir des experts comme nécessaire.

En interne, la consultation a aussi une fonction complémentaire de « sensibilisation » et de « formation » des acteurs à la prise en compte de la protection des données à caractère personnel et, plus généralement, des droits et libertés fondamentaux des

personnes concernées. Tous les métiers de l'organisme sont ainsi potentiellement concernés :

- l'équipe projet qui propose le nouveau traitement, ou des modifications significatives d'un traitement existant ;
- les ingénieurs, développeurs, designers qui vont participer à la conception du traitement, de l'outil, etc ;
- le service juridique ;
- les services en charge de la sécurité informatique et de la protection de l'information ;
- le service informatique qui sera en charge d'héberger le traitement, de le maintenir ;
- le service éthique et conformité ;
- le service des achats ;
- les « fournisseurs internes » ;
- le service communication qui sera impliqué dans la promotion du projet ;
- le service clients qui sera confronté aux personnes concernées lorsque le projet sera en phase d'exploitation ;
- les services en charge de la gestion des risques en général et informatiques en particulier ;
- la direction qui devra faire les nécessaires arbitrages ;
- le contrôle interne ;
- etc.

Le rôle du délégué à la protection des données est défini à l'article 39 du Règlement. Dans le cadre de la conduite de l'analyse d'impact, le G29 précise que ce dernier :

- peut suggérer la conduite d'une analyse d'impact ;
- devrait assister les participants sur la méthodologie ;
- devrait aider à évaluer la qualité de l'analyse de risque ;
- devrait aider à évaluer si le risque résiduel est acceptable ;
- devrait contribuer au développement des connaissances spécifiques au contexte du responsable de traitement.

En externe, la consultation doit permettre de faire émerger les points de vue des personnes susceptibles d'être « touchées » directement ou indirectement par le traitement. Il s'agit, d'une part, d'identifier leurs éventuelles préoccupations et, d'autre part, de montrer une forme de transparence indispensable pour l'établissement d'une relation de confiance. La consultation peut concerner directement des personnes individuelles ou des représentants de groupements. Elle peut utiliser les outils habituels de l'organisme pour ce type d'opération lorsqu'il en a déjà en place, comme des panels, des groupes de travail, des questionnaires en ligne, etc. L'organisme peut aussi consulter des « experts » externes dans les cas où il ne disposerait pas, en propre, des compétences

nécessaires.

Qu'elle soit interne ou externe l'étape de consultation doit bien sûr être adaptée, dimensionnée, à la nature du projet, au type et au nombre de personnes concernées, etc. sans oublier de prendre en considération les nécessités et impératifs liés à l'innovation et à sa protection dans un contexte concurrentiel.

4.2.2.2 *Identifier le périmètre, documenter le contexte et cartographier les données et les flux de données de façon globale*

Cette étape est la première de la « phase d'analyse des risques initiale ». Elle a pour principal objectif de recueillir un minimum d'informations sur le traitement étudié de façon à pouvoir être à même de décider, à « l'étape 2 » qui suit, si ce traitement doit ou non faire l'objet d'une analyse d'impact relative à la protection des données. Dans cette perspective, il s'agit de documenter - même de façon imprécise pour commencer- les éléments qui sont regroupés dans le tableau qui suit et dont les études de cas en annexe proposent des illustrations :

Nom du traitement	
Entité juridique (Organisme)	
Responsable du traitement (coordonnées)	
Responsables du traitement conjoints	
Direction ou service en charge de la mise en œuvre du traitement	Responsable, service ou prestataire extérieur manipulant les données
Sous-traitants (liste des sous-traitants)	
DPO	
Entités concernées	
Finalités du traitement	Objectifs et finalités : ▪ principales ▪ détaillées
Formalités (à accomplir ou accomplies) et référentiels applicables	Par exemple normes simplifiées, etc.

Catégories de personnes concernées	Toutes les catégories de personnes dont les données sont traitées : salariés, clients, utilisateurs, etc.
Présence de données relatives à des enfants	
Catégories de données traitées à caractère personnel	Liste des données à caractère personnel traitées (par ex, identification, vie professionnelle, connexion, localisation)
Présence de données sensibles	Origines raciales ou ethniques, opinions politiques, convictions philosophiques ou religieuses, appartenance syndicale, santé, vie sexuelle, NIR, données génétiques, données biométriques aux fins d'identifier une personne physique de manière unique, infractions-condamnations-mesures de sureté, difficultés sociales
Catégories de destinataires et données concernées	Internes et/ou externes
Zone de libre commentaire (ZLC)	Oui/Non
Encadrement des ZLC	Audit de l'application, charte, sensibilisation des utilisateurs
Collecte directe des informations	
Collecte indirecte des informations	
Information des personnes concernées	Modalités prévues ou existantes
Consentement des personnes concernées	Modalités prévues ou existantes
Durées de conservation	Politique pour les durées de conservation Modalités de suppression des données
Interconnexion	Lien avec d'autres fichiers de données à caractère personnel dont les finalités sont différentes
Flux transfrontières (FT) hors UE	Oui/Non, pays/entités/finalités concernées
Encadrement des FT	Modalités
Sécurité	Mesures techniques ou organisationnelles en place ou à prévoir

Le travail ainsi réalisé sera directement utile au Data Protection Officer (DPO) pour la constitution ou la mise à jour de l'inventaire des traitements mis en œuvre par son organisation. Il servira aussi à répondre aux éventuelles demandes des autorités de contrôle et contribuera à l'obligation d'accountability.

La CNIL dans son guide « PIA 3 : les bases de connaissances » fournit un exemple de catégorisation des données à caractère personnel, ainsi qu'un exemple de formalisation d'une description détaillée des données à caractère personnel.

Exemple catégorisation des données à caractère personnel[51]

Types de DCP	Catégories de DCP
DCP courantes	État-civil, identité, données d'identification
	Vie personnelle (habitudes de vie, situation familiale, hors données ou dangereuses...)
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale...)
	Données de connexion (adresse IP, journaux d'évènements...)
	Données de localisation (déplacements, données GPS, GSM...)
DCP perçues comme sensibles	Numéro de sécurité sociale (NIR)
	Données biométriques
	Données bancaires
DCP sensibles au sens de la Loi I&L 1	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle
	Infractions, condamnations, mesures de sécurité

Enfin, pour compléter et synthétiser les informations obtenues, il est essentiel de « brosser » une première cartographie des flux de données entre les acteurs concernés par le traitement.

4.2.2.3 *Analyser les traitements et données au regard des critères susceptibles d'engendrer un risque élevé*

Rappel G29

- Une analyse d'impact n'est pas obligatoire pour tous les traitements

[51] Source « Analyse d'impact relative à la protection des données (PIA) 3 : les bases de connaissances », février 2018

Source : "Guidelines on Data Protection Impact Assessment and determining whether processing is « likely to result in a high risk »for the purposes of Regulation 2016/679 – Revised and adopted on 4 October 2017"

- Une seule analyse d'impact pour plusieurs traitements
  - Article 35-1 et considérant 92 :
    - Un même DPIA peut servir à évaluer différents traitements qui présentent les mêmes risques. Par exemple, lorsqu'une technologie équivalente est utilisée pour collecter les mêmes données pour une finalité identique
    - Pour le G29, doivent être pris en compte la nature, le champ, le contexte et la finalité de chaque traitement
  - Cas particuliers :
    - Dans le cas de co-responsables de traitement, L'analyse d'impact relative à la protection des données devra expliquer quelle partie est responsable des mesures prises pour limiter les risques et protéger les droits des personnes concernées
    - Un DPIA peut permettre d'évaluer l'impact d'une technologie, software ou hardware, qui sera utilisée par différents responsables pour divers traitements. Chaque responsable devra mener L'analyse d'impact relative à la protection des données correspondant à son traitement, cependant elle pourra être renseignée par celle menée par le fournisseur de produit

- Le périmètre des critères d'évaluation
  - DPIA obligatoire lorsque le traitement « est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes »
  - Eléments à prendre en compte :
    - l'évaluation ou la notation de personnes, notamment les opérations de profilage et d'analyse des comportements ;
    - la prise de décisions produisant des effets juridiques ou l'affectant de manière significative, fondées sur un traitement automatisé ;
    - la surveillance systématique (traitement utilisé pour observer, surveiller et contrôler les sujets concernés) ;
    - la collecte de données sensibles (au sens large) ;
    - la collecte de données à grande échelle ;
    - les traitements qui ont été rapprochés ou interconnectés ;
    - les données concernant des personnes vulnérables ;
    - l'utilisation ou l'application de moyens technologiques ou organisationnels innovants;
    - les transferts de données hors du territoire de l'Union européenne ;
    - si le traitement empêche les personnes concernées d'exercer un droit ou d'utiliser un service ou un contrat.
  - Notion de donnée sensible qui inclut :
    - données de l'article 9 ;
    - données relatives aux condamnations et infractions pénales ;
    - données qui augmentent les risques possibles pour les droits et libertés des personnes: communications électroniques, données de localisation, données financières (paiement) ;
    - données traitées dans le cadre strictement privé et domestique (email, journaux intimes, notes etc...) ;
    - question de la publication des données ou non.
  - Notion de traitement à grande échelle fonction de :
    - nombre de personnes concernées : nombre élevé en lui-même ou proportionnellement à une population donnée ;
    - volume de données et/ou palette de différentes données traitées ;
    - durée ou permanence des opérations de traitement ;
    - périmètre géographique des opérations de traitement.
- La prise de décision
  - Principe: un traitement qui remplit moins de deux critères n'est pas soumis à analyse d'impact
  - Exceptions possibles :

  - Un traitement ne remplissant qu'un critère peut présenter des risques élevés
  - Un traitement remplissant au moins deux critères peut ne pas présenter de risque élevé
- En cas de doute, il est recommandé de faire un DPIA

Cette étape « 2 » clôt la « phase d'analyse de risque initiale ». Pour faciliter la prise de décision, le groupe de travail a élaboré un « arbre de décision » sur la base de l'article 35 du Règlement et des recommandations du G29 dans son « Guidelines on Data Impact assessment and determining whether processing is « likely to result in a high risk » for the purposes of regulation 2016/679 ».

Cet arbre de décision a été présenté au Chapitre 2.4 du présent Cahier. L'étude de cas du Chapitre 5 en fournit un exemple d'utilisation.

Dans une perspective de traçabilité et « d'accountability », l'ensemble de cette première phase pourra être formalisée dans un rapport d'analyse de risque initiale regroupant les informations du tableau proposé au Chapitre 4.2.2, la cartographie des flux et les résultats significatifs obtenus en parcourant l'arbre de décision. Si la réalisation d'une analyse d'impact sur la protection des données à caractère personnel est requise, alors ce rapport d'analyse de risque initiale pourra constituer la première partie du rapport principal attendu dans le cadre de l'analyse d'impact. Dans le cas contraire, il servira à documenter le traitement et pourra être mis à jour en cas de modifications significatives du traitement.

4.2.2.4 *Détailler le contexte et cartographier précisément les données et les flux de données*

Si une analyse d'impact est requise, il convient dans cette nouvelle étape, qui marque le début de la deuxième phase, de préciser l'ensemble des informations obtenues lors des étapes précédentes afin d'avoir une représentation la plus précise possible du traitement étudié. Il sera par exemple utile de préciser les éléments qui suivent :

- mode de développement du logiciel utilisé, environnement technique ;
- date de mise en service, évolutions récentes et prévues ;
- enjeux et finalités du traitement actuels et prévus ;
- périmètre du traitement ;
- utilisateurs concernés ;
- données entrantes et sources ;
- types d'opérations effectuées ;
- données sortantes et destinataires ;
- interfaces avec d'autres systèmes internes ou externes ;

- liens entre données à caractère personnel directes et déduites ;
- personnes ayant accès aux données ;
- cycle de vie de la donnée ;
- etc.

Il convient en particulier de documenter et justifier le « pourquoi », par exemple, telle personne à accès aux données ou « pourquoi » telle personne est destinataire de la donnée.

La cartographie des flux de données sera elle aussi affinée en utilisant les informations nouvellement obtenues ou actualisées. Et il pourra s'avérer très utile d'en faire une représentation graphique, par exemple en utilisant la norme BPMN (Business Process Model and Notation), en incluant toutes les informations utiles, comme les types de données concernées, leur sensibilité, les types d'acteurs, le sens des échanges, la localisation géographique, les équipements utilisés, etc.

Une bonne compréhension de l'application facilite la détermination des risques et permet de focaliser plus directement sur les seuls processus concernés.

À ce stade, il est utile de remarquer que dans le cas de systèmes existants, ces informations sont la plupart du temps disponibles dans les organisations sous forme, par exemple, de rapport d'audit ou de documentation fonctionnelle et de dossiers d'architecture.

De même, afin de faciliter le déroulement du processus d'une analyse d'impact, un volet complémentaire, propre aux problématiques liées au respect de la vie privée, pourra judicieusement être ajouté aux processus de documentation déjà opérationnels dans l'organisation.

Le cas de l'archivage

Par ailleurs, la démarche de l'analyse d'impact intègre aussi l'évaluation du dispositif de gestion des documents d'activité et d'archivage électronique.

La série des normes de management et techniques consacrée à la gestion des documents d'activité ou records management[52]

[52] La maîtrise du cycle de vie des données à caractère personnel et le records management : Dans le cadre de la mise en place du système de records management, les acteurs doivent définir techniquement des tableaux de gestion des données et documents qui incluent la durée de conservation de chaque donnée et document. Une procédure doit être établie pour déterminer les périodes de conservation conformément aux exigences de chaque processus. Les conditions d'accès, de purge ou d'anonymisation y sont précisées. Chaque donnée est aussi associée à un plan de classement qui correspond au processus dans le cadre duquel la donnée a été produite. Durées de conservation, règle de purge, gestion des accès et droits, lien avec le classement et l'archivage complètent les critères de gestion d'une donnée.

(série des ISO 3030X et notamment ISO 15489) ainsi que les normes consacrées à l'archivage électronique des données (norme NF Z 42-013 et son pendant ISO 14641) font partie intégrante de l'évaluation du risque.

Ces deux séries de normes ont pour objectif de maîtriser la totalité des traitements opérés sur le cycle de vie des données. Leur mise en place ainsi que la certification des systèmes mis en place à cette occasion démontrent que les données à caractère personnel sont identifiées, tracées, purgées au terme de la période réglementaire et protégées contre toute consultation abusive. La maîtrise de ces données est désormais une obligation légale et une exigence normative pour tout organisme. Elle vise à assurer davantage de transparence et de gouvernance.

Ces normes énoncent les exigences qui président à la création et à la gestion des données produites et reçues par chaque activité, tout support et tout format. La création (y compris les données bureautiques et celles issues d'applications métiers) et la réception de documents font partie intégrante des activités, processus et systèmes des organismes.

Ces normes permettent de garantir une définition plus précise des rôles et responsabilités des acteurs, en ce qui concerne l'identification des documents et données obligatoires à prendre en compte dans le processus de gestion des documents d'activité, et de préciser les fonctions à mettre en œuvre (capture, classement, traitement, archivage, purge, accès, suppression, versement), telles que décrites dans la norme ISO 15489-1 et 2.

Le système d'archivage électronique gouverné par la norme ISO 14641 concerne les données qui doivent être archivées et qui ont vocation probatoire. Notons que ce composant d'archivage peut être interne ou externalisé (tiers archiveurs).

Lors de l'analyse d'impact, les questions suivantes sont posées :

- un système de records management selon les normes ISO 3030X[53] et ISO 15489 est-il appliqué ? si oui, est-il certifié ?
- un système d'archivage électronique selon les normes NF Z 42-013 ou ISO 14641 est-il appliqué ? si oui, est-il certifié ?

[53] La démarche du PIA contribue à la maintenance d'un système de records management (gestion des documents d'activités dans les organisations privées comme publiques). Le chapitre 2.5, de la norme ISO 30300 qui définit les principes essentiels et le vocabulaire du records management, présente l'approche par processus d'un système de gestion des documents d'activité (SGDA) et met l'accent sur l'importance de définir une politique et des objectifs relatifs aux données et documents produits et reçus par un organisme et par conséquence les données pour partie à caractère personnel qui y sont associées. La norme insiste sur la gestion des risques associés à ses données d'activité et dans le cadre d'une gestion globale de ses risques. Les critères de risques sont cités comme opérationnels, réglementaires et légaux. Dans le chapitre 4.2 de l'ISO 30301, l'organisme doit évaluer et documenter les exigences opérationnelles, légales, règlementaires et les autres exigences affectant ses activités auxquelles il doit se conformer et pour lesquelles des preuves de conformité sont exigées. Les conclusions du PIA sont prises en compte par le record manager qui met à jour la documentation décrite par le rapport technique (TR) ISO 26122 intitulé « analyse des processus pour la gestion des documents d'activité) qui précise que la mise en œuvre d'un système de records management passe d'abord par l'analyse des risques et liste des séries complètes de question pour l'évaluation : quelles données, quels traitements, quelles responsabilités, quel impact, quelles contraintes réglementaires, etc.

Si les réponses sont affirmatives, un cadre de confiance s'applique naturellement à la maîtrise des données à caractère personnel. Dans le cas contraire, une démarche de mise en place de ces processus de gestion documentaire et d'archivage aurait dû être initialisée ou mise à jour en parallèle ou à la suite de l'analyse d'impact.

4.2.2.5 *Identifier les mesures de conformité et de suppression ou de réduction des risques*

Cette deuxième étape de la phase 2 doit permettre d'identifier les mesures (éventuellement existantes, dans le cas d'un traitement déjà opérationnel) de réduction ou de suppression des risques, les options et les alternatives possibles en vue de minimiser le niveau de risque.

Ces mesures peuvent être techniques, liées à l'application informatique (par exemple, chiffrement des données, authentification, contrôle d'accès, sauvegardes redondantes, etc.) ou organisationnelles, avec des mesures liées aux processus et au fonctionnement de l'organisation (par exemple charte pour les utilisateurs, les administrateurs, etc.).

S'agissant des mesures liées à des systèmes d'information, le cadre de référence COBIT et le modèle de gouvernance des systèmes d'information fournissent une base appréciable pour identifier des mesures applicables aux critères de sécurité propres aux systèmes d'information (quelle pratique de contrôle est en place pour atteindre les critères de sécurité[54] ? le degré de maturité acquis par l'organisation est-il de nature à limiter les risques ? etc.). Les mesures proposées sont principalement des bonnes pratiques et des dispositifs de prévention et de détection d'incidents.

En France, la CNIL catégorise ces mesures existantes ou prévues en deux grandes parties :

- les mesures de nature juridique garantissant le respect des principes fondamentaux, c'est-à-dire les mesures de conformité, qu'il convient obligatoirement de détailler. Il s'agit des mesures garantissant la proportionnalité et la nécessité du traitement et des mesures protectrices des droits des personnes concernées.
- et les mesures destinées à traiter les risques liés à la sécurité des données, c'est-à-dire les mesures de sécurité des données des traitements (par exemple, anonymisation ou chiffrement), les mesures générales de sécurité du système dans lequel le traitement est mis en œuvre (par exemple, sécurité de l'exploitation ou contrôles d'accès physiques), et les mesures organisationnelles ou de gouvernance (par exemple, gestion des projets ou gestion des incidents ou des violations de données)
- et, à titre d'exemple, fournit le modèle d'identification et de documentation de ces mesures existantes ou prévues adaptable comme nécessaire dans son guide PIA Les modèles[55].

[54] Confidentialité, intégrité, disponibilité, conformité, fiabilité.

[55] Source « Analyse d'impact relative à la protection des données : PIA, les modèles »- CNIL février 2018

Par ailleurs et à titre d'exemple, la Cnil a listé des bonnes pratiques et des mesures visant à traiter des risques sur la sécurité des données personnelles dont le tableau de synthèse est repris ci-dessous[56].

Fiches		Mesures	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	☐
		Rédigez une charte informatique et donnez lui une force contraignante	☐
2	Authentifier les utilisateurs	Définissez un indentifiant (login) unique à chaque utilisateur	☐
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	☐
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	☐
		Limitez le nombre de tentatives d'accès à un compte	☐
3	Gérer les habitations	Définitions des profils d'habilitation	☐
		Supprimez les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	☐
		Informez les utilisateurs de la mise en place du système de journalisation	☐
		Protégez les équipements de journalisation et les informations journalisées	☐
		Prévoyez les procédures pour les notifications de violation de données à caractère personnel	☐
5	Sécuriser les postes de travail	Prévoyez une procédure de vérouillage automatique de session	☐
		Utilisez des antivirus régulièrement mis à jour	☐
		Installez un "pare-feu" (firewall) logiciel	☐
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	☐
6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	☐
		Faites des sauvegardes ou des synchronisations régulières des données	☐
		Exigez un secret pour le déverrouillage des smartphones	☐
7	Protéger les réseau informatiqure interne	Limitez les flux réseaux au strict nécessaire	☐
		Sécurisez les accès distants des appareils informatiques nomades par VPN	☐
		Mettez en oeuvre le protocole WPA2 ou WPA2-PSK pour les réeaux WI-FI	☐
8	Sécurisez les serveurs	Limitez l'acccès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installez sans délai les mises à jour critiques	☐
		Assurez une disponibilité des données	☐

[56] Guide sur la sécurité des données personnelles 2018 , p. 30

9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en oeuvre	☐
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les URL	☐
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	☐
		Mettez un bandeau de consentement pour les cookies non nécessaire au service	☐
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	☐
		Stockez les supports de sauvegarde dans un endroit sûr	☐
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	☐
		Prévoyez et testez régulièrement la continuité d'activité	☐
11	Archiver de manière sécurisée	Mettez en oeuvre des modalités d'accès spécifiques aux données archivées	☐
		Détruisez les archives obsolètes de manières sécurisée	☐
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	☐
		Encadrez par un responsable de l'organisme les interventions par des tiers	☐
		Effacez les données de tout matériel avant sa mise au rebus	☐
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats de sous-traitants	☐
		Prévoyez les conditions de restitution ou de destruction des données	☐
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc..)	☐
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	☐
		Assurez-vous qu'il s'agit du bon destinataire	☐
		Transmettez le secret lors d'un envoi distinct et via un canal différent	☐
15	Protéger les locaux	Resteignez les accès au locaux au moyens de portes vérouillées	☐
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	☐
16	Encadrer les développements informatiques	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	☐
		Évitez les zones commentaires ou encadrez-les strictement	☐
		Testez sur des données fictives ou anonymisées	☐
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	☐
		Conservez les secrets et les clés cryptographiques de manières sécurisée	☐

Pour finir, les mesures identifiées doivent être introduites dans l'analyse pour réévaluer les risques et identifier, si besoin, des mesures complémentaires nécessaires pour atteindre un niveau de risque acceptable par l'organisation. Les mesures retenues doivent être adaptées et proportionnées au niveau de risque recherché et il pourra être utile de réaliser des analyses coûts/bénéfices afin de sélectionner les mesures pertinentes.

Enfin, une organisation pourra décider d'arrêter ou de refondre un projet si elle estime que, malgré les solutions de suppression ou de réduction envisagées, les risques résiduels ne sont toujours pas acceptables ou si les mesures envisagées ne peuvent être raisonnablement mis en œuvre en raison d'un rapport coûts/bénéfices trop défavorable.

4.2.2.6 *Cartographier et décrire les risques résiduels et leurs impacts potentiels*

Dans le cadre de cette troisième étape de la phase 2, le groupe de travail considère que l'étendue de l'analyse d'impact et la documentation subséquente doivent être proportionnées à la nature du traitement envisagé, au nombre de personnes concernées et au niveau de risque identifié. Par exemple, si la gravité des évènements redoutés est négligeable ou faible, l'étude des menaces pourra être allégée.

Tout projet qui implique la collecte, l'utilisation, le traitement, le stockage, la restitution ou la destruction de données à caractère personnel peut engendrer des risques sur la vie privée, si les opérations ne sont pas correctement conçues ni exploitées. Dès que le traitement concerne des données à caractère personnel, il existe des risques sur la vie privée.

Par exemple, les risques sont susceptibles de survenir de vulnérabilités :

- liées à l'organisation :
  - absence de mesure de sécurité d'accès aux données ;
  - absence de protection de l'intégrité des données ;
  - non-pertinence des données, moyens de traitement ou destinataires ;
  - absence de définition des conditions d'archivage des données ;
  - absence de mise en place d'une procédure de gestion des droits des personnes ;
  - absence d'encadrement de flux de données effectués vers des pays situés en dehors de l'Union européenne ;
  - détournement de finalité ;
  - etc.
- externes à l'organisation :
  - vol de données ;
  - détournement de finalité ;
  - insuffisance des mesures de sécurité mises en œuvre par les prestataires ;
  - etc.

A ce titre, il est important de noter que l'article 35 du Règlement paragraphe 1 mentionne la conduite d'une analyse d'impact

relative à la protection des données afin d'identifier les risques élevés « pour les droits et libertés des personnes physiques », et l'article 35 du Règlement paragraphe 7 précise que l'analyse doit comporter une « évaluation des risques pour les droits et liberté des personnes ». L'évaluation des risques ne se limite donc pas à ceux portant atteinte à la vie privée, et en particulier à la protection des données à caractère personnel, et il convient de prendre en compte les droits et intérêts légitimes des personnes concernées par les données et des autres personnes touchées. Le G29 rappelle ainsi que « les droits et libertés des personnes physiques concernent en premier lieu le droit à la vie privée, mais induit aussi d'autres droits fondamentaux comme la liberté d'expression, la liberté de pensée, la liberté de mouvement, l'interdiction de discrimination, le droit à la liberté, de conscience et religion »[57].

Dans le cadre de la conduite d'une analyse d'impact sur la protection des données à caractère personnel, il convient donc d'identifier de manière systématique tous les risques susceptibles d'affecter le respect des droits et libertés des personnes, et en cas de flux de données hors UE, les risques liés à la conformité réglementaire locale seront aussi identifiés et appréciés.

La méthodologie d'identification de ces risques s'appuiera de préférence sur celles existantes dans le cadre du système de gestion des risques de l'organisation ou dans le cadre de préconisations formulées dans certains secteurs d'activité par des instances professionnelles ou des régulateurs, ou sur tout autre guide de bonnes pratiques, reconnu.

D'une manière générale, l'identification des risques doit être objective et conduite par des acteurs indépendants, qu'ils soient internes ou externes à l'organisation. De plus, comme cela a déjà été indiqué, la consultation des acteurs pertinents, en interne ou en externe, est une source d'information à ne surtout pas négliger.

Quantification des risques

Le niveau d'un risque est estimé en termes de gravité des évènements redoutés (impact) et en termes de vraisemblance (probabilité d'occurrence) des menaces qui permettraient aux évènements redoutés de survenir. De façon simplifiée, il se calcule selon la formule :

« Niv. = (Impact x Probabilité d'occurrence) ».

La gravité des évènements redoutés (l'impact) est appréciée au regard du caractère identifiant des données à caractère personnel (par exemple : nom, prénom, date de naissance, ou numérotation neutre), et de son caractère préjudiciable. Le caractère préjudiciable pourra être évalué en fonction des atteintes possibles aux droits et libertés fondamentaux des personnes physiques, des valeurs de l'entreprise ou de l'organisme responsable du traitement et de son appétence aux risques (« risk appetite »).

Le cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données approuvé par

[57] Article 29 data Protection Working Party (WP29) statement 14/EN WP 218(p.4)

le G29 précise que les risques doivent « être quantifi[és] de manière relative ». Tandis que le responsable de traitement « devrait déterminer, compte tenu des principes de proportionnalité, la probabilité de voir se concrétiser les risques pour la vie privée dans des conditions raisonnables »[58].

L'évaluation finale des risques sera établie en tenant compte des mesures de suppression ou de réduction existantes.

Métriques

La méthode Ebios, à l'instar d'autres méthodes d'analyse de risque, se retrouve confrontée à l'épineuse question de l'estimation de deux éléments fondateurs de l'équation du risque, à savoir la probabilité d'occurrence d'une violation et l'impact induit, ce dernier pouvant se décomposer en une «chaîne» d'impacts représentée par un modèle de branchement conditionnel.

La méthode Ebios est basée sur une méthode d'approche qualitative du risque. Les niveaux arrêtés par la méthode se limitent à « négligeable », « limité », « important », « maximal » propres à chaque responsable de traitement.

Ces niveaux ne sont intelligibles qu'en fonction de la perception qu'en a le responsable de traitement. Cette perception doit être confrontée aux éléments quantifiés identifiés dans les différentes bases de données qui sont constituées par le responsable de traitement ou qui lui sont accessibles (incidents, sinistres, etc.).

S'appuyant sur la méthode Ebios, la CNIL propose dans son guide « PIA 1, la méthode » février 2018 de caractériser la gravité et la vraisemblance sur l'échelle de notation à 4 niveaux de la méthode Ebios.

De manière identique, la norme ISO29134 juin 2017 propose une notation sur 4 niveaux de la gravité et de la probabilité d'occurrence.

Exemples de sources

Les systèmes d'information sont, selon les secteurs d'activité et la maturité des outils de gouvernance, pourvoyeurs de métriques. À défaut de système d'information, les métriques peuvent être obtenues sur base d'interviews d'experts métier ou dans le cadre de groupes de travail regroupant des représentants pluridisciplinaires du domaine.

Une base de sinistralité qui consigne les sinistres déclarés permet d'établir des typologies de sinistres et d'identifier le nombre de sinistres de typologie identique (occurrence) ou le montant des dommages (gravité).

Une base contentieuse souvent gérée par les départements juridiques permet aussi d'identifier l'occurrence (par exemple, nombre

[58] Cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données du 11-2-2011, mis à jour le 28-10-2015, p. 10.

de contentieux par famille) et le niveau de gravité (correspondant à la demande). En pratique, le risque maximal peut être représenté par la demande du plaignant, la gravité du risque peut aussi être évaluée par le niveau de provision correspondant à l'estimation la plus juste du risque encouru, sachant que le montant de la condamnation informe sur la gravité réelle.

Une base de plaintes qui centralise des réclamations orales ou écrites est aussi source d'indicateurs pour effectuer la cotation des risques.

D'une manière générale, les bases d'incidents en place dans les organisations sont constituées de données historiques permettant de procéder à la cotation des risques. Il est important de s'assurer que les risques liés au respect de la vie privée y sont enregistrés.

4.2.2.7 *Décrire les risques résiduels acceptés et prévoir la mise en œuvre des actions correctives*

Pour cette avant-dernière étape de la deuxième phase, il convient de formaliser la décision d'accepter ou pas les risques résiduels et de formaliser le plan d'actions associé (Qui ? Quand ? Comment ?).

L'exploitation opérationnelle de l'application soumise à l'analyse d'impact n'est possible qu'après acceptation formelle par l'organisation des risques résiduels, c'est-à-dire après la mise en œuvre du plan d'actions visant à rendre les risques résiduels acceptables.

Pour ce faire, les mesures de réduction ou de suppression des risques doivent être planifiées dans le projet pour être intégrées au traitement.

L'acceptation finale des risques résiduels doit faire l'objet d'un visa formel par le responsable de traitement.

La CNIL fournit un exemple de tableau pouvant être utilisé pour résumer l'évaluation de l'analyse d'impact (Source : PIA, les modèles - février 2018)

CADRE MÉTHODOLOGIQUE

CHAPITRE 4

Légendes				
Symbole :	○○○	●○○	○●○	○○●
Signification :	Non applicable	Insatisfaisant	Amélioration prévue	Satisfaisant

Mesures permettant de respecter les principes fondamentaux	Evaluation
Mesures garantissant la proportionnalité et la nécessité du traitement	
Finalités : déterminées, explicites et légitimes	○○○
Fondement : licéité du traitement, interdiction du détournement de finalité	○○○
Minimisation des données : adéquates, pertinentes et limitées	○○○
Qualité des données : exactes et tenues à jour	○○○
Durées de conservation : limitées	○○○
Mesures protectrices des droits des personnes des personnes concernées	
Information des personnes concernées (traitement loyal et transparent)	○○○
Recueil du consentement	○○○
Exercice des droits d'accès et à la portabilité	○○○
Exercice des droits de rectification et d'effacement	○○○
Exercice des droits de limitation du traitement et d'opposition	○○○
Sous-traitance : identifiée et contractualisée	○○○
Transferts : respects des obligations en matière de transfert de données en dehors de l'Union européenne	○○○

CHAPITRE 4

Mesures contribuant à traiter les risques liés à la sécurité des données	Evaluation
Mesures portant spécifiquement sur les données du traitement	
Chiffrement	OOO
Anonymisation	OOO
Cloisonnement des données (par rapport au reste du système d'information)	OOO
Contrôle des accès logiques des utilisateurs	OOO
Traçabilité (journalisation)	OOO
Contrôle d'intégrité	
Archivaxge	
Sécurité des documents papier	
Mesures générales de sécurité du système dans lequel le traitement est mis oeuvre	
Sécurité de l'exploitation	OOO
Lutte contre les logiciels malveillants	OOO
Gestion des postes de travail	OOO
Sécurité des sites Web	OOO
Sauvegardes	OOO
Maintenance	OOO
Sécurité des canaux informatiques (réseaux)	OOO
Surveillance	OOO
Contrôle d'accès physique	OOO
Sécurité des matériels	OOO
Éloignement des sources de risques	OOO
Protection contre les sources de risques non humaines	OOO
Mesures organisationnelles (gouvernance)	
Organisation	OOO
Politique (gestion des règles)	OOO
Gestion des risques	OOO
Gestion des projets	OOO
Gestion des incidents et des violation de données	OOO
Gestion de personnels	OOO
relations avec les tiers	OOO
Supervision	OOO

4.2.2.8 *Réaliser une revue générale, constater les risques résiduels, définir les modalités de la revue périodique ou sur événements déclencheurs et rédiger le rapport de PIA et valider*

Cette étape est la dernière de la deuxième phase, elle doit aboutir au rapport de PIA principal. Cependant avant sa finalisation, une règle de bonne pratique consiste à faire une revue générale afin de s'assurer que l'analyse est conforme à l'état du projet, que les mesures de suppression ou de réduction de risques ont été prises en compte et que les risques résiduels décrits correspondent à la réalité.

Une analyse d'impact est un instantané caractérisé par un contexte et un système dans un état précis. Or contexte et système sont dynamiques. Il convient donc de mettre régulièrement à jour l'analyse, soit en fonction d'une périodicité déterminée (tous les ans ou plus selon la nature ou la criticité de l'application), soit à la suite d'événements déclencheurs prédéterminés, dont voici quelques exemples possibles :

- intégration d'actions correctives dans le projet permettant de réviser le niveau de risque ;
- violation des données à caractère personnel (divulgation accidentelle, perte d'un support, etc.) ;
- plaintes de clients ;
- failles de sécurité dans une ou plusieurs applications (serveurs, mobiles, point de vente, etc.) ;
- évolution réglementaire ;
- changements chez un ou plusieurs sous-traitants (rachat, changements techniques, etc.) ;
- modifications (importantes) des applications ;
- modifications des finalités ;
- etc.

Le rapport d'analyse d'impact principal doit en particulier détailler les mesures de suppression ou de réduction des risques, existantes ou recommandées. Il doit indiquer en quoi elles sont adaptées aux différents risques et comment leur mise en œuvre doit permettre d'obtenir un niveau de risque acceptable. D'une certaine façon, il doit aussi « raconter l'histoire » du traitement et être compréhensible par le plus grand nombre, en permettant au lecteur de saisir, sans ambiguïté, les enjeux et les éventuels risques résiduels à mettre en balance des bénéfices attendus du traitement. Il peut contenir les éléments qui suivent :

- nom de l'application utilisée pour le traitement ;
- identification du/des rédacteurs ;
- éléments de traçabilité du circuit de validation du document ;
- identification de l'équipe qui a réalisé l'analyse d'impact ;

- identification des personnes interviewées (internes, externes), le cas échéant ;
- identification du responsable de traitement ;
- identification du responsable (propriétaire) de l'application ;
- description du contexte de l'organisation (existence d'une politique de protection de la vie privée, etc.) ;
- description du contexte de l'application ;
- description (précise) de la/des finalité(s) ;
- description (précise) des données collectées et éventuellement produites par l'application ;
- cartographie des flux de données avec identification des acteurs et de leurs implantations géographiques, si nécessaire ;
- analyse des risques sur les données à caractère personnel et en termes de droits et de libertés des personnes concernées ;
- identification des mesures et alternatives pour la suppression ou la réduction des risques, éventuellement complétées par une cartographie des risques actuels et cibles ;
- liste des recommandations – proposition de plan d'actions ;
- conclusion et décisions ;
- périodicité et déclencheurs pour la mise à jour de l'analyse d'impact et du rapport ;
- résumé pouvant faire l'objet d'une large diffusion sans enfreindre les règles de protection de la propriété intellectuelle de l'entreprise ;
- tout autre élément utile à la bonne compréhension de l'analyse ;
- Formalisation de la validation

Le rapport d'analyse d'impact est communiqué en interne en particulier au responsable de traitement, au responsable en charge de la sécurité des données, au responsable Informatique & Libertés et au responsable de la gestion des risques. Il peut être communiqué, en externe, à l'autorité de contrôle sur sa demande ou en cas de consultation de l'Autorité si les risques résiduels restent élevés. Ce rapport (ou éventuellement son résumé expurgé des informations relevant de la propriété intellectuelle) peut aussi être utilisé comme outil de communication et de sensibilisation aux risques liés au respect de la vie privée.

4.2.2.9 Revue périodique ou à la suite d'événements déclencheurs, mise à jour et, le cas échéant, correction(s)

Cette dernière étape est le seul constituant de la troisième et dernière phase de l'approche d'analyse d'impact présentée dans ce chapitre. Elle consiste à reprendre régulièrement l'analyse d'impact durant toute la durée de vie du traitement, soit après une période prédéterminée soit à la suite d'un ou de plusieurs événements faisant craindre une aggravation des risques pour les droits et libertés fondamentaux des personnes concernées. Il s'agit donc ici de reprendre tous les éléments consignés dans le rapport précédent et d'identifier les variations et leurs éventuelles conséquences.

En l'absence de tout changement, le rapport d'analyse d'impact précédent sera mis à jour avec ce simple constat.

En cas d'aggravation des risques, au contraire, la totalité de l'analyse devra être déroulée à nouveau pour identifier des solutions visant à supprimer les risques ou à les limiter. Si des solutions sont possibles et validées alors elles devront être mises en œuvre et les risques résiduels devront être évalués avant d'être consignés dans un rapport mettant à jour le rapport d'analyse d'impact précédent. Si au contraire, aucune solution satisfaisante ne peut être trouvée ou mise en œuvre –par exemple en raison d'un coût prohibitif au regard des effets attendus, le responsable de traitement devra reconsidérer son traitement et décider s'il accepte l'aggravation des risques ou s'il préfère les supprimer totalement en interrompant le traitement. Cette réflexion et cette décision devront aussi être formalisées dans une mise à jour du rapport d'analyse d'impact précédent.

Enfin, comme dans tout système de contrôle interne, une revue de conformité du traitement objet de l'analyse d'impact pourra être menée afin de valider que les processus et diverses mesures de réduction des risques décrits dans le rapport d'analyse d'impact et ses éventuelles mises à jour sont effectivement mis en œuvre et assurent le niveau de protection attendu.

ÉTUDE DE CAS
« APPLICATION PROGRAMME DE FIDÉLITÉ »

CHAPITRE 5

L'étude de cas suivante a pour objectif de permettre de visualiser l'approche documentaire pouvant être retenue.

Il est proposé d'utiliser l'outil logiciel développé par la Cnil.

Il est rappelé que la documentation est libre. Il est toutefois recommandé de respecter les critères listés dans l'annexe 2 des recommandations du groupe de l'article 29[59].

A noter que la dernière version de l'outil PIA téléchargeable sur le site de la Cnil est actuellement en cours d'agrément par l'ANSSI[60].

Le cas de l'application Programme De Fidélité a été choisi puisqu'il concerne potentiellement tous les consommateurs.

5.1 Présentation générale

L'étude qui suit concerne le cas fictif d'une grande enseigne du secteur de la grande distribution qui met en place un traitement pour la gestion et le suivi d'un programme de fidélité réservé aux personnes majeures. Ce traitement s'utilise sur une application à installer sur un smartphone.

Le traitement vise en particulier à :

- évaluer la fidélité des clients en fonction de leur historique d'achats ;
- informer le client en temps réel des acquis au titre du programme de fidélité ;
- suivre les modalités de transformation des avantages fidélité acquis ;
- identifier des habitudes de consommation des clients ;
- réaliser des statistiques générales sur les habitudes de consommation.

Il s'appuie sur les fonctionnalités suivantes :

- collecter et modifier les données d'identification des utilisateurs qui ont volontairement adhéré au programme, grâce à l'application pour mobiles ou via le site web dédié ;
- collecter et synchroniser l'historique des achats effectués dans n'importe quel magasin de l'enseigne pour évaluer la fidélité des clients (ex : liste des produits achetés, prix, fréquence des achats, etc.) ;

[59] Guidelines on Data Protection Impact Assessment and determining whether processing is « likely to result in a high risk »for the purposes of Regulation 2016/679 – Revised and adopted on 4 October 2017

[60] Agence nationale de la sécurité des systèmes d'information

- rétribuer la fidélité des utilisateurs sous forme de coupons d'achats, points de fidélité, cadeaux, etc. en fonction de critères tels que la fréquence des achats et les montants dépensés ;
- informer en temps réel les utilisateurs du suivi de leur participation au programme de fidélité via notifications push ;
- suivre l'usage fait par les utilisateurs de la rétribution de leur fidélité (conversion des points de fidélité/produit) ;
- établir des profils d'acheteurs, en fonction des habitudes de consommation des utilisateurs, afin de leur offrir des cadeaux rétribuant leur fidélité qui correspondent à leurs habitudes d'achat ;
- établir des statistiques générales et anonymes relatives aux habitudes de consommation des utilisateurs.

5.2 Analyse du contexte et cartographie des traitements mis en œuvre

Nom du traitement	
Entité juridique (Organisme)	EGD
Responsable du traitement (coordonnées)	EGD
Responsables du traitement conjoints	N/A
Direction ou service en charge de la mise en œuvre du traitement	Direction marketing
Sous-traitants (liste des sous-traitants)	HT _ Prestataire d'hébergement
DPO	Oui
Entités concernées	EGD
Finalités du traitement	Gestion et suivi d'un programme de fidélité via une application mobile avec production de statistiques anonymes : ▪ évaluer la fidélité des clients a la société EGD (en comptabilisant les passages en caisse des clients), ▪ élaborer des statistiques de fréquentation des magasins de la société EGD, ▪ élaborer des statistiques afin d'identifier les habitudes de consommation des clients, ▪ rétribuer la fidélité des clients a la société EGD a travers des bons d'achats correspondant a leurs habitudes de consommation (telles qu'elles ressortent des statistiques) et a faire valoir dans les magasins fréquentés.

Formalités (à accomplir ou accomplies) et référentiels applicables	Une déclaration normale a été effectuée auprès de la Cnil antérieurement au 25 mai 2018
Catégories de personnes concernées	Clients EGD
Présence de données relatives à des enfants	non
Catégories de données traitées à caractère personnel	Données d'identification : genre, nom, prénom, date d'anniversaire, adresse de courrier électronique, téléphone, n° du département de résidence Données relatives aux habitudes/profils de consommation : historique des achats effectués, coupons, points de fidélité, cadeaux offerts. Données de connexion à l'application : adresse IP, date et heure de la dernière connexion, rubriques consultées, token_id (téléphone). Données de géolocalisation (pour la détermination du magasin le plus proche).
Présence de données sensibles	Aucune donnée sensible n'est directement collectée auprès des clients. Cependant certaines informations sensibles peuvent être obtenues à partir de l'analyse de l'historique détaillé des achats. Notamment : Données pouvant révéler les croyances religieuses : produits kasher, halal, etc. Données relatives à la vie sexuelle : préservatifs. Données pouvant révéler l'origine raciale ou ethnique : produits de beauté ciblés (ex. : solution pour défriser des cheveux crépus, crème pour éclaircir la peau, etc.).
Catégories de destinataires et données concernées	Enseigne de la grande distribution : ▪ équipe informatique (consultation et modification) ▪ équipe marketing (consultation et production des analyses) Prestataire informatique hébergeur : ▪ équipe informatique (consultation
Zone de libre commentaire (ZLC)	Non
Encadrement des ZLC	N/A

Collecte directe des informations	Oui
Collecte indirecte des informations	Non
Information des personnes concernées	Les personnes concernées sont informées des traitements mis en œuvre, de leur finalité, de leurs droits, des destinataires, etc. au moment de l'adhésion au programme de fidélité.
Consentement des personnes concernées	Consentement spécifique à la collecte des données Acceptation des CGU de l'application
Durées de conservation	J / Données d'identification : nom, prénom, genre, date de naissance, adresse électronique, adresse postale, numéro de programme de fidélité. Durée de conservation de ces données : jusqu'à suppression de l'application par le client utilisateur. Destinataires : la société EGD (équipe dédiée du marketing et équipe informatique) et la société hébergeur de l'application. 2/ Données de connexion à l'application mobile et données de connexion à l'espace utilisateur accessible depuis le site web de la société EGD : adresse IP du téléphone, date et heure de la dernière connexion à l'application et à l'espace utilisateur, identifiant du téléphone. Durée de conservation de ces données : 6 mois. Destinataire : la société EGD et la société hébergeur de l'application. 3/ Données relatives aux articles achetés par le client dans les magasins de la société EGD : nom de l'article, quantité achetée, magasin de la société EGD, ces données étant collectées automatiquement à partir du ticket de caisse. Durée de conservation de ces données : jusqu'à suppression de l'application par le client utilisateur. Destinataire : la société EGD (équipe dédiée du marketing et équipe informatique) et la société hébergeur de l'application.
Interconnexion	Pas d'interconnexion avec une autre application, ou une base de données ou un fichier.
Flux transfrontières (FT) hors UE	L'application est hébergée sur les serveurs d'un prestataire informatique situé hors UE (Tunisie).

Encadrement des FT	Clauses spécifiques prévues dans le contrat d'hébergement entre l'enseigne et le prestataire informatique en sa qualité de sous-traitant, selon les modèles proposés par la Cnil, et transferts encadrés par des clauses contractuelles types de la Commission européenne.
Sécurité	Côté responsable de traitement : ▪ les locaux du siège de l'enseigne de grande distribution sont équipés d'un dispositif de contrôle d'accès par badge et d'un accueil. ▪ l'accès aux postes de travail est sécurisé par l'utilisation d'un identifiant personnel et d'un mot de passe. ▪ l'utilisation des systèmes d'information au sein de l'enseigne de grande distribution est encadrée par une Charte informatique générale pour l'ensemble des salariés ainsi que par une Charte administrateur spécifique à cette catégorie de salariés. ▪ toutes les opérations effectuées avec l'application de gestion du programme de fidélité sont enregistrées dans un journal. Côté utilisateur : ▪ chaque utilisateur dispose d'un compte propre, associé à l'application qu'il a téléchargée sur son appareil mobile et à son profil web, après avoir accepté les conditions générales d'utilisation, ainsi que la politique de gestion des données personnelles afférentes à l'application. ▪ chaque utilisateur a accès via l'application aux données collectées le concernant. ▪ les accès à l'application et les actions effectuées par l'utilisateur sur les données sont enregistrés dans l'application (journal). ▪ l'accès à l'application est protégé par un mot de passe librement choisi par l'utilisateur. toutes les transmissions via internet utilisent un protocole sécurisé

CHAPITRE 5

Pour compléter le tableau précédent, voici un schéma simplifié des flux de données. Les flèches en bleu (en pointillés et pleines) représentent les flux de données. Les flèches en orange indiquent des destinataires.

5.3 Arbre de décision

* Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a higt risk » for the purposes of Regulation 2016/679 du 4-4-2017 : WP248

Oui
Non

5.4 Analyse d'impact via le logiciel PIA Cnil

Informations du PIA

Nom du PIA
Application Programme de Fidélité

Nom de l'auteur
Julie Dupont

Nom de l'évaluateur
Pierre Durand

Nom du validateur
Amy Douglas

Date de création
04/10/2018

Contexte

Vue d'ensemble

Quel est le traitement qui fait l'objet de l'étude ?

Traitement mis en oeuvre par une enseigne de la grande distribution ("société EGD") dans le cadre d'une application mobile permettant à ses clients de bénéficier de son programme de fidélité.

Principales finalités :

- évaluer la fidélité des clients à la société « EGD » (en comptabilisant les passages en caisse des clients),
- élaborer des statistiques de fréquentation des magasins de la société « EGD »,
- élaborer des statistiques afin d'identifier les habitudes de consommation des clients,
- rétribuer la fidélité des clients à la société « EGD » à travers des bons d'achats correspondant à leurs habitudes de consommation (telles qu'elles ressortent des statistiques, faites à partir des achats effectués dans l'enseigne) et à faire valoir dans les magasins « EGD » fréquentés.

Enjeu: Proposer au client de bénéficier d'un programme de fidélité particulièrement adapté à son profil "acheteur", en fonction de ses habitudes de consommation et des magasins « EGD » qu'il fréquente.

Quelles sont les responsabilités liées au traitement ?

L'enseigne de la grande distribution est responsable du traitement (société « EGD »).

Quels sont les référentiels applicables ?

Néant

Évaluation : Acceptable

Données, processus et supports

Quelles sont les données traitées ?

Données collectées et traitées, durées de conservations associées et destinataires:

1/ Données d'identification: nom, prénom, genre, date de naissance, adresse électronique personnelle, adresse postale personnelle, numéro de programme de fidélité.
Durée de conservation de ces données: un mois maximum après la suppression de l'application par le client utilisateur.
Destinataires: la société « EGD » (équipe dédiée du marketing et équipe informatique) et la société hébergeur de l'application.

2/ Données de connexion à l'application mobile de la société « EGD »: adresse IP du téléphone, date et heure de la dernière connexion à l'application, identifiant du téléphone.
Durée de conservation de ces données: 6 mois.
Destinataires : la société « EGD » et la société hébergeur de l'application.

3/ Données relatives aux articles achetés par le client dans les magasins de la société « EGD » (données statistiques) : nom de l'article, quantité achetée, magasin de la société « EGD », ces données étant collectées automatiquement à partir du ticket de caisse.
Durée de conservation de ces données: un mois maximum après la suppression de l'application par le client utilisateur.
Destinataires : la société « EGD » (équipe dédiée du marketing et équipe informatique) et la société hébergeur de l'application.

4/ Données de géolocalisation :
Durée de conservation de ces données : aucune donnée n'est conservée au-delà de la durée d'utilisation de l'application par

l'utilisateur.
Destinataires : la société « EGD » et la société hébergeur de l'application.

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

1/ Collecte:
Les données sont collectées de la façon suivante:

- données d'identification collectées auprès du client via le formulaire d'adhésion en version papier,
- données d'identification collectées via formulaire de collecte depuis l'application,
- données de profil acheteur telles que transmises par l'utilisateur client, depuis l'application (statistiques),
- données de géolocalisation,
- données de connexion du téléphone mobile personnel à l'application.

2/ Stockage hébergeur:
Sont stockées côté hébergeur: l'ensemble de l'application et des données d'identification, de connexion et de profil utilisateur.

3/ Stockage côté société « EGD »:
Sont stockées, côté responsable de traitement, les données suivantes:

- données d'identification contenues dans le formulaire d'adhésion,
- données d'identification contenues dans l'application,
- données de profil acheteur (statistiques),
- données de géolocalisation,
- et données de connexion.

4/ Suppression:

- suppression de données ou de l'application (et donc la totalité des données) du serveur hébergeur,
- suppression de données ou de l'application (et donc la totalité des données) des supports de la société « EGD ».

Quels sont les supports des données ?

Coté clients utilisateurs:

- matériels : smartphone, ticket de caisse,
- logiciel: application mobile,
- réseau: wifi/4-4G (internet),
- support papier : le formulaire d'adhésion au programme de fidélité à renseigner en magasin.

Côté « EGD »:

- support papier: formulaire d'adhésion renseigné par le client,
- matériel: ordinateurs,
- réseau: wifi - fibre (internet),
- serveurs de la société « EGD » qui stockent l'application et les données qui y sont contenues,
- serveurs de l'hébergeur (qui stockent les bases de données à caractère personnel de l'application).

Évaluation : Acceptable

Principes fondamentaux

Proportionnalité et nécessité

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

Les données sont collectées pour fournir aux utilisateurs clients le service demandé, à savoir bénéficier via une application mobile d'un programme de fidélité adapté à leurs habitudes de consommation et dans les magasins de l'enseigne « EGD » fréquentés.

Les finalités du traitement sont les suivantes:

- évaluer la fidélité des clients à la société « EGD » (en comptabilisant les passages en caisse des clients),
- élaborer des statistiques afin d'identifier les habitudes de la consommation des clients,
- élaborer des statistiques de fréquentation des magasins de la société « EGD »,
- rétribuer la fidélité des clients à la société « EGD » à travers des bons d'achats correspondant à leurs habitudes de consommation (telles qu'elles ressortent des statistiques faites à partir des achats effectués dans l'enseigne), à utiliser dans les magasins « EGD ».

Évaluation : Acceptable

Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Article 6-1 a) du règlement: la personne a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques.

Article 6-1 b) du règlement: le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie (l'utilisateur client accepte les conditions contractuelles de l'application, en ayant téléchargé l'application mobile).

Évaluation : Acceptable
Commentaire d'évaluation :
Il est indispensable de vérifier qu'un consentement libre, spécifique, éclairé et univoque a été recueilli en conformité avec le RGPD.

S'agissant de la géolocalisation, il sera essentiel de recueillir le consentement spécifique de l'utilisateur, dans ces mêmes conditions.

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

- Les données d'identification (nom, prénom, adresse électronique personnelle, adresse postale personnelle, numéro de programme fidélité) sont nécessaires pour recevoir (si le client le souhaite) des bons de réductions via l'application par email ou courrier postal.
- NB : l'utilisateur doit obligatoirement remplir les champs nom prénom, et selon qu'il souhaite recevoir les bons de réductions par email ou par courrier postal, il doit saisir son adresse postale personnelle ou son adresse email personnelle (selon son choix).
- Le genre et la date de naissance associés aux données relatives aux habitudes de consommation telles qu'elles ressortent du ticket de caisse (statistiques) permettent d'établir des profils de consommation afin de proposer des bons de réductions adaptées au profil "acheteur", à faire valoir dans les magasins fréquentés.
- NB : les champs genre et date de naissance ne sont pas obligatoires. Ils permettent simplement d'améliorer la pertinence du profil acheteur.
- Les données de connexion à l'application (identifiant smartphone) sont traitées à des fins de sécurité.

Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

Le client utilisateur dispose de la possibilité de mettre à jour lui-même ses données d'identification directement dans l'application.

Évaluation : Acceptable

Quelle est la durée de conservation des données ?

Serveurs de l'hébergeur:
Les données d'identification et données de profil acheteur collectées depuis l'application sont conservées sur les serveurs de l'hébergeur jusqu'à un mois suivant la suppression de l'application (afin de permettre la restauration de l'application et des données contenues en cas d'erreur de suppression).
Les données de connexion sont conservées sur ces serveurs 6 mois maximum.

Les données d'identification et de profil acheteur (statistiques) collectées depuis l'application sont conservées jusqu'à un mois suivant la suppression de l'application.

Les données de géolocalisation ne sont pas conservées au-delà de la durée d'utilisation de l'application par l'utilisateur.

L'ensemble de ces données, hébergées sur les serveurs de l'hébergeur, est accessible pour la société « EGD ».

Formulaire d'adhésion papier:
Le formulaire d'adhésion papier au programme de fidélité de la société « EGD » est conservé jusqu'à sa numérisation sous format informatique. Le formulaire d'adhésion est supprimé après numérisation. Il est précisé que le formulaire d'adhésion est numérisé dans un délai maximum d'un mois suivant sa signature par l'utilisateur.

En local (sur le téléphone), l'utilisateur peut à tout moment supprimer toutes données (identification/profil acheteur).

Évaluation : Améliorable
Plan d'action / mesures correctives :
Mise en place d'une notification dans l'application proposant à l'utilisateur de supprimer son compte à la suite de la résiliation de son adhésion au programme de fidélité. Cette notification pourrait s'afficher au terme d'un délai correspondant à la durée de l'adhésion au programme, augmentée de la prescription légale.
Commentaire d'évaluation :
Il conviendrait de limiter la conservation du formulaire d'adhésion au format numérique pendant la durée du contrat augmentée de la durée de prescription légale.

Mesures protectrices des droits

Comment les personnes concernées sont-elles informées à propos du traitement ?

Le formulaire d'adhésion au programme de fidélité, ainsi que les formulaires de collecte figurant dans l'application comportent les mentions d'information I&L requises.

Évaluation : Acceptable
Commentaire d'évaluation :

Il conviendrait de s'assurer que ces mentions prennent bien en compte les exigences du RGPD, et les recommandations du groupe de l'article 29 (devenu le comité européen pour la protection des données) en la matière. En particulier, il sera indispensable de vérifier que les informations de premier niveau, telles que l'identité du responsable de traitement, la finalité et la liste des droits sont portés à l'attention de l'utilisateur et que les informations de deuxième niveau sont détaillées, en conformité avec les lignes directrices sur la transparence publiées le 11 avril 2018 par le groupe de travail de l'article 29.

Une attention particulière devra être portée à l'information nécessaire requise en matière de collecte de données de géolocalisation.

Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Le consentement au traitement est obtenu sur le formulaire d'adhésion au programme de fidélité (comportant aussi une mention I&L) ainsi que via la validation des formulaires de collectes de l'application (sur lesquels figurent également des mentions I&L adaptées).

Évaluation : Acceptable
Commentaire d'évaluation :
Il sera décisif de respecter les conditions requises par le RGPD en matière de consentement, en particulier, les lignes directrices sur le consentement, publiées le 10 avril 2018 par le groupe de travail de l'article 29.

Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

Les droits d'accès et à la portabilité peuvent s'exercer en envoyant un email à : vosdroits@egd.com. L'utilisateur dispose par ailleurs de fonctionnalités permettant d'accéder à ses données d'identification depuis l'application via la rubrique "Mon Profil" et à ses données de profil d'achat (statistiques)depuis la rubrique "Tickets de caisse". Il dispose également d'une fonctionnalité d'exportation de ses données de profil d'achat en format « csv ».

Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit à l'effacement (droit à l'oubli) ?

Les droits de rectification et à l'effacement peuvent s'exercer en envoyant un email à : vosdroits@egd.com. Par ailleurs, les utilisateurs disposent de fonctionnalités permettant de rectifier et d'effacer directement leurs données depuis la rubrique "Mon Profil". Les données de profil acheteur peuvent être modifiées et effacées depuis la rubrique "Tickets de caisse".
En cas d'effacement de l'ensemble des données, après suppression de l'application par le client, un AR est envoyé automatiquement par email au client pour accuser réception de la prise en compte de sa demande.

Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit d'opposition ?

Les droits de limitation et d'opposition s'effectuent par email à l'adresse: vosdroits@egd.com.

Évaluation : Acceptable
Commentaire d'évaluation :
Il convient de rappeler que figurent parmi ces droits à porter la connaissance de l'utilisateur, les droits d'opposition à la prospection commerciale et au profilage. Par ailleurs, il sera essentiel de mettre en place les procédures internes permettant de respecter le délai de réponse requis par le RGPD, c'est-à-dire, un mois. Pour ce qui concerne le droit de s'opposer à la prospection commerciale, il devra être rappelé à chaque communication.

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Oui, le contrat en place avec le sous-traitant hébergeur de l'application comprend notamment les mentions requises par le RGPD.

Évaluation : Acceptable
Commentaire d'évaluation :
Après vérification, le contrat en place prévoit les mentions requises à l'article 28 du RGPD.

Il faudra vérifier que la mention d'information portée à la connaissance de l'utilisateur indique l'existence d'un transfert hors Union Européenne, en conformité avec les articles 13 et 14 du RGPD.

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

L'hébergeur de l'application est localisé en Tunisie, qui n'est pas reconnu comme un pays assurant un niveau de protection des données adéquat. Le contrat en place avec ce sous-traitant comprend les clauses contractuelles type de la Commission Européenne.

Évaluation : Acceptable
Commentaire d'évaluation :
Confirmation obtenue que les clauses contractuelles types de la Commission Européenne ont été signées avec ce sous-traitant le 10 septembre 2018.

Risques

Mesures existantes ou prévues

Chiffrement

Accès aux bases de données hébergées sur les serveurs de l'hébergeur par les équipes Informatiques et les Commerciaux de la société « EGD » depuis un VPN.

Évaluation : Acceptable

Sécurisation des documents papier

Procédure de destruction du formulaire papier d'inscription après numérisation.

Évaluation : Acceptable

Lutte contre les logiciels malveillants

Mise en place de logiciels anti-virus/malware et accès restreint en cas d'accès aux données non-sécurisé.

Évaluation : Acceptable

Gestion des postes de travail

Postes de travail sécurisés, mise en place d'identifiant et mots de passe complexes, à changer à intervalles réguliers, mise en place de contrôleurs d'intégrité, de journalisation sur les postes, travail exclusivement sur un espace réseau sauvegardé et déconnexion automatique des postes de travail.

Évaluation : Acceptable

Sauvegarde des données

Mise en place d'une politique de sauvegarde régulière des données, avec une duplication dans des data centers localisés sur un site différent de la localisation du serveur principal (mais toujours en Tunisie).

Évaluation : Acceptable

Organisation de la politique de protection de la vie privée

Désignation d'un DPO Groupe « EGD » auprès de la CNIL.

Évaluation : Acceptable

Gestion des tiers accédant aux données.

Mise en place de procédures visant à empêcher l'accès non autorisé aux données à un tiers (ex: clauses contractuelles type, accès sécurisé aux données par profil et mot de passe régulièrement mis à jour, chiffrement, etc...).

Évaluation : Acceptable

Anonymisation

Anonymisation de la base de données en vue de son traitement par certaines équipes commerciales de la société « EGD » (le traitement anonymisé demeure stocké sur les serveurs de l'hébergeur).

Évaluation : Acceptable

Journalisation

Mise en place d'une politique de journalisation des événements et de conservation des traces qui en résultent. Les informations journalisées sont: l'identification de la personne connectée, les actions effectuées par la personne connectée (via VPN).

Évaluation : Acceptable

Protection contre les sources de risques non humaines

Mise en place d'un plan de secours et de remise en service en cas de phénomène climatique, ou incendie, ou accident externe ou interne côté hébergeur.

Évaluation : Améliorable
Plan d'action / mesures correctives :
Il sera essentiel de mettre en place un plan de formation/sensibilisation des équipes s'agissant des questions de la protection des données à caractère personnel et de prévoir un document interne définissant la politique à suivre en la matière, qui font partie de la documentation du DPO.

Sécurisation de l'exploitation

Mise en place d'une politique de sécurisation de l'exploitation, incluant par exemple des restrictions d'accès aux matériels (badges, contrôle à l'accueil, locaux fermés à clé en dehors des heures d'ouverture), logiciels anti virus/malware, avec mises à jour obligatoires et régulières, dispositifs permettant d'assurer une haute disponibilité des systèmes, SLA élevé s'agissant de la disponibilité des systèmes et des accès aux données stockées sur les serveurs de l'hébergeur, garanties de confidentialité élevées, plan de secours et de reprise d'activité testés.

Évaluation : Acceptable

Sensibilisation

Formation à des bonnes pratiques en matière de gestion des données à caractère personnel.

Évaluation : Acceptable

Sauvegarde

Sauvegarde régulière des données sur un site différent du site d'exploitation.

Évaluation : Acceptable

Plan de secours

Mise en place d'un plan de secours détaillé et de procédures à suivre en cas de sinistre.

Évaluation : Acceptable

Accès illégitime à des données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Conséquence d'une communication d'informations potentiellement sensibles (révélation de la religion, de l'orientation sexuelle, etc., pouvant éventuellement entraîner des risques de discriminations, menaces, agressions, etc.)

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Vol/consultation de données, usurpation (vol de smartphone)

Quelles sources de risques pourraient-elles en être à l'origine ?

Employé de la société « EGD », attaquant (hacker, ransomware,...), membre de l'entourage de l'utilisateur, employé de l'hébergeur

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Gestion des tiers accédant aux données., Sécurisation des documents papier, Organisation de la politique de protection de la vie privée, Sécurisation de l'exploitation, Lutte contre les logiciels malveillants, Gestion des postes de travail, Chiffrement, Anonymisation, Journalisation, Sensibilisation

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limitée, Gravité du risque limitée.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Limitée, Vraisemblance du risque limitée.

Évaluation : Acceptable

Modification non désirées de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Détérioration de la qualité du programme de fidélité

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Altération des données

Quelles sources de risques pourraient-elles en être à l'origine ?

Employé, attaquant (hacker, ransomware), membre de l'entourage

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Sécurisation de l'exploitation, Gestion des postes de travail, Gestion des tiers accédant aux données., Lutte contre les logiciels malveillants, Organisation de la politique de protection de la vie privée, Anonymisation, Journalisation, Chiffrement, Sécurisation des documents papier, Sensibilisation

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Négligeable, Gravité du risque négligeable.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Vraisemblance du risque négligeable.

Évaluation : Acceptable

Disparition de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Nécessité de recréer un compte, perte de l'historique des achats et donc du profil acheteur, détérioration de la qualité du programme de fidélité

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Problème affectant le serveur de l'hébergeur (événement technique, climatique, social, politique ou autre impactant le service d'hébergement)

Quelles sources de risques pourraient-elles en être à l'origine ?

Employé, sinistre, attaquant (hacker, ransomware)

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Protection contre les sources de risques non humaines, Lutte contre les logiciels malveillants, Journalisation, Sauvegarde, Plan de secours

CHAPITRE 5

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limitée, Gravité du risque limitée.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, Gravité du risque négligeable.

Évaluation : Acceptable

Plan d'action

Principes fondamentaux

Durée de conservation

Plan d'action / mesures correctives :
Mise en place d'une notification dans l'application proposant à l'utilisateur de supprimer son compte à la suite de la résiliation de son adhésion au programme de fidélité. Cette notification pourrait s'afficher au terme d'un délai correspondant à la durée de l'adhésion au programme, augmentée de la prescription légale.

Commentaire d'évaluation :
Il conviendrait de limiter la conservation du formulaire d'adhésion au format numérique pendant la durée du contrat augmentée de la durée de prescription légale.

Par ailleurs, en cas de résiliation par l'utilisateur de son adhésion au programme de fidélité, il conviendrait de prévoir la possibilité d'afficher une notification sur son téléphone lui proposant de supprimer son compte, à l'issue d'une période correspondant à la durée du contrat d'adhésion, augmentée du délai de prescription.

Mesures existantes ou prévues

Protection contre les sources de risques non humaines

Plan d'action / mesures correctives :

Il sera essentiel de mettre en place un plan de formation/sensibilisation des équipes s'agissant des questions de la protection des données à caractère personnel et de prévoir un document interne définissant la politique à suivre en la matière, qui font partie de la documentation du DPO.

ÉTUDE DE CAS
« APPLICATION PROGRAMME DE FIDÉLITÉ »

- Mesures prévues ou existantes
- Avec les mesures correctives mises en oeuvre
- (A)ccès illégitime à des données
- (M)odification non désirée des données
- (D)isparition de données

CHAPITRE 5

Impacts potentiels
Conséquence d'une commu
Détérioration de la qualité..
Nécessité de recréer un con
Menaces
Vol/consultation de donnée
Altération des données
Problème affectant le serve
Sources
Employé de la société « EC
Employé, attaquant (hacker
Employé, sinistre, attaquan
Mesures
Gestion des tiers accédant .
Sécurisation des documents
Organisation de la politiqu.
Sécurisation de l'exploitat..
Lutte contre les logiciels ...
Gestion des postes de trava
Chiffrement
Anonymisation
Journalisation
Sensibilisation
Protection contre les sourc.
Sauvegarde
Plan de secours
Accès illégitime à des données
Gravité : Limitée
Vraisemblance : Limitée
Modification non désirées de données
Gravité : Négligeable
Vraisemblance : Négligeable
Disparition de données
Gravité : Limitée
Vraisemblance : Négligeable

6.1 Traitement

Le règlement général sur la protection des données définit le traitement comme :

« 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 »[61].

6.2 Finalité

Dans son glossaire en ligne, la Cnil définit la finalité d'un traitement comme :

« L'objectif principal d'une application informatique de données personnelles. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.[62]»

6.3 Risque

Dans son guide relatif à l'étude d'impact sur la vie privée (EIVP)[63], la Cnil définit la notion de « risque sur la vie privée » comme un scénario hypothétique qui décrit :

- comment des sources de risques (ex : un salarié soudoyé par un concurrent) ;
- pourraient exploiter les vulnérabilités des supports de données à caractère personnel (ex : le système de gestion des fichiers, qui permet de manipuler les données) ;
- dans le cadre de menaces (ex : détournement par envoi de courriers électroniques) ;
- et permettre à des événements redoutés de survenir (ex. : accès illégitime aux DCP)
- sur les DCP (ex. : fichier des clients) ;
- et ainsi provoquer des impacts sur la vie privée des personnes concernées (ex : sollicitations non désirées, sentiment d'atteinte à la vie privée...).

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance :

- la gravité représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels

[61] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4
[62] https://www.cnil.fr/fr/glossaire
[63] Etude d'impact sur la vie privée (EIVP), 6-2015, p.6

compte tenu du contexte du traitement (nature des données, personnes concernées, finalité du traitement...) ;

- la vraisemblance traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

6.4 Responsable du traitement

Le règlement général sur la protection des données définit le responsable du traitement comme :

« 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; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre [64]».

6.5 Données à caractère personnel

Le règlement général sur la protection des données définit les données à caractère personnel comme :

« toute information se rapportant à une personne physique identifiée ou identifiable [65]».

6.6 Délégué à la protection des données

Le délégué à la protection des données est une création du règlement général sur la protection des données.

Il s'agit d'une personne désignée par un responsable du traitement ou un sous-traitant, chargée a minima des missions suivantes :

- « 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 en vertu du [règlement] et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données » ;
- « contrôler le respect du [règlement], d'autres dispositions du droit de l'Union ou du droit des États membres 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 »;
- « dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et

[64] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4
[65] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4

vérifier l'exécution de celle-ci en vertu de l'article 35 » du règlement ;

- « coopérer avec l'autorité de contrôle »;
- « 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 [66]».

6.7 Traitement automatisé

Au titre de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, le traitement automatisé « s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion [67]» .

6.8 Profilage

Le règlement général sur la protection des données définit le profilage comme :

« toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique [68]».

6.9 Autorité de contrôle

Le règlement général sur la protection des données définit l'autorité de contrôle comme :

« une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51 » du règlement[69].

6.10 Données génétiques

Le règlement général sur la protection des données définit les données génétiques comme :

[66] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 39
[67] Conv. STCE, 108, art. 2
[68] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4
[69] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4

« les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question [70]».

6.11 Données biométriques

Le règlement général sur la protection des données définit les données biométriques comme :

« les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopique [71]».

6.12 Données concernant la santé

Le règlement général sur la protection des données définit les données concernant la santé comme :

« les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

6.13 Proportionnalité

Après avoir énoncé que « le traitement des données à caractère personnel devrait être conçu pour servir l'humanité », le règlement général sur la protection des données évoque le principe de proportionnalité en ces termes [72]:

« Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le [règlement général sur la protection des données] respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la [Charte des droits fondamentaux de l'Union européenne], consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique ».

[70] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4
[71] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4
[72] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., considérant (4)

6.14 Personne concernée

Le règlement général sur la protection des données définit la personne concernée comme :

« une personne physique identifiée ou identifiable ; 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 [73]».

6.15 Sécurité du traitement

Le règlement général sur la protection des données évoque la sécurité du traitement en prévoyant que le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque[74].

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Les mesures techniques et organisationnelles mises en place tiennent compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques.

Elles incluent entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

[73] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4
[74] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 32

6.16 Preuve

Selon la norme ISO 9000 : 2005[75], une preuve tangible désigne des : « données démontrant l'existence ou la véracité de quelque chose ».

La norme précise que la preuve tangible est obtenue par observation, mesurage, essai ou un autre moyen.

6.17 Sous-traitant

Le règlement général sur la protection des données définit le sous-traitant comme :

« 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 [76]».

6.18 Représentants des personnes concernées

Le règlement général sur la protection des données définit le « représentant » du responsable du traitement ou du sous-traitant comme :

« une personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du [règlement] [77]».

Par analogie, les représentants des personnes concernées pourraient être définis comme les personnes physiques ou morales établies dans l'Union, désignées par la personne concernée par écrit, qui les représentent en ce qui concerne leurs droits en vertu du règlement.

[75] Norme ISO 9000 : 2005 Systèmes de management de la qualité - Principes essentiels et vocabulaire.
[76] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4
[77] Règl. UE 2016/679 du 27-4-2007 : JOUE 2016 L 119 p. 1 s., art. 4

BIBLIOGRAPHIE INDICATIVE

CHAPITRE 7

7.1 Textes européens

- Directive 95/46/CE du 24-10-1995 relative à la protection des données à caractère personnel et à la libre circulation de ces données, JOCE 23-11-1995.
- Règlement CE 45/2001 du 18-12-2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JOCE 12-1-2001 L8.
- Recommandations de la Commission européenne du 12-5-2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence, JOUE 16-5-2009 L 122.
- Proposition de Règlement du Parlement européen et du Conseil du 25-1-2012 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données).
- Résolution législative du Parlement européen du 12-3-2014 sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Note from the President of the Council of the European Union dated 30-6-2014 regarding the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

7.2 Travaux du groupe de travail « Article 29 » sur la protection des données

- Avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) : Groupe « Article 29 » WP180 du 11-2-2011.
- Avis 01/2012 sur les propositions de réforme de la protection des données : WP 191 du 23-3-2012.
- Avis 08/2012 apportant des contributions supplémentaires au débat sur la réforme de la protection des données : WP199 du 5-10-2012.
- Avis 02/2013 sur les applications destinées aux dispositifs intelligents : WP 202 du 27-2-2013.
- Advice paper dated 13-5-2013 on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation.

7.3 Travaux des autorités de protection des données

- Guide « La sécurité des données personnelles – 2018 ».
- Guide mesures pour traiter les risques sur les libertés et la vie privée Cnil 6-2012.
- Article-by-article analysis paper on proposed new EU General Data Protection Regulation, Information Commissioner's Office 12-2-2013.
- Comment réaliser une évaluation d'impact sur la vie privée (EIVP) pour les dispositifs RFID ? Cnil 9-2013.
- L'évaluation d'impact sur la vie privée pour les dispositifs RFID : questions-réponses, Cnil, 26-9-2013.

7.4 Autres

- Recommendations for a privacy impact assessment framework for the European Union, PIAF 11-2012.
- Cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données du 11-2-2011, mis à jour le 28-10-2015.
- Report from the Cabinet Office of the United Kingdom's Government dated 6-2008 regarding Data Handling Procedures in Government.

COMPOSITION DU GROUPE DE TRAVAIL

GROUPE DE TRAVAIL ANIMÉ PAR :

- Alain BENSOUSSAN
- Serge YABLONSKY

RÉDACTEURS :

- Anne RENARD
- Florence HOUDOT
- Emmanuelle NAHUM
- Olivianne JUES

CONTRÔLE QUALITÉ :

- Hélène LEGRAS
- Dominique ENTRAYGUES

MEMBRES DU GROUPE DE TRAVAIL :

- **BENSOUSSAN Alain**, Avocat, Président ADPO
- **BINEAU Claude,** Atos, Membre ADPO
- **De CADEVILLE Aymonette,** Expertise juridique du SI –Juriste d'Entreprise, CNAM
- **DESHAYES Mireille,** Adjoint DPO Groupe, Groupe GROUPAMA, Membre ADPO
- **EL KHOURY Hadi,** Conseil indépendant en cartographie des traitements et en gestion des risques numériques
- **ENTRAYGUES Dominique,** Directeur Privacy, Groupe MICHELIN, Administrateur ADPO
- **FUZEAU Pierre,** Vice-président, SERDA
- **HOUDOT Florence,** Expert-comptable, Commissaire aux comptes, SYC Consultants, Membre ADPO
- **JOUBREL Michel,** Service du DPO, AXA France , Membre ADPO
- **JUES Olivianne,** Avocate
- **LEGRAS Hélène,** DPO, Groupe Orano, Vice-Présidente ADPO
- **NAHUM Emmanuelle,** Avocat associé, Quantic Avocats
- **RAMBALDINI Diane,** Conseil en gestion des risques numériques et informationnels, Crossing Skills
- **RENARD Anne,** Avocat, Directeur du département conformité et certification, Alain Bensoussan Avocats Lexing
- **SCHUMACHER Anne-Sophie,** Avocat, Juris Values
- **YABLONSKY Serge,** Expert-comptable, Commissaire aux comptes, SYC Consultants

l'Academie
SCIENCES TECHNIQUES COMPTABLES FINANCIERES

L'Académie est une initiative de l'Ordre des experts-comptables

ORDRE DES EXPERTS-COMPTABLES

"Ce cahier vous guidera dans la réalisation des analyses d'impact prévues par le RGPD, avec, à titre d'exemple, un cas pratique réalisé avec les outils de la CNIL."

GOUVERNANCE DES DONNEES PERSONNELLES ET ANALYSE D'IMPACT DANS LE CADRE DU RGPD

www.lacademie.info

CONTACTS

Académie des Sciences et Techniques Comptables et Financières

19 rue Cognacq-Jay, 75341 Paris Cedex 07
Tél. +33 (0)1 44 15 62 52

www.lacademie.info

William NAHUM
Président fondateur

Pierre VALENCIEN
Directeur Délégué
pvalencien@cs.experts-comptables.org