Cahier n°28

l'Académie
SCIENCES TECHNIQUES COMPTABLES FINANCIERES

GOUVERNANCE DES DONNEES PERSONNELLES ET ANALYSE D'IMPACT

OCTOBRE 2014

sage

EDITO

La protection des données personnelles est un enjeu important pour le respect de la liberté de chacun.

Les technologies numériques de l'internet font que nous sommes « pistés » en permanence et nos données personnelles permettent de connaître presque tout de nous.

Des enjeux économiques majeurs sont derrière ces phénomènes. Le BIG DATA permet aux commerçants d'offrir le bon produit au bon moment au bon prix à un individu identifié.

On peut trouver dans ces évolutions de nombreux bienfaits et avantages pour les entreprises, mais pour les consommateurs aussi.

Cependant les dérives peuvent exister. Jusqu'où les données personnelles peuvent-elles être utilisées ?
Certaines d'entre-elles reliées aux habitudes de consommation ne peuvent-elles servir aussi à caractériser socialement, voire politiquement, voire sexuellement, les individus ?

L'autre question est de savoir qui peut avoir accès à ces données ? Son médecin ? Son employeur ? Son voisin ?

L'Europe a décidé de renforcer les dispositions sur ce sujet en mettant en cause la responsabilité de ceux qui abuseraient de ces données et en simplifiant les démarches administratives permettent aux particuliers de préserver leur confidentialité.

Le règlement est en projet. Il s'agira de contrôle interne et d'analyse de risques. Le présent cahier insiste sur l'analyse d'impact qui montre une évolution importante dans le degré de réflexion et de maturité de la gouvernance en matière de données personnelles.

Je salue les membres du groupe de travail, en particulier Alain Bensoussan et Serge Yablonsky, ainsi que les représentants de nombreuses Entreprises qui ont apporté leurs expériences et leurs contributions à la réalisation de cet ouvrage utile.

William NAHUM
Président fondateur

EDITO

Nous nous connectons quotidiennement à un compte e-mail, un profil Facebook, un service bancaire par Internet ou à des services des pouvoirs publics. Pour ces transactions, nous avons besoin de nous identifier et de nous authentifier.

Nous transférons chaque jour des données privées ou non, sensibles ou non, pour l'ensemble de ces transactions. Plus que jamais, nous sommes confrontés à des questions sur la protection et la confidentialité de nos données personnelles lors de l'envoi d'informations sur Internet.

La croissance et la circulation toujours plus importante des données nécessitent que les sociétés mettent en place une vraie politique de sécurité, de gouvernance des données et de gestion des identités numériques afin d'empêcher leur vol ou leur perte.

En 2013 la Commission Européenne a lancé une enquête sur l'échange d'informations électroniques sensibles. Pour 53% des PME Européennes, le premier frein à la croissance des échanges électroniques concerne la sécurité d'accès, la fiabilité et la qualité de l'information dont l'absolue nécessité de garantir que ces données proviennent bien de l'entreprise sensée les avoir transmises. Ainsi sur la question de l'identité numérique et de l'authentification par exemple en continuité du projet européen ELSA (European Large Scale bridging Actionfor eID) qui recommandait la mise en place d'une consultation portant sur les conditions d'émergence d'une identité numérique européenne. Le rapport ELSA/EID soulignait l'importance pour l'Europe de la réussite de ce défi, et donnait les bases méthodologiques permettant d'aborder cette question de façon systémique.

La gouvernance des données personnelles doit donc prendre en compte la fiabilité et la qualité des données numériques personnelles tout autant que le respect des obligations juridiques et opérationnelles en matière d'archivage. Il est évidemment nécessaire de surveiller et normaliser la structure de l'information, avec de vrais mécanismes d'alerte.

Il est tout autant vital de contrôler et d'authentifier les personnes qui accèdent ou alimentent ces données. L'économie numérique où nous vivons nécessite que les entreprises appréhendent l'absolue nécessité de définir des politiques de gouvernance et de gestion des accès à l'information. Ce livre blanc pratique « Gouvernance des Données Personnelles » a pour ambition de donner des pistes de réflexions pour améliorer la gouvernance des données personnelles. Nous sommes heureux et fiers de soutenir cette initiative, qui vient nourrir notre réflexion sur l'identité Numérique, menée au sein de groupes de travail sous l'égide de la Commission Européenne tels que le SSEDIC et dans le respect des directives eIDAS et NIS.

L'essor de l'économie numérique au sein de l'Union Européenne a besoin d'un véritable réseau de confiance, de s'appuyer sur des standards et des modèles garantissant la sécurité et la valeur probante des échanges financiers et commerciaux, la fiabilité de ces données échangées entre les membres de la Communauté.

José TEIXEIRA
Responsable des Offres Cash Management et Paiements de Sage
Membre du Groupe de travail de la Commission Européenne SSEDIC (Scoping the Single European Digital Identity Community)

Project funded under ICT PSP Call4

AVANT PROPOS

La proposition de règlement de la Commission Européenne a des conséquences importantes sur les enjeux de gouvernance des données personnelles au sein des organismes. Ces dernières devront s'adapter à un principe de responsabilité accrue qui se traduit par l'obligation pour un responsable de traitement de rendre des comptes.

Concrètement, cela implique, pour le responsable du traitement, de prendre des mesures efficaces et appropriées afin de se conformer au règlement européen et d'apporter la preuve, sur demande de l'autorité de contrôle, que les mesures nécessaires ont bien été prises.

Il s'agit d'une démarche de renforcement du cadre de la gouvernance d'entreprise où les notions de contrôle interne et de gestion des risques revêtent une place majeure. L'introduction de l'obligation d'une analyse d'impact en est la traduction.

Dans ce contexte, la conduite de l'analyse d'impact se doit :
- d'être intégrée aux processus de gestion des risques des organisations et d'amélioration continue,
- d'être orientée sur les processus des organisations,
- d'être menée le plus tôt possible dans la conception des applications,
- d'être souple et adaptée au niveau de risques identifiés.

A ce jour, de nombreuses zones d'incertitudes subsistent, telle la notion de grande échelle ou de risques particuliers.

Le présent guide présente les réflexions du groupe de travail. Il sera mis à jour et actualisé au fur et à mesure de l'évolution des textes et de la jurisprudence ainsi que de la confrontation des expériences.

Ce livre blanc, réalisé par une équipe pluridisciplinaire comprenant des délégués aux données personnelles ou CIL des plus grands groupes, des RSSI, des ingénieurs spécialisés, des juristes d'entreprises, des avocats et des commissaires aux comptes, se veut un guide pratique pour :
- comprendre le cadre juridique de l'analyse de risques et de l'analyse d'impact
- comprendre quand une analyse d'impact est obligatoire
- comprendre comment conduire une analyse d'impact
- démontrer par l'exemple le déroulement d'une analyse d'impact

Au-delà du règlement européen, l'analyse de risques et l'analyse d'impact relatives à la protection des données personnelles sont des bonnes pratiques que les entreprises ont intérêt à appliquer pour montrer à leurs écosystèmes le respect qu'elles ont des personnes.

Serge YABLONSKY
Expert-comptable
Commissaire aux comptes

Alain BENSOUSSAN
Avocat à la Cour d'appel de Paris

COMPOSITION DU GROUPE DE TRAVAIL

Groupe de travail animé par :
Alain BENSOUSAN - Serge YABLONSKY

Rédacteurs :
Olivianne JUES, Florence HOUDOT, Eric CHARIKANE

Contrôle qualité :
Anne-Sophie SCHUMACHER

Membres du groupe de travail :

Annick BAILLY
Juriste - LA POSTE

Alain BENSOUSSAN
Avocat

Claude BINEAU
Cil - BULL

Sylvain BONENFANT
Cil - Département de Seine-Maritime

Eric CHARIKANE
Consultant indépendant - PIAWATCH

Mireille DESHAYES
Adjoint Cil - Groupe GROUPAMA

Hadi EL KHOURY
Conseil en Cybersécurité et en Modélisation des processus
O'SERVICE2 SEKIMIA

Dominique ENTRAYGUES
Privacy, Cil - Groupe MICHELIN

Pierre FUZEAU
Vice-président - SERDA

Marie-Noelle GIBON
Cil - Groupe La Poste

Muriel GRATEAU
Cil Groupe - Groupe GROUPAMA

Bertrand HIROT
Responsable sécurité, Cil CSO France, BT France

Alain GUISLAIN
PDG - TMG

Florence HOUDOT
Expert-comptable - Commissaire aux comptes SYC Consultants

Michel JOUBREL
Service du Correspondant informatique et libertés AXA France

Olivianne JUES
Avocate - ALAIN BENSOUSSAN AVOCATS

Eric LACHAUD
Project manager

Hélène LEGRAS
Cil - Groupe AREVA

Dominique MOISAND
PDG - ASK OPTIVAL

Emmanuelle NAHUM
Avocat - Cabinet Emmanuelle Nahum

Christian PARDIEU
Executive Counsel, Privacy & Regulatory Affairs - GE Corporate

Diane RAMBALDINI
Présidente - ISSA France / Crossing Skills

Anne-Sophie SCHUMACHER
Avocat - JURIS VALUES

Fabienne VILLARS
Cil - RENAULT SAS

Serge YABLONSKY
Expert-comptable Commissaire aux comptes SYC Consultants

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

PARTIE I - APPROCHE GÉNÉRALE

1. PRÉAMBULE

Le présent livre blanc 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 la proposition de règlement du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (ci-après règlement général sur la protection des données ou RGPD), publiée par la Commission européenne le 25 janvier 2012.

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 juridique, technique et économique.

Cette démarche est appelée à se généraliser, dans la mesure où elle correspond à l'esprit du RGPD visant 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).

2.1 La révision du cadre légal européen relatif à la protection des données à caractère personnel

La directive 95/46/CE du 24 octobre 1995 constitue aujourd'hui 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[1].

Près de 20 ans après l'adoption de la directive 95/46/CE, les institutions européennes ont entamé un processus de réforme de ce texte fondateur. Considérant que le cadre juridique actuel au sein de l'Union européenne apparaissait «satisfaisant en ce qui concerne ses principes et ses objectifs», la Commission européenne n'en a pas moins relevé «une véritable fragmentation de la mise en œuvre de la protection des données à caractère personnel au sein de l'Union européenne, une insécurité juridique, et le sentiment, largement répandu dans le public, que des risques importants subsistent, notamment dans l'environnement en ligne»[2].

[1] 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).
[2] Proposition Règl. CE 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) p. 2.

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 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. Le processus de révision du cadre légal de leur protection au sein de l'Union européenne avait ainsi 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'ajoutait également la volonté d'assurer une application rigoureuse des règles[3].

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, qui, pour entrer en vigueur, devra d'abord être adopté par le Parlement européen et le Conseil de l'Union européenne, a fait l'objet de très nombreux amendements de la part de ces deux instances. Chacune a d'ailleurs publié en 2014 une version qui promeut sa propre vision. La version finale, qui devrait être soumise au vote en 2015, sera issue de la phase dite de « trilogue » au cours de laquelle la Commission, le Parlement et le Conseil devront s'accorder sur un texte commun.

En attendant, le groupe de travail a pris le parti d'examiner les différentes propositions. En l'absence d'indication complémentaire, les références qui sont faites dans la suite de ce texte concernent la proposition initiale de la Commission publiée en janvier 2012.

2.2 Vers un principe de responsabilité des organismes

La proposition de 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 :

- l'obligation, sous certaines conditions tenant à l'organisme ou aux traitements mis en œuvre, de désigner un délégué à la protection des données[4],
- la consécration d'un droit à l'oubli numérique pour les personnes concernées ainsi qu'un droit à la portabilité des données[5],
- la création de l'obligation de mettre en œuvre la protection des données dès la conception et par défaut[6],
- l'introduction de l'obligation de notification des violations de données à caractère personnel[7],
- la prise en compte du principe de responsabilité (« accountability[8] »).

3 Proposition Règl. CE du 25-1-2012 p.2.
4 Proposition Règl. CE du 25-1-2012 art. 35.
5 Proposition Règl. CE du 25-1-2012 art. 17 et 18.
6 Proposition Règl. CE du 25-1-2012 art. 23.
7 Proposition Règl. CE du 25-1-2012 art. 31 et 32.
8 Proposition Règl. CE du 25-1-2012 art. 22.

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 règlementation 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 européen ;
- d'apporter la preuve, sur demande de l'autorité de contrôle, que les mesures appropriées ont été prises.

La proposition de RGPD décrit plusieurs de ces mesures dans son article 22 §(2) :

- la tenue de la documentation en application de l'article 28,
- la mise en œuvre des obligations en matière de sécurité des données prévues à l'article 30,
- la réalisation d'une analyse d'impact relative à la protection des données en application de l'article 33,
- le respect des obligations en matière d'autorisation ou de consultation préalables de l'autorité de contrôle en application de l'article 34, paragraphes 1 et 2,
- la désignation d'un délégué à la protection des données en application de l'article 35, paragraphe 1.

2.3 L'introduction de l'analyse d'impact

Au titre des mesures qui s'imposent aux responsables de traitement, la Commission européenne prévoit, au travers de l'article 33 de la proposition de RGPD, de rendre obligatoire la réalisation d'une analyse de l'impact de certains traitements envisagés par un organisme sur la protection des données à caractère personnel.
Cet article a fait l'objet de plusieurs propositions d'amendements, issues à la fois du Parlement européen[9] et du Conseil de l'Union européenne[10]. Il fait référence à une terminologie nouvelle en matière de protection des données à caractère personnel, avec notamment l'introduction des notions de « grande échelle », de « fiabilité » ou encore de « comportement ».

D'une manière générale, l'obligation de mener des analyses d'impact s'inscrit dans le cadre d'une tendance 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 au cours des dernières années[11].
Ainsi, si cette nouvelle obligation ne repose pas à ce jour sur un texte juridiquement contraignant, certains organismes ont 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.

9 La proposition de règlement général sur la protection des données a été largement étudiée par les différentes commissions du Parlement européen. Plusieurs rapports ont ainsi été publiés, dont notamment celui de la commission des libertés civiles, de la justice
et des affaires intérieures (LIBE), qui avait été saisie par le Président du Parlement européen afin d'examiner le texte. Le groupe de travail a choisi ici de se concentrer sur les propositions d'amendements adoptées par la formation plénière du Parlement européen le 12 mars 2014.
10 La proposition de RGPD a fait l'objet de plusieurs publications au sein du Conseil de l'Union européenne. Le groupe de travail a choisi de se concentrer sur le document adressé par le Président du Conseil au groupe « Échange d'informations et protection des données »
le 30 juin 2014, qui prend en compte les échanges ayant eu lieu au sein de ce groupe de travail.
11 Guide gérer les risques sur les libertés et la vie privée Cnil 6-2012 ; Guide mesures pour traiter les risques sur les libertés et la vie privée Cnil 6-2012 ; 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.

2.4 Politique générale

La mise en place d'analyses d'impact 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 ?

En premier lieu, la définition du périmètre de l'analyse d'impact (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 (le « Qui ? ») est également essentielle. Elle répond à des impératifs majeurs tels que la complétude de l'étude ou encore l'acceptation en interne des résultats de l'étude et des actions identifiées comme nécessaires.

De nombreux acteurs peuvent être impliqués dans une analyse d'impact. Par exemple, 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. Le recours à la sous-traitance peutégalement être envisagé.Par exemple, l'identificationet 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 traitements.

Le recours à la sous-traitance dès la phase 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 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.

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 financier et juridique liés à la réalisation d'une analyse d'impact tardive.

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 livre blanc, les grands axes de la méthodologie applicables à l'analyse d'impact, en attendant l'éventuelle adoption d'une norme internationale[12].

Le partage de réflexions et d'expériences au sein du groupe de travail a fourni la matière pour l'élaboration de ce livre blanc.

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 33 de la proposition de RGPD 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 depuis la fin des années 90. Dans tous ces pays, il apparaît sous la dénomination « Privacy Impact Assessment » ou PIA. Dans la version anglaise du RGPD, la Commission a choisi une autre appellation «Data Protection Impact Assessment » ou DPIA.

Dans un souci d'harmonisation avec la terminologie déjà utilisée par les pays précédemment mentionnés, le groupe de travail a fait le choix d'utiliser en français l'expression « analyse d'impact relative à la protection des données » ou en anglais « Privacy Impact Assessment » avec son acronyme PIA.

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.

3. PLAN

Le présent livre blanc 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,
- des études de cas.

[12] La norme ISO/IEC 29151 Privacy Impact Assessment est prévue pour une publication en juin 2016.

PARTIE II - PÉRIMÈTRE DE L'ANALYSE D'IMPACT

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 33 de la proposition de règlement général sur la protection des données.

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

La proposition de RGPD prévoit que l'analyse d'impact s'applique aux traitements présentant des risques particuliers au regard des droits et libertés des personnes concernées, et définit plusieurs critères permettant de déterminer les situations correspondantes.

Comme indiqué précédemment, la proposition de RGPD a fait l'objet de nombreux amendements de la part du Parlement européen comme du Conseil de l'Union européenne. Pour le Parlement, le texte de référence a été adopté en mars 2014 par la formation plénière du Parlement européen[13]. Pour le Conseil, il s'agit d'un document publié le 30 juin 2014[14]. A ce jour, les trois versions disponibles – Commission, Parlement et Conseil - de l'article 33 font apparaître des différences parfois significatives qui révèlent des visions différentes selon les instances qui en sont à l'origine. Il a donc paru opportun d'en tenir compte pour les différentes analyses de ce livre blanc. Un tableau comparatif est présenté en Annexe 1.

Le groupe de travail a étudié les différents critères permettant de déterminer les situations soumises à une analyse d'impact et les a 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 décliné en trois versions – présentées au Chapitre 2.3, correspondant chacune aux propositions de la Commission, du Parlement ou du Conseil. Il a été conçu comme un outil fonctionnel à la disposition des organismes et son utilisation est illustrée à travers deux études de cas présentées au chapitre 4.

Enfin, concernant la terminologie employée dans l'article 33, 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.

[13] 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.

[14] 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).

PARTIE II - PÉRIMÈTRE DE L'ANALYSE D'IMPACT

1. LES TRAITEMENTS PRÉSENTANT DES RISQUES PARTICULIERS

L'article 33 §(1) de la proposition initiale par la Commission du projet de règlement général sur la protection des données dispose que :

- « Lorsque les traitements présentent des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités, le responsable de traitement ou le sous-traitant agissant pour le compte du responsable de traitement effectuent une analyse d'impact des traitements envisagés sur la protection des données à caractère personnel ».

Les «traitements» concernés par l'analyse d'impact sont donc ceux présentant des «risques particuliers » au regard « des droits et libertés des personnes ». La nature, la portée 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.

1.1 La notion de traitement

Le groupe de travail a noté que la notion de « traitement », reprise dans l'article 33, 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 proposition de RGPD remplace le terme « appliquées » par « appliquée(s) »[16], ce qui permet de préciser qu'une opération isolée, telle que l'interconnexion ou la destruction de données, constitue également un traitement de données à caractère personnel.

La directive 95/46/CE et la proposition de RGPD listent également différents types d'opérations devant être considérées comme des traitements de données à caractère personnel.

[15] Dir. 95/46/CE du 24-10-1995 art. 2 b).
[16] Proposition Règl. CE du 25-1-2012 art. 4 §(3).

A ce titre, deux modifications ont été apportées par la proposition de RGPD pour qualifier un traitement de données à caractère personnel :

- l'ajout de la notion de « structuration »,
- 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 la proposition de règlement général sur la protection des données[17] 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 33 soit susceptible de s'appliquer aussi bien aux traitements automatisés qu'aux traitements non automatisés de données[18].

1.2 La référence aux droits et libertés des personnes

L'article 33 §(1) de la proposition de RGPD énonce que les « traitements » concernés par l'analyse d'impact sont ceux présentant des « risques particuliers » au regard « des droits et libertés des personnes ».

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 au regard des « droits et libertés des personnes », cette notion apparaissant plus large.

A cet égard, le groupe de travail souligne l'importance d'adopter une approche « multi-droit » 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 question pourrait également se poser de savoir si les traitements visés sont uniquement ceux qui présentent des risques au regard du droit et des libertés des personnes ou si d'autres types de risques devraient également être pris en compte dans la détermination du périmètre de l'analyse d'impact (par exemple, risques au regard du droit de la concurrence ?).

[17] L'article 4 §(3) de la proposition de 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, ainsi que l'effacement ou la destruction des données.

[18] Il est important de préciser que l'article 33 de la proposition initiale de la Commission restreint parfois le périmètre de l'analyse d'impact à certains traitements automatisés de données. Ainsi, l'article 33 §(2) point a) fait uniquement référence aux traitements automatisés de données liés à l'observation du comportement des personnes. De même, l'article 33 §(2) point d) vise expressément les fichiers informatisés de données relatives aux enfants, aux données génétiques ou biométriques.

1.3 La notion de risques particuliers

La notion de « risques particuliers » ne fait l'objet d'aucune définition dans la proposition de règlement général sur la protection des données. Il est seulement indiqué que ces risques s'apprécient « au regard des droits et libertés des personnes concernées ».

Au titre de l'article 33 §(1) les éléments devant être pris en compte pour déterminer si des traitements présentent des risques particuliers au regard des droits et libertés des personnes concernées sont :

- « leur nature »,
- « leur portée »,
- « leurs finalités ».

Quelques critères d'appréciation ressortent également des considérants (71) à (74) de la proposition de RGPD, à savoir :

- la taille du traitement
  - systèmes d'archivage à grande échelle ayant pour objet de traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, susceptibles d'affecter un nombre important d'individus,
  - application ou plateforme de traitement commune à plusieurs autorités ou organismes publics, à un secteur ou segment professionnel, ou relative à une activité transversale largement répandue,

- la privation d'un droit d'une personne,
- l'utilisation de technologies nouvelles.

1. La notion de traitements présentant des « risques particuliers » au regard « des droits et libertés des personnes concernées » figurait déjà dans le Règlement n°45/2001 du 18 décembre 2000[19] qui dresse une liste des traitements « susceptibles » d'entrer dans cette définition. Ces traitements incluent[20] :

- « 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 ».

[19] 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.
[20] Règl. CE 45/2001 du 18-12-2000, art. 27.

De la même manière, l'article 33 §(2) liste plusieurs traitements devant être considérés comme présentant des risques particuliers au regard des droits et libertés des personnes, en prenant soin toutefois d'indiquer que cette liste n'est pas limitative (grâce à l'utilisation de l'adverbe « notamment »).

Or, la notion de « risque » connaît de nombreuses définitions, parfois très différentes en fonction du secteur d'activité concerné.

En conséquence, et dans la mesure où la conduite d'une analyse d'impact permettra précisément de déterminer les différents niveaux de risque associés à un traitement, il conviendrait de préciser davantage la notion de « risques particuliers » visée dans l'article 33.

A ce titre, il est intéressant de noter que la version du RGPD publiée par le Conseil propose de supprimer l'adverbe « notamment » de l'article 33§(2), ce qui semble préconiser le recours à une liste exhaustive de situations reconnues comme présentant des risques particuliers au regard des droits et libertés des personnes.

Cette idée est également reprise par le Parlement européen, qui fait toutefois référence aux traitements susceptibles de présenter des risques « spécifiques ». Ce dernier appuie le principe d'une approche en trois temps, consistant à[21] :

- 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 traitement sont susceptibles de présenter des risques spécifiques »[22] ,
- 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[23] ,
- 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[24].

Enfin, le Groupe de l'article 29 (ci-après « G29 »), qui rassemble les autorités de protection des données à caractère personnel au sein des États membres de l'Union européenne, considère que l'analyse d'impact doit être réalisée également lorsque l'on ne peut savoir avec certitude si le traitement est susceptible de présenter des risques particuliers pour les droits et libertés des personnes concernées. En conséquence, il suggère de viser à l'article 33§(1) de la proposition de RGPD les traitements « susceptibles de » présenter des risques particuliers[25], afin de tenir compte de cet élément d'incertitude.

[21] Cette approche en plusieurs étapes est d'autant mieux mise en lumière par la création de deux nouveaux articles : l'article 32bis et l'article 33 bis.
[22] Résolution législative du Parlement européen du 12-3-2014, art. 32bis.
[23] Les traitements susceptibles de présenter des risques spécifiques qui sont concernés par l'analyse d'impact sont listés à l'art. 32bis.
[24] Résolution législative du Parlement européen du 12-3-2014, art. 33bis.
[25] Avis 01/2012 sur les propositions de réforme de la protection des données : Groupe « Article 29 » WP 191 du 23-3-2012, p. 17.

2. LISTE INDICATIVE DES TRAITEMENTS PRÉSENTANT DES RISQUES PARTICULIERS

Les réflexions du groupe de travail ont notamment porté sur les traitements considérés comme présentant des risques particuliers au regard des droits et libertés des individus, tels que listés à l'article 33§(2) de la proposition de règlement général sur la protection des données.

Ces traitements peuvent être organisés de la manière suivante :

- les traitements « à grande échelle »,
- les traitements sur la base desquels des décisions ou mesures sont prises,
- les traitements de surveillance,
- les traitements concernant des enfants, des données génétiques ou des données biométriques,
- les traitements soumis à consultation de l'autorité de contrôle ou du délégué à la protection des données.

2.1 Les traitements « à grande échelle »

2.1.1 Proposition de la Commission Européenne

La proposition de règlement général sur la protection des données fait plusieurs références à la notion de « grande échelle ».

L'article 33 §(2) fait ainsi entrer dans le périmètre de l'analyse d'impact :

- « l'évaluation systématique et à grande échelle des aspects personnels propres à une personne physique ou visant à analyser ou à prévoir, en particulier, la situation économique de ladite personne physique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement, qui est fondée sur un traitement automatisé et sur la base de laquelle sont prises des mesures produisant des effets juridiques concernant ou affectant de manière significative ladite personne »[26],

- « le traitement d'informations relatives à la vie sexuelle, à la santé, à l'origine raciale et ethnique ou destinées à la fourniture de soins de santé, à des recherches épidémiologiques ou à des études relatives à des maladies mentales ou infectieuses, lorsque les données sont traitées aux fins de l'adoption de mesures ou de décisions à grande échelle visant des personnes précises »[27],

[26] *Proposition Règl. CE du 25-1-2012 art. 33 §(2) point a).*
[27] *Proposition Règl. CE du 25-1-2012 art. 33 §(2) point b).*

- « la surveillance de zones accessibles au public, en particulier lorsque des dispositifs opto- électroniques (vidéosurveillance) sont utilisés à grande échelle »[28],

- « le traitement de données à caractère personnel dans des fichiers informatisés de grande ampleur concernant des enfants, ou le traitement de données génétiques ou biométiques »[29].

A titre liminaire, il convient de noter que la terminologie utilisée dans la version anglaise est légèrement différente de celle utilisée dans la version française du RGPD. La version anglaise utilise ainsi les termes suivants :

- « a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual »,

- « information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases where the data are processed for taking measures or decisions regarding specific individuals on a large scale »,

- « monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale »,

- « personal data in large scale filing systems on children, genetic data or biometric data ... ».

Le considérant (71) de la proposition de RGPD apporte quelques précisions sur la notion de grande échelle, en indiquant qu'un système d'archivage visant à traiter un volume considérable de données et susceptible d'affecter un nombre important de personnes présenterait des risques particuliers au regard des droits et libertés des personnes et nécessiterait donc une analyse d'impact.

La notion de grande échelle doit donc être entendue comme pouvant concerner à la fois le volume de données traitées et le nombre de personnes concernées.

[28] Proposition Règl. CE du 25-1-2012 art. 33 §(2) point c).
[29] Proposition Règl. CE du 25-1-2012 art. 33 §(2) point d).

2.1.2 Commentaires

S'il apparaît légitime de pointer du doigt les traitements mis en œuvre à grande échelle, en les considérant comme présentant des risques particuliers, il est important de noter que, dans le texte de l'article 33 proposé par la Commission, la référence à la notion de grande échelle réduit considérablement le périmètre de l'analyse d'impact. En effet, elle permettrait d'exclure du champ de l'analyse d'impact, par exemple, les traitements de données biométriques, de données relatives à la santé ou encore le recours à des dispositifs de vidéosurveillance qui seraient mis en œuvre à petite échelle.

Le G29 a également attiré l'attention sur la restriction introduite par l'expression «à grande échelle» dans les termes suivants[30] :

- « Il conviendrait de supprimer la restriction introduite par l'expression «à grande échelle» en ce qui concerne les traitements mentionnés à l'article 33, paragraphe 2, points b), c) et d), car le [G29] estime qu'une analyse d'impact relative à la protection des données est requise pour les traitements de ce type, même à petite échelle».

- «Cela vaut tout particulièrement en ce qui concerne le traitement des données biométriques, qui, de l'avis du [G29], devrait être considéré comme risqué dans certaines circonstances, et une analyse d'impact relative à la protection des données devrait dès lors être effectuée indépendamment d'un quelconque seuil prévu à l'article 33. ».

La résolution du Parlement européen souligne particulièrement le caractère sensible des traitements de données mis en œuvre à grande échelle. Le Parlement européen propose en effet de créer un nouveau critère permettant de faire entrer dans le périmètre de l'analyse d'impact :

- « le traitement de données à caractère personnel de plus de 5 000 personnes concernées sur une période de douze mois consécutifs »[31].

L'adoption d'un tel critère permettrait de prendre en compte les risques liés au traitement de données à caractère personnel se rapportant à un nombre important d'individus, et ce quelle que soit la nature des données ou des technologies utilisées.

[30] Avis 01/2012 du 23-3-2012, p. 18.
[31] Résolution législative du Parlement européen du 12-3-2014, art. 32bis.2 point a).

2.2 Les traitements sur la base desquels des décisions ou mesures sont prises

2.2.1 Proposition de la Commission Européenne

La proposition de règlement général sur la protection des données inclut dans l'analyse d'impact différents traitements sur la base desquels sont prises des décisions ou des mesures.

Plus précisément, l'article 33 §(2) fait entrer dans le périmètre de l'analyse d'impact :

- « l'évaluation systématique et à grande échelle des aspects personnels propres à une personne physique ou visant à analyser ou à prévoir, en particulier, la situation économique de ladite personne physique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement, qui est fondée sur un traitement automatisé et sur la base de laquelle sont prises des mesures produisant des effets juridiques concernant ou affectant de manière significative ladite personne »[32],

- « le traitement d'informations relatives à la vie sexuelle, à la santé, à l'origine raciale et ethnique ou destinées à la fourniture de soins de santé, à des recherches épidémiologiques ou à des études relatives à des maladies mentales ou infectieuses, lorsque les données sont traitées aux fins de l'adoption de mesures ou de décisions à grande échelle visant des personnes précises »[33].

Le considérant (21) de la proposition de RGPD apporte quelques précisions sur la notion de traitement pouvant être considéré comme « observant un comportement ». Il y est indiqué que :

- « afin de déterminer si une activité de traitement peut être considérée comme observant le comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur l'internet au moyen de techniques de traitement de données consistant à appliquer un profil à un individu, afin notamment de prendre des décisions le concernant ou d'analyser ou de prévoir ses préférences, son comportement et sa disposition d'esprit ».

2. La notion de « données de santé » est également précisée au considérant (26) de la proposition de RGPD, qui prévoit que :

- «les données à caractère personnel concernant la santé devraient comprendre, en particulier, l'ensemble des données se rapportant à l'état de santé d'une personne concernée ; les informations relatives à l'enregistrement du patient pour la prestation de services de santé ; les informations relatives aux paiements ou à l'éligibilité du patient à des soins de santé ; un numéro ou un symbole attribué à un patient, ou des informations détaillées le concernant, destinés à l'identifier de manière univoque à des fins médicales ; toute information relative au

[32] Proposition Règl. CE du 25-1-2012 art. 33 §(2) point a).
[33] Proposition Règl. CE du 25-1-2012 art. 33 §(2) point b).

patient recueillie dans le cadre de la prestation de services de santé audit patient ; des informations obtenues lors d'un contrôle ou de l' examen d'un organe ou d'une substance corporelle, y compris des échantillons biologiques; l'identification d'une personne en tant que prestataire de soins de santé au patient ; ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostic in vitro» .

Cette dernière notion doit donc être entendue de manière large.

2.2.2 Commentaires

Le groupe de travail a tout d'abord relevé que le périmètre de l'analyse d'impact tel que décrit à l'article 33 §(2) de la proposition de règlement général sur la protection des données permet d'inclure le traitement de données non nominatives, dès lors par exemple que la collecte de ces données permet l'étude du comportement des personnes[34].

Cette problématique est d'autant plus marquée dans la résolution du Parlement, qui fait référence de manière générale à « l'établissement de profils sur la base desquels sont prises des mesures produisant des effets juridiques concernant ou affectant de manière tout aussi significative ladite personne »[35].

Parmi les modifications proposées par le texte du Conseil, celui-ci vise également « l'établissement de profils » permettant l'évaluation systématique et à grande échelle des aspects personnels propres à des individus, « sur la base de laquelle sont prises des décisions produisant des effets juridiques concernant ou affectant gravement les personnes concernées »[36].

Par ailleurs, il ne semble pas que la notion de « mesure ou décision produisant des effets juridiques concernant ou affectant de manière significative un individu » ait été définie. Dans un avis du 23 mars 2012, le G29 considérait, à propos de la définition du profilage prévue à l'article 20§(1) de la proposition de RGPD, que les termes « l'affectant de manière significative » devaient être précisés[37]. Cet appel a été renouvelé dans un autre avis du G29 concernant la définition du profilage dans la proposition de règlement général sur la protection des données[38].

Le groupe de travail considère également que cette notion devrait être clarifiée, afin de mieux définir le périmètre de l'analyse d'impact.

[34] Cela sous réserve que le traitement envisagé entre dans le champ d'application du règlement.
[35] Résolution législative du Parlement européen du 12-3-2014, art. 32 bis §(2) point c).
[36] Note from the President of the Council of the European Union dated 30-6-2014, art. 33 §(2) point a).
[37] Avis 01/2012 du 23-3-2012.
[38] Advice paper dated 13-5-2013 on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation.

Enfin, il est intéressant de noter que, si l'article 33§(2) point b) fait référence notamment au traitement de données relatives à la vie sexuelle, à la santé, à l'origine raciale et ethnique des personnes, il ne semble pas que le traitement de données relatives aux opinions politiques, à la religion ou aux croyances, ainsi qu'à l'appartenance syndicale d'un individu ne soit particulièrement visé par l'analyse d'impact. Cette remarque vaut également pour les données relatives aux condamnations pénales ou à des mesures de sûreté connexes concernant un individu.

A cet égard, il convient de relever que le Conseil préconise notamment d'inclure dans l'article 33 (2) point b) les traitements de données qui révèlent les opinions politiques, la religion ou les croyances philosophiques, l'appartenance syndicale, et les traitements de données relatives aux condamnations, aux infractions ou aux mesures de sûreté, et de soumettre ces traitements à analyse d'impact, « lorsque les données sont traitées aux fins de l'adoption de décisions à grande échelle visant des personnes précises »[39].
La proposition du Parlement va plus loin encore et considère comme suffisamment risqués pour nécessiter une analyse d'impact notamment[40] :

- le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques d'un individu, son orientation sexuelle, son identité de genre, son appartenance et ses activités syndicales,
- le traitement des données concernant la santé ou relatives à la vie sexuelle d'un individu,
- le traitement des données relatives aux sanctions administratives, aux jugements, à des infractions pénales ou à des suspicions, à des condamnations, ou encore à des mesures de sûreté connexes.

Avec cette proposition, le Parlement considère ainsi que le traitement de données dites « sensibles », telles que décrites à l'article 9 §(1) de la résolution du Parlement, justifie en lui-même la conduite d'une analyse d'impact.

2.3 Les traitements de surveillance

2.3.1 Proposition de la Commission Européenne

La Commission européenne a également souhaité inclure dans le périmètre de l'analyse d'impact certains traitements de surveillance des individus.

L'article 33 §(2) point c) vise ainsi :

- « la surveillance de zones accessibles au public, en particulier lorsque des dispositifs opto-électroniques (vidéosurveillance) sont utilisés à grande échelle ».

[39] Note from the President of the Council of the European Union dated 30-6-2014, art. 33 §(2) point b).
[40] Résolution législative du Parlement européen du 12-3-2014, art. 32bis §(2) point b).

2.3.2 Commentaires

Il apparaît que les zones impactées par cet alinéa sont susceptibles de comprendre aussi bien :

- la voie publique,
- les bâtiments et installations publiques,
- les lieux recevant le public.

Si les dispositifs opto-électroniques sont seuls visés dans la proposition de RGPD, l'utilisation du terme « en particulier » suggère toutefois que ces derniers ne sont pas les seuls dispositifs concernés par l'analyse d'impact. Il semble au contraire que tous les mécanismes permettant la surveillance de zones accessibles au public soient visés.

Le texte du Conseil apporte toutefois une limitation à cette proposition en visant non pas « la surveillance de zones accessibles au public », mais plus restrictivement « la surveillance de zones accessibles au public à grande échelle »[41].

Dans son article 32 bis §(2) point e), la résolution du Parlement prévoit également de limiter le périmètre de l'analyse d'impact et ne fait ainsi référence qu'à la « surveillance automatisée à grande échelle de zones accessibles au public ».

En revanche, le Parlement introduit une nouvelle catégorie de traitement susceptible de présenter des risques, en considérant que « lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées », ces traitements doivent être soumis à analyse d'impact. Tel serait le cas par exemple des services en ligne qui collectent en permanence des données mesurant les pratiques des utilisateurs comme dans le cas du Quantified Self.

2.4 Les traitements concernant les enfants ou des données génétiques ou biométriques

2.4.1 Proposition de la Commission Européenne

La Commission européenne fait spécifiquement entrer dans le périmètre de l'analyse d'impact les données relatives aux enfants, ainsi que le traitement de données génétiques ou biométriques.
L'article 33 §(2) point d) de la proposition de règlement général sur la protection des données vise ainsi :

- « le traitement de données à caractère personnel dans des fichiers informatisés de grande ampleur **concernant des enfants, ou le traitement de données génétiques ou biométriques ».**

La notion « d'enfant » est définie à l'article 4§(18) de la proposition de RGPD comme « toute personne âgée de moins de 18 ans ».

[41] Note from the President of the Council of the European Union dated 30-6-2014, art. 33 §(2) point.

Au titre de l'article 4 §(10), sont considérées comme des « données génétiques », « toutes les données, de quelque nature que ce soit, concernant les caractéristiques d'une personne physique qui sont héréditaires ou acquises à un stade précoce de son développement prénatal ».

Enfin, l'article 4 §(11) définit les « données biométriques » comme « toutes les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques ».

2.4.2 Commentaires

Si la Commission européenne considère que le traitement de données concernant des enfants, ou le traitement de données génétiques ou biométriques est susceptible de comporter des risques particuliers, elle ne soumet à analyse d'impact que ceux de ces traitements qui sont mis en œuvre de manière automatisée et qui ont une grande ampleur.
Le Conseil suggère quant à lui de supprimer du périmètre de l'analyse d'impact les traitements de données relatives à des enfants. Il propose en revanche, pour les données biométriques et génétiques, d'enlever la référence au caractère informatisé des fichiers[42].

Le Parlement européen va plus loin encore en proposant non seulement de soumettre à une analyse d'impact les traitements de données génétiques ou biométriques quels qu'ils soient, les traitements de données relatives à des enfants dans des fichiers informatisés de grande ampleur, mais également les données relatives à des employés, lorsqu'elles figurent dans des fichiers informatisés de grande ampleur[43].

En outre, il est rappelé que le Parlement propose de soumettre à une analyse d'impact :

- les traitements de données révélant l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques d'un individu, son orientation sexuelle ou son identité de genre, son appartenance et ses activités syndicales,
- les traitements de données concernant la santé d'un individu ou relatives à sa vie sexuelle ; les traitements de données relatives aux sanctions administratives, aux jugements, à des infractions pénales ou à des suspicions, à des condamnations ou des mesures de sûreté connexes,
- le traitement de données de localisation.

Et cela que le traitement soit automatisé ou non, qu'il soit effectué à grande, moyenne ou à petite échelle et quelle que soit la finalité pour laquelle les données sont traitées.

Aucun critère additionnel, tenant à l'ampleur ou à la nature automatisée du traitement, ne devrait alors être pris en compte afin de faire entrer le traitement dans le périmètre de l'analyse d'impact.

[42] Note from the President of the Council of the European Union dated 30-6-2014, art. 33 §(2) point d).
[43] Résolution législative du Parlement européen du 12-3-2014, art. 32bis §(2) point b).

2.5 Les traitements soumis à consultation

2.5.1 Proposition de la Commission Européenne

La Commission européenne a souhaité également inclure dans le périmètre de l'analyse d'impact :

- « les autres traitements pour lesquels la consultation de l'autorité de contrôle est requise en application de l'article 34, paragraphe 2, point b) »[44].

L'article 34 §(2) point b) susvisé prévoit en effet que l'autorité de contrôle établit et publie une liste des traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, du fait de leur nature, de leur portée et/ou de leurs finalités, pour lesquels elle estime nécessaire de procéder à une consultation préalable. Cette liste doit être communiquée au comité européen de la protection des données.

L'autorité de contrôle pourra ainsi compléter la liste des traitements considérés comme « présentant des risques particuliers au regard des droits et libertés des personnes concernées, du fait de leur nature, de leur portée et/ou de leurs finalités ».

2.5.2 Commentaires

Le périmètre de l'analyse d'impact pourra être encore complété par les autorités de contrôle de l'Union européenne. Ainsi, par exemple, le groupe de travail a noté qu'à ce jour, malgré les risques qu'ils comportent au regard de la protection des données à caractère personnel, l'existence de flux transfrontières de données n'est pas considérée comme un élément révélateur d'un risque particulier, nécessitant la réalisation d'une analyse d'impact.

L'existence de flux transfrontières de données pourrait toutefois être incluse dans le périmètre de l'analyse d'impact, dans le cas où l'autorité de contrôle déciderait de soumettre ce type de traitement à consultation.
Il en va de même pour les traitements qui utilisent la technologie RFID. Ils ne figurent pas dans la liste des traitements présentant des risques particuliers pour les droits et libertés fondamentaux des personnes décrits par la proposition de RGPD alors même que la Commission a, dès mai 2009, souhaité que ceux-ci fassent l'objet d'une analyse d'impact spécifique comme indiqué dans la recommandation « 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 » [45].

[44] Proposition Règl. CE du 25-1-2012 art. 33 §(2) point e).
[45] Recommandations de la Commission européenne du 12-5-2009 sur la mise en oeuvre 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.

La prise en compte des risques liés à l'utilisation de technologies « nouvelles » est d'ailleurs présente dans le considérant (74) qui dispose :

> - « [...] des opérations de traitement exposent les droits et libertés concernées à un degré élevé de risques particuliers comme [...] par l'utilisation de technologies nouvelles ».

Il convient de noter que le Parlement européen propose de soumettre également à analyse d'impact les traitements pour lesquels la consultation du délégué à la protection des données serait requise[46].

L'implication du délégué à la protection des données dans la détermination du périmètre de l'analyse d'impact correspond bien au principe de responsabilité introduit dans la proposition de règlement général sur la protection des données et permettrait, en outre, de prendre en compte les spécificités liées à l'environnement propre à chaque organisme.

Le Conseil propose quant à lui que l'autorité de contrôle compétente établisse et publie une liste des traitements soumis à l'exigence d'une analyse d'impact, lorsqu'elle estime que ces traitements sont susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, et cela sans qu'une consultation préalable de l'autorité ne soit nécessairement requise pour ces traitements[47]. Cette liste devrait également être communiquée au Comité européen de la protection des données.

Pour finir, il est intéressant de noter qu'en ce qui concerne les violations de données à caractère personnel, le Parlement européen propose, en plus d'une obligation de notification à l'autorité de contrôle et aux personnes concernées, d'imposer la réalisation d'une analyse d'impact lorsque la violation « risque de porter atteinte à la protection des données à caractère personnel, de la vie privée, des droits ou des intérêts légitimes de la personne concernée »[48].

[46] Résolution législative du Parlement européen du 12-3-2014, art. 32bis §(2) point f).
[47] Note from the President of the Council of the European Union dated 30-6-2014, art. 33 §(2a) et §(2b).
[48] Résolution législative du Parlement européen du 12-3-2014, art. 32bis §(2) point g).

3. SYNTHÈSE

3. En conclusion de ce premier chapitre, il apparaît que les traitements entrant dans le périmètre de l'analyse d'impact sont tous les traitements présentant des « risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités ». Si cette notion nécessiterait d'être précisée, certains critères permettent d'ores et déjà de comprendre le type de traitement visé, à savoir :

- Concernant la nature du traitement :
- les traitements portant sur un volume important de données ou concernant un nombre important de personnes,
    - les traitements ayant recours à des technologies sensibles, telles que la biométrie,
    - les traitements concernant des populations sensibles, tels que les enfants,
    - les traitements impliquant la manipulation de données sensibles, telles que des données génétiques.

- Concernant la portée du traitement :

    - les traitements susceptibles d'engendrer la privation d'une personne d'un droit, et notamment les traitements sur la base desquels des mesures ou décisions concernant des personnes peuvent être prises.

- Concernant la finalité du traitement :

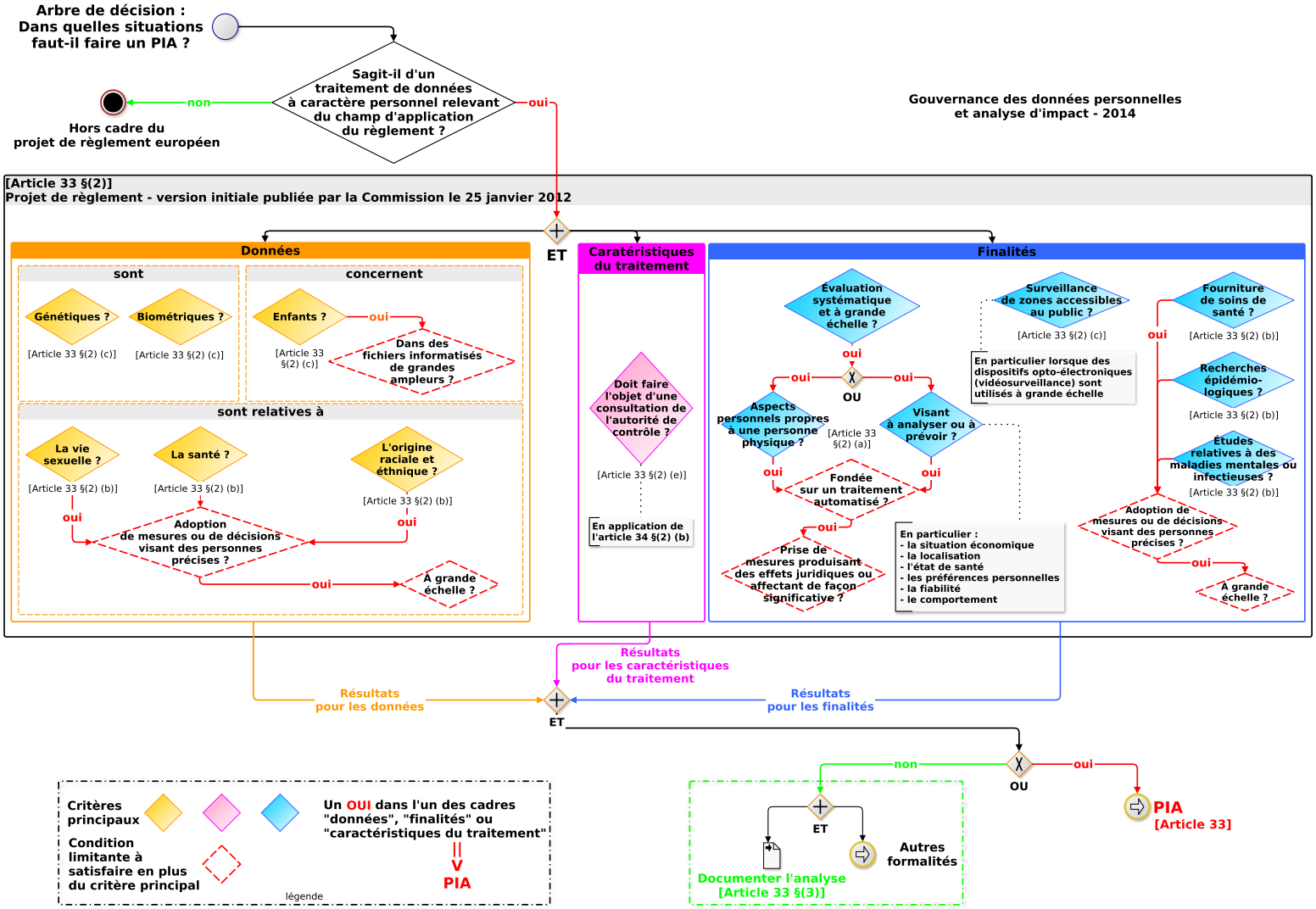
    - les traitements de surveillance.

Le périmètre de l'analyse d'impact pourra être précisé par les autorités de contrôle ou les délégués à la protection des données, afin d'augmenter la sécurité juridique des opérations.

Les trois illustrations qui suivent tentent respectivement de représenter, sous la forme « d'arbres de décision », les critères retenus par la Commission, le Parlement et le Conseil quant aux traitements pouvant présenter des risques particuliers.

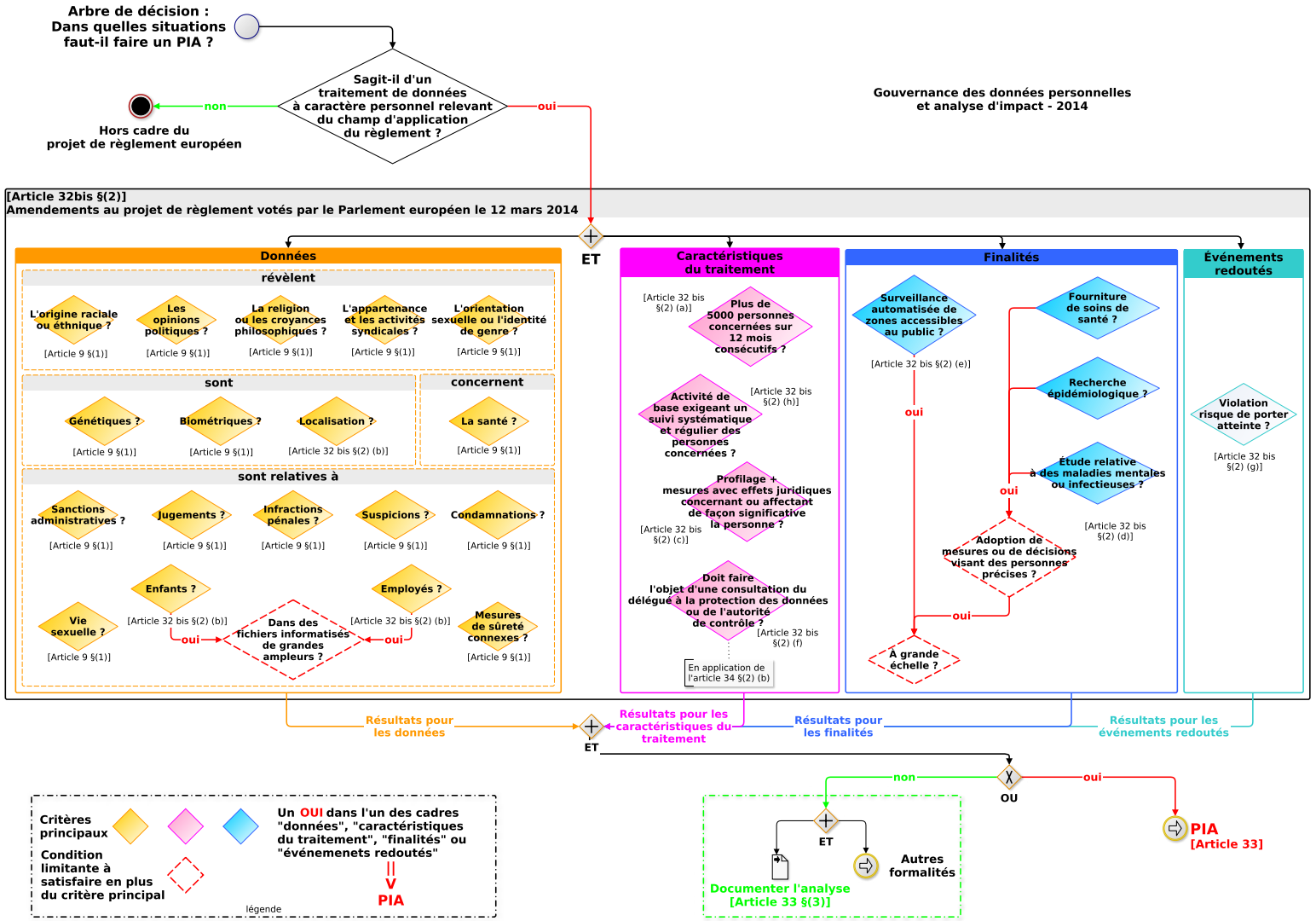
La méthodologie d'utilisation des arbres de décisions est présentée en Annexe 2.

Article 33 dans sa version initiale proposée par la Commission



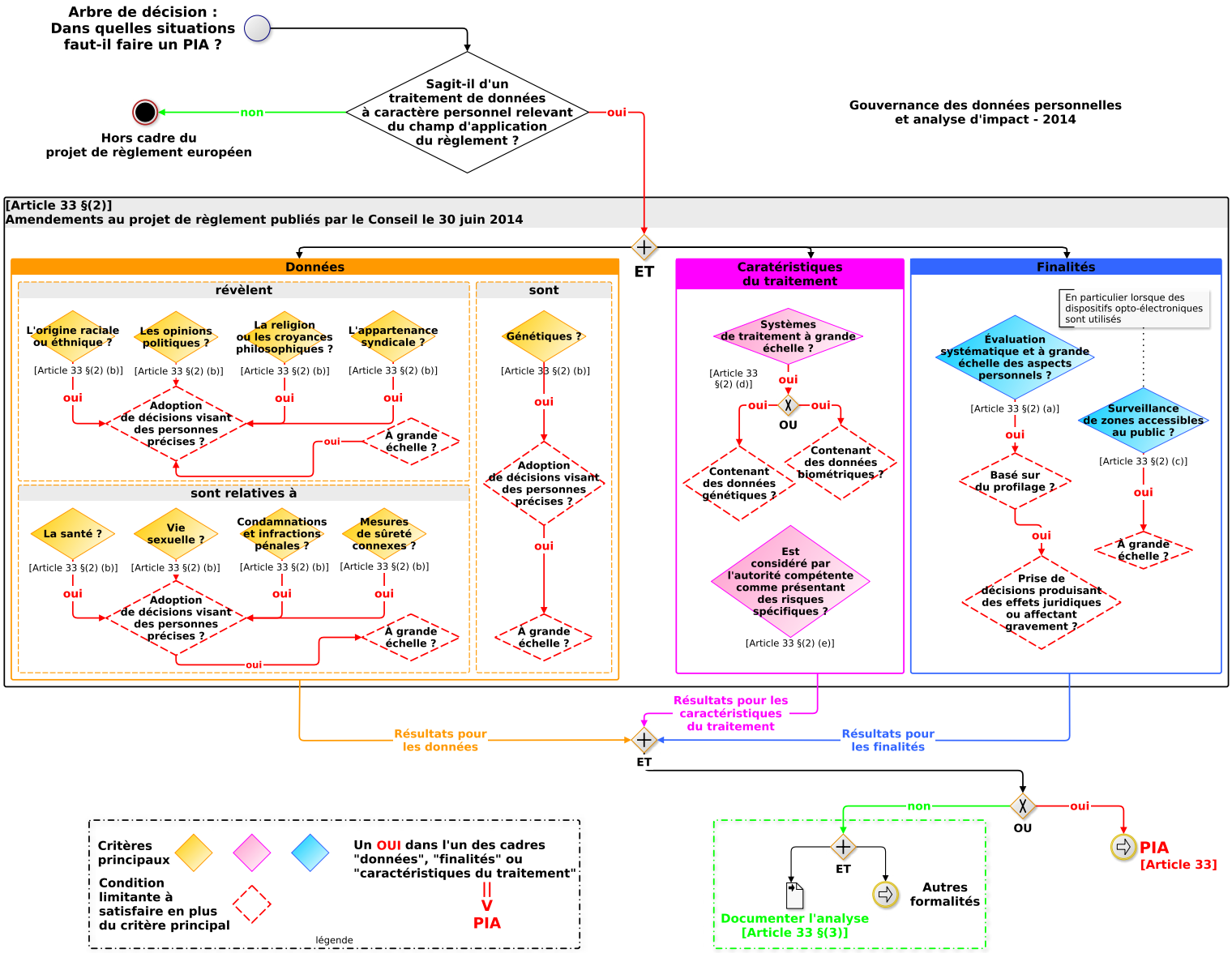
PARTIE II - PÉRIMÈTRE DE L'ANALYSE D'IMPACT

Article 32bis dans sa version votée par le Parlement en mars 2014



PARTIE II - PÉRIMÈTRE DE L'ANALYSE D'IMPACT

Article 33 dans sa version publiée par le Conseil en juin 2014



Une fois le périmètre de l'analyse d'impact déterminé, il convient de définir les grands principes de la conduite d'une telle analyse.

PARTIE III - CONDUITE DE L'ANALYSE D'IMPACT

Après avoir étudié les aspects règlementaires relatifs à la conduite de l'analyse d'impact, décrite par l'article 33 de la proposition de 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 de leurs traitements sur la protection des données à caractère personnel.

1. LES ASPECTS RÈGLEMENTAIRES

1.1 Le déclenchement de l'analyse d'impact

Les participants du groupe de travail se sont interrogés sur le moment auquel l'analyse d'impact devait être effectuée.

1.1.1 Cadre légal

L'article 33 §(1) de la proposition initiale de RGPD publiée par la Commission prévoit que le responsable du traitement ou le sous-traitant agissant pour son compte « effectuent une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel ».

L'utilisation du terme « envisagé » suggère ainsi que l'analyse d'impact doit être conduite avant la mise en œuvre du traitement, voire dès sa phase de conception[49].

La Commission européenne précise également au considérant 70 de la proposition de RGPD que :

> - pour « les traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées, du fait de leur nature, de leur portée ou de leur finalité [...], une analyse d'impact relative à la protection des données devrait être réalisée par le responsable du traitement ou le sous-traitant, préalablement au traitement, et devrait examiner notamment les dispositions, garanties et mécanismes envisagés pour assurer la protection des données à caractère personnel et pour démontrer que le présent règlement est respecté ».

La résolution du Parlement européen, dans son considérant 71 bis, explique par ailleurs que :

> - « les analyses d'impact sont l'essence même de tout cadre viable de protection des données. Elles garantissent que les entreprises soient conscientes dès le départ de toutes les conséquences possibles de leurs traitements ».

[49] Il est intéressant de noter que, si l'Information Commissioner's Office (ICO) au Royaume-Uni a également relevé l'usage du terme « envisagé » à l'article 33 §(1) de la proposition de RGPD, celle-ci retient une autre interprétation du texte. Selon l'autorité britannique de protection des données, en effet, le terme « envisagé » signifierait que l'analyse d'impact ne s'applique qu'aux traitements de données futurs. L'ICO considère toutefois justifié de conduire des analyses d'impact sur des traitements déjà existants présentant des risques importants, dans l'hypothèse où de telles analyses n'auraient pas déjà été effectuées. Article-by-article analysis paper on proposed new EU General Data Protection Regulation, Information Commissioner's Office 12-2-2013, p. 43.

Enfin, le texte du Conseil de l'Union européenne évoque directement dans l'article 33 §(1) la question du moment du déclenchement de l'analyse d'impact. Le Conseil énonce ainsi que :

- « lorsque le traitement, compte tenu de sa nature, de sa portée ou de ses finalités, est susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées, le responsable du traitement effectue, préalablement au traitement, une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel ».

1.1.2 La détermination du moment opportun

Il ressort de l'ensemble des dispositions précitées que l'analyse d'impact 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 l'analyse d'impact doit être effectuée.

L'analyse d'impact doit être menée sur un traitement suffisamment abouti pour que ses caractéristiques principales soient correctement définies.

En outre, il convient de ne pas négliger les ressources nécessaires en temps et en personnel pour réaliser l'analyse d'impact.

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 européen.

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 facilement être modifié, sans engendrer de coût financier ou de lourdeur administrative difficilement surmontable.

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.

Pour s'assurer de l'efficacité de l'analyse d'impact, un organisme devra donc veiller à ce que cette analyse d'impact 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 risques en terme de responsabilité pour l'organisme au regard du règlement européen.

1.1.3 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 79 de la proposition initiale de RGPD de la Commission européenne. Cet article prévoit des sanctions allant du simple avertissement par écrit à une amende pouvant s'élever à 1 000 000 d'euros ou 2 % du chiffre d'affaires annuel mondial d'une entreprise.

Le Parlement européen évoque quant à lui des amendes pouvant atteindre 100 000 000 euros ou au maximum 5 % du chiffre d'affaire annuel mondial d'une entreprise, le montant le plus élevé devant être retenu[50].

Concernant la réalisation d'une analyse d'impact, la Commission européenne et le Conseil de l'Union européenne envisagent la peine maximale pour quiconque, de propos délibéré ou par négligence, « omet d'effectuer » une analyse d'impact relative à la protection des données conformément à l'article 33[51] ou « n'effectue pas » une analyse d'impact en violation de l'article 33[52].

De nombreux éléments doivent être pris en compte dans la détermination du montant de l'amende administrative parmi lesquels notamment[53] :

- le fait que l'infraction a été commise de propos délibéré ou par négligence,
- les mesures et procédures techniques et d'organisation mises en œuvre conformément à l'article 23 (Protection des données dès la conception et protection des données par défaut).

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 : il risque alors une amende maximale,
- 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 d'être conforme au règlement européen : il risque alors la peine prévue pour l'infraction constatée (par exemple : traitement de données sensibles en dehors des cas autorisés).

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.

[50] Résolution législative du Parlement européen du 12-3-2014, art. 79 §(2bis) point c).
[51] Proposition Règl. CE du 25-1-2012 art. 79 §(6) point i).
[52] Note from the President of the Council of the European Union dated 30-6-2014, art. 79a §(3) point i).
[53] Proposition Règl. CE du 25-1-2012 art. 79 §(2) ; Résolution législative du Parlement européen du 12-3-2014, art. 79 §(2quater) ; Note from the President of the Council of the European Union dated 30-6-2014, art. 79 §(2a). La résolution législative du Parlement européen vise également les mesures et procédures techniques et d'organisation mises en oeuvre conformément aux articles 33 (Analyse d'impact relative à la protection des données) et 33 bis (Évaluation de la conformité de la protection des données).

1.2 Une approche continue

La résolution du Parlement européen est riche d'enseignements en ce qui concerne les différentes étapes de l'analyse d'impact. Elle prévoit ainsi une action en trois parties :

- analyse de risque : l'étude d'un traitement débutera par une analyse des risques présentés par ce traitement.

Cette analyse devra être révisée au plus tard après un an, ou immédiatement si la nature, la portée ou les finalités des traitements sont sensiblement modifiées[54].

A l'issue de l'analyse de risque :

- s'il apparaît que le traitement ne nécessite pas une analyse d'impact, alors l'analyse des risques devra être documentée,

- 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 conduite, en compte la gestion de la totalité du cycle de vie des données à caractère personnel, de la collecte à la suppression, en passant par le traitement[55].

Il conviendra de documenter l'analyse d'impact, en prévoyant un calendrier d'examens périodiques de la conformité de la protection des données[56].

Le rapport issu de l'analyse d'impact pourra également être communiqué à l'autorité de contrôle, à sa demande.

- Examen de conformité : deux ans au plus tard après avoir mené l'analyse d'impact, un examen de conformité devra être effectué, afin de vérifier que le traitement des données à caractère personnel est effectué conformément à l'analyse d'impact relative à la protection des données[57].

L'examen de conformité devra être mené périodiquement, au moins tous les deux ans, et immédiatement si un changement intervient dans les risques spécifiques présentés par les traitements.

[54] Résolution législative du Parlement européen du 12-3-2014, art. 32bis §(4).
[55] Résolution législative du Parlement européen du 12-3-2014, art. 33 §(3).
[56] Résolution législative du Parlement européen du 12-3-2014, art. art. 33 ter.
[57] Résolution législative du Parlement européen du 12-3-2014, art. art. 33bis.

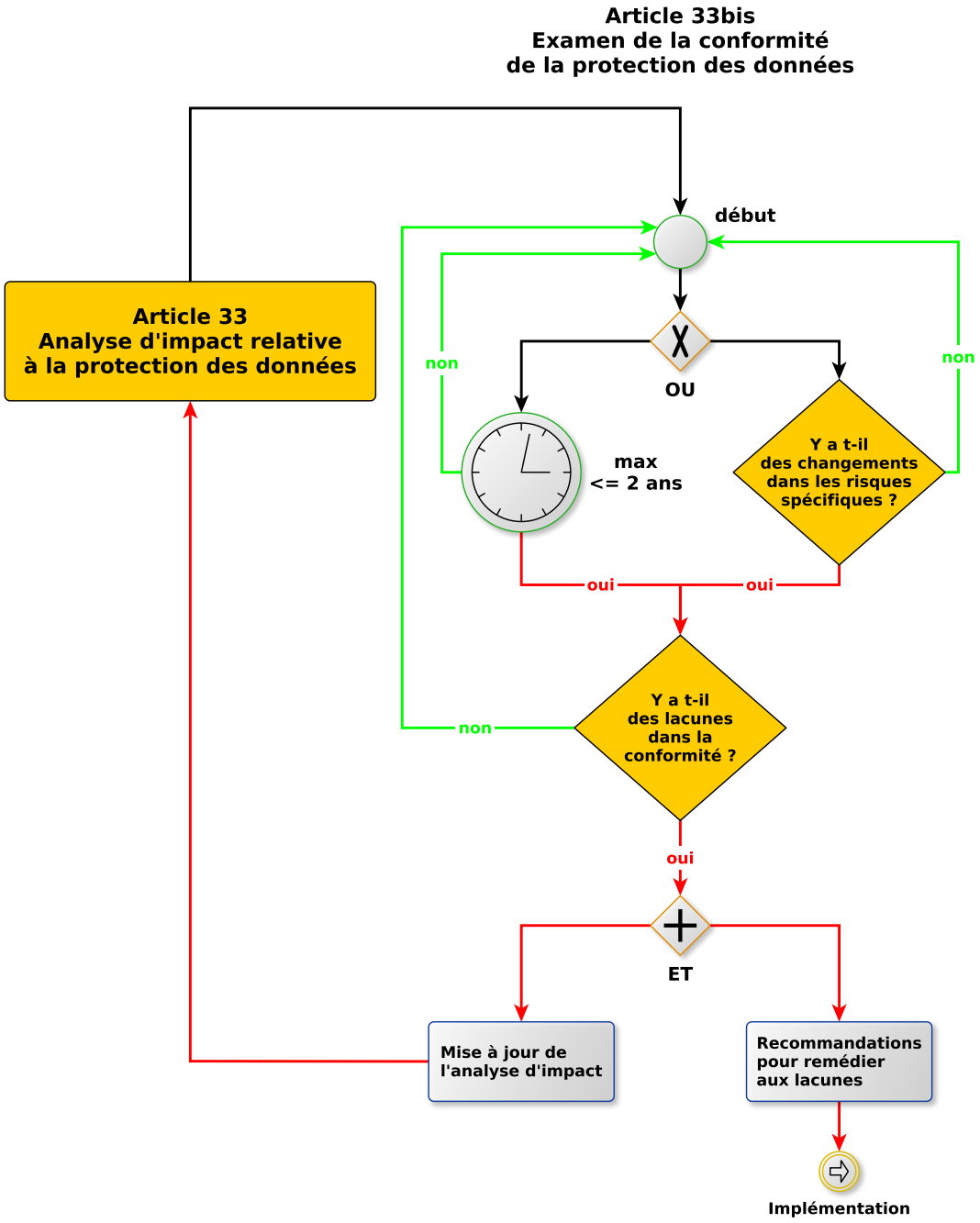
A l'issue de l'examen, si des lacunes sont identifiées :

- des recommandations pour remédier aux lacunes devront être proposées,
- l'analyse d'impact devra être mise à jour sans retard indu.

L'examen de conformité et ses recommandations devront être documentés.

Il pourra également être communiqué à l'autorité de contrôle, à sa demande.

Le fonctionnement des examens de conformités peut être illustré comme suit.


Article 33bis
Examen de la conformité
de la protection des données
Article 33
Analyse d'impact relative
à la protection des données
début
non
OU
non
max
<= 2 ans
Y a t-il
des changements
dans les risques
spécifiques ?
oui
oui
Y a t-il
des lacunes
dans la
conformité ?
non
oui
ET
Mise à jour de
l'analyse d'impact
Recommandations
pour remédier
aux lacunes
Implémentation

Ces différentes étapes permettent ainsi d'assurer que le traitement continuera à être conforme tout au long de son existence. Le Parlement européen, en proposant d'inclure directement dans le texte du RGPD ces étapes, souligne l'importance d'adopter une approche continue de l'analyse d'impact.

Par ailleurs, en insistant sur le fait que l'analyse d'impact doit prendre en compte l'intégralité du cycle de vie des données, et ce depuis leur collecte, le Parlement suggère que l'analyse de risques qui précède l'analyse d'impact devra être elle aussi effectuée en amont du projet de traitement, dès sa phase de conception.

1.3 Le contenu de l'analyse d'impact

L'article 33 §(3) de la proposition de 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 générale des traitements envisagés,
- une évaluation des risques pour les droits et libertés des personnes concernées,
- les mesures envisagées pour faire face aux risques,
- les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité avec le futur règlement, en tenant compte des droits et intérêts légitimes des personnes concernées par les données et des autres personnes touchées.

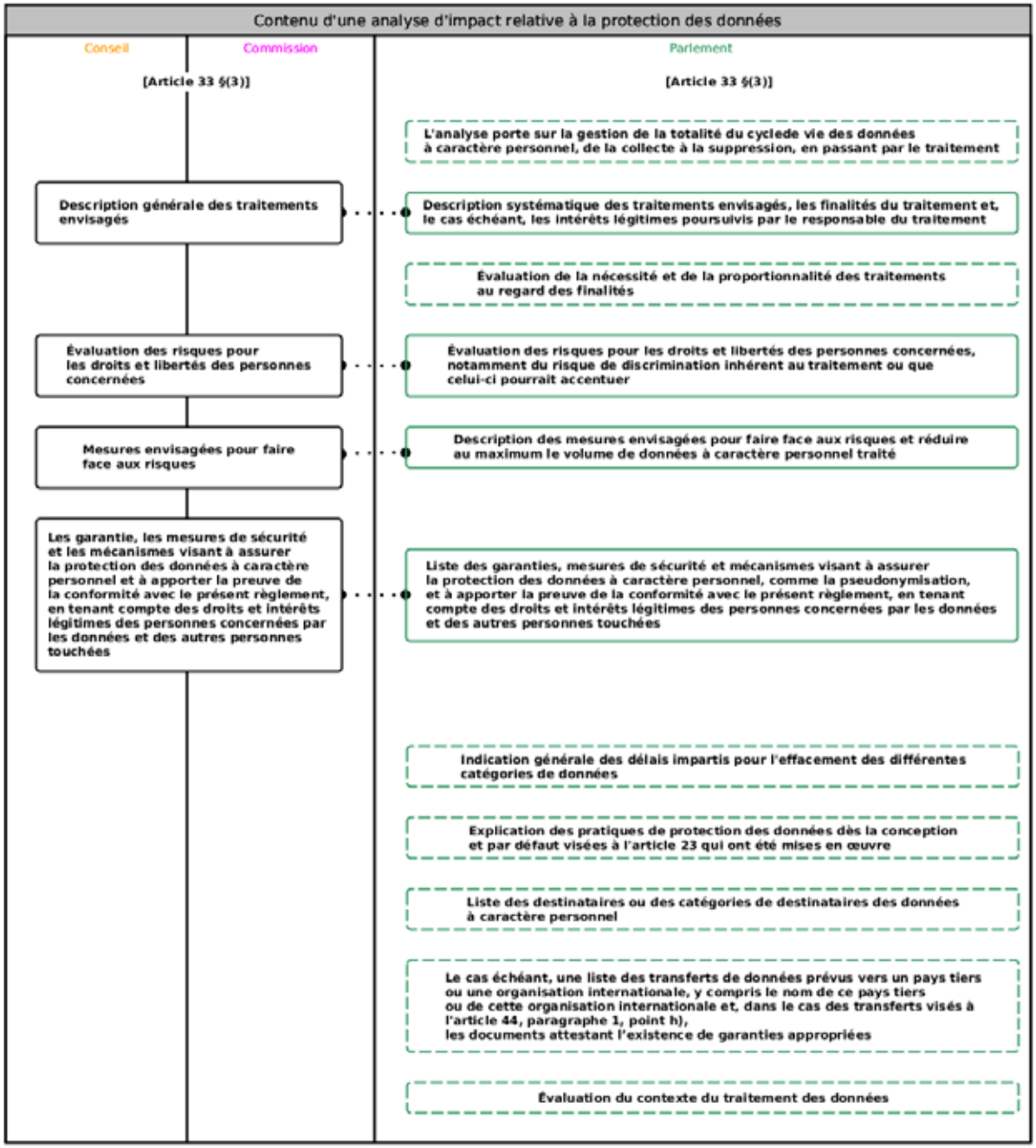
Le Parlement propose d'inclure également dans la liste ci-dessus les informations concernant [58]:

- une description systématique des traitements envisagés, les finalités du traitement et, le cas échéant, les intérêts légitimes poursuivis par le responsable du traitement,
- la nécessité et la proportionnalité des traitements par rapport à leur finalité,
- les mesures envisagées pour réduire au maximum le volume de données à caractère personnel traité,
- les délais impartis pour l'effacement des différentes catégories de données,
- les pratiques de protection des données dès la conception,
- les destinataires ou catégories de destinataires des données à caractère personnel,
- le cas échéant, les transferts de données prévus vers un pays tiers ou une organisation internationale,
- le contexte du traitement de données.

[58] *Résolution législative du Parlement européen du 12-3-2014, art.33§(3).*

PARTIE III - CONDUITE DE L'ANALYSE D'IMPACT

Le schéma qui suit illustre le contenu théorique d'une analyse d'impact en fonction des différents textes.



1.4 Les personnes impliquées dans l'analyse d'impact

1.4.1 Les débiteurs de l'obligation

L'article 33 §(1) de la proposition initiale de RGPD de la Commission fait peser l'obligation de mener une analyse d'impact aussi bien sur les responsables de traitement que sur les sous-traitants agissant pour le compte des responsables de traitement.
L'idée de soumettre également les sous-traitants à cette obligation est rejetée dans la proposition du Conseil, qui précise cependant que[59] :

- « le sous-traitant, sur demande, aide le responsable du traitement à réaliser l'analyse d'impact relative à la protection des données ».

L'article 33 §(5) de la proposition initiale de RGPD suggère par ailleurs que les responsables de traitement, autorité ou organisme publics, pourraient échapper à l'obligation de mener une analyse d'impact, lorsque le traitement est effectué en exécution d'une obligation légale à laquelle cette autorité ou organisme seraient soumis, sauf dans le cas où les États Membres estimeraient qu'une telle analyse serait nécessaire avant le traitement.
Cette proposition fait toutefois l'objet de nombreux débats. Notamment, le Parlement européen rejette cette disposition, proposant de soumettre les autorités ou organisme publics aux mêmes obligations que tout autre responsable de traitement.

De même, le G29 considère que :

- « la dérogation, à l'article 33, paragraphe 5, dispensant les autorités publiques d'effectuer une analyse d'impact n'est pas justifiée, à moins que ladite analyse n'ait déjà été effectuée lors de la procédure législative[60] ».

Il est également intéressant de noter qu'au titre de l'article 33 §(6), la Commission envisage d'adopter des mesures spécifiques pour les micro, petites et moyennes entreprises.

Le G29 s'est 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[61] ».

[59] Note from the President of the Council of the European Union dated 30-6-2014, art. 33 §(1).
[60] Avis 01/2012 sur les propositions de réforme de la protection des données : Groupe « Article 29 » WP 191 du 23-3-2012, p. 18.
[61] 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.

1.4.2 Le délégué à la protection des données

La proposition initiale de RGPD prévoit dans son article 37 que le délégué à la protection doit vérifier que le responsable du traitement ou le sous-traitant a réalisé l'analyse d'impact. La Commission n'a cependant pas jugé utile de préciser le rôle du délégué à la protection des données dans la conduite de l'analyse d'impact, directement dans l'article 33 de la proposition de RGPD.
La proposition issue du Conseil prévoit également que le délégué à la protection des données doit s'assurer de la réalisation de l'analyse d'impact. Mais le délégué se voit en plus assigner un rôle de conseil[62]. Le texte de l'article 33 précise ainsi que lorsqu'un délégué à la protection des données a été désigné, le responsable du traitement doit le « consulter » lors de la réalisation de l'analyse d'impact[63].

Le Parlement va plus loin encore en considérant que le délégué à la protection des données, s'il en existe un, doit être « associé » à la procédure d'analyse d'impact[64].

1.4.3 Les personnes concernées par le traitement

La question de l'implication des personnes concernées dans l'analyse d'impact a également été discutée lors des réunions du groupe de travail.

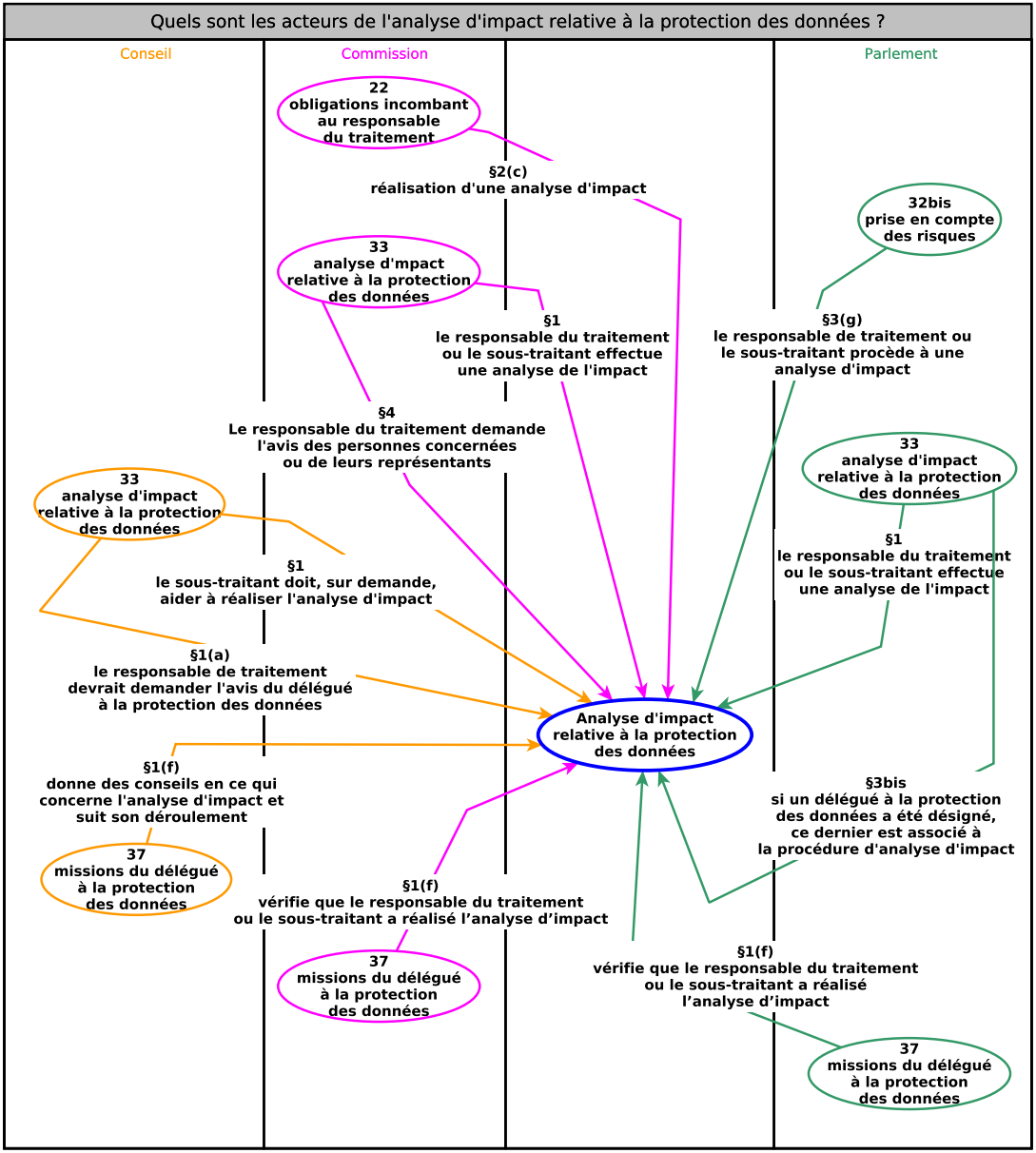
L'article 33 §(4) de la proposition de RGPD prévoit en effet que le responsable du traitement doit demander « l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu ».

Cette obligation de 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 » ou à « la sécurité des traitements ». Cette réserve pourrait permettre aux organismes de limiter le périmètre de la consultation du public, afin que ceux-ci ne soient pas obligés de dévoiler des informations confidentielles sur leurs projets les plus innovants. Cette proposition fait toutefois elle aussi l'objet de désaccords. Le Parlement et le Conseil proposent ainsi de supprimer l'obligation de consultation des personnes concernées[65].
L'ICO souligne quant à elle la nécessité d'obliger les responsables de traitement ou sous-traitants à prendre en compte le point de vue du public, cela plus particulièrement en cas de traitement novateur, mis en œuvre à grande échelle et étant susceptible de porter atteinte à la vie privée. L'autorité britannique relève également que des panels de citoyens ou des groupes de discussion pourraient être organisés avant la mise en place d'une nouvelle base de données ou d'un service du gouvernement[66].

[62] Note from the President of the Council of the European Union dated 30-6-2014, art. 37 §(1) point f).
[63] Note from the President of the Council of the European Union dated 30-6-2014, art. 33 §(1bis).
[64] Résolution législative du Parlement européen du 12-3-2014, art.33 §(3).
[65] Résolution législative du Parlement européen du 12-3-2014, art. 33 ; Note from the President of the Council of the European Union dated 30-6-2014, art. 33.
[66] Article-by-article analysis paper of 12-2-2013, p. 44.

1.4.4 Schéma des acteurs de l'analyse d'impact

Le schéma qui suit tente de représenter le rôle des différents acteurs pouvant être impliqués dans une analyse d'impact, au titre du projet de règlement européen.



1.5 Le rôle de la Commission

Au titre de l'article 33 §(6) de la proposition de RGPD, la Commission pourra préciser davantage les critères et conditions applicables aux traitements susceptibles de présenter des risques particuliers, ainsi que les exigences applicables à l'analyse d'impact, par l'adoption d'« actes délégués ». La Commission pourra plus particulièrement déterminer les conditions de modularité, de vérification et d'auditabilité des analyses d'impact.

L'article 33 §(7) de la proposition de RGPD prévoit en outre que la Commission pourra définir, via des « actes d'exécution », des normes et procédures pour la réalisation, la vérification et l'audit de l'analyse.

Le Parlement et le Conseil proposent de supprimer les dispositions prévues aux articles 33 §(6) et 33 §(7)[67].

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

2. LES ASPECTS MÉTHODOLOGIQUES

2.1 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.

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 risques relatifs à la vie privée et à la protection de données personnelles, des entreprises ont répondu à l'appel lancé par la Commission européenne en proposant une approche d'évaluation de l'impact des dispositifs RFID[68]. Ce cadre, qui a été approuvé par le G29[69], est aussi conforme aux attentes de la Cnil qui en a récemment précisé la méthodologie[70]. 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.

[67] Résolution législative du Parlement européen du 12-3-2014, art. 33 ; Note from the President of the Council of the European Union dated 30-6-2014, art. 33.

[68] 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. Cette proposition faisait suite à la recommandation de la Commission européenne sur la mise en oeuvre 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.

[69] 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.

[70] 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.

Ce qui a donné lieu à la publication de deux guides méthodologiques :

- « Gérer les risques sur les libertés et la vie privée, la méthode - Juin 2012 » qui présente une méthode pour gérer les risques que les traitements de données à caractère personnel peuvent faire peser sur les personnes concernées et qui est lié à un catalogue de bonnes pratiques destinées à traiter les risques appréciés avec cette méthode,

- « Mesures pour traiter les risques sur les libertés et la vie privée - Juin 2012 », qui est un catalogue de bonnes pratiques destinées à traiter les risques que les traitements de données à caractère personnel peuvent faire peser sur les libertés et la vie privée des personnes concernées.

De son côté, l'ICO a publié en février 2014 un code de bonnes pratiques « Conducting privacy impact assessment – code of practice » qui remplace son « Handbook » sur le PIA publié en 2009. Il faut noter que dans le cadre du Data Protection Act – l'équivalent de la loi Informatique et libertés française – le PIA n'est pas obligatoire, ni pour le secteur public ni pour le secteur privé. Cependant, à la suite d'importantes violations de données, le gouvernement britannique a décidé de rendre le PIA obligatoire pour l'ensemble de l'administration publique[71].

Enfin, dans le cadre du projet PIAF (Privacy Impact Assessment Framework), des recommandations sur la conduite de l'analyse d'impact visée à l'article 33 de la proposition de règlement général sur la protection des données ont été formulées à l'attention de la Commission européenne en novembre 2012[72].

S'agissant d'apporter une réponse pragmatique à l'obligation liée à l'article 33 de la proposition de RGPD, la démarche développée ci-après est fondée sur les approches ou bonnes pratiques préconisées par la Commission européenne et les recommandations Cnil.

2.2 Objectifs et principes clés de l'analyse d'impact

Comme cela a déjà été indiqué, l'analyse d'impact relative à la protection des donnée est très liée à la mise en œuvre du principe de prise en compte des risques d'atteinte à la vie privée dès la conception d'une application ou d'un traitement de données (« privacy by design » en anglais) introduit par l'article 23 de la proposition de RGPD.

Son objectif est de s'assurer que les risques liés à la vie privée sont minimisés tout au long du traitement des données. Il s'agit dans ce cadre de permettre une identification des risques le plus tôt possible en analysant dès la phase de conception les modalités d'utilisation des données personnelles et les finalités des traitements et en identifiant quelles mesures sont prises pour prévenir et pour limiter de manière proportionnée les impacts sur le vie privée.

[71] Report from the Cabinet office of the United Kingdom's Government dated 6-2008 regarding Data Handling Procedures in Government.
[72] Recommendations for a privacy impact assessment framework for the European Union, PIAF 11-2012.

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

- de mettre en évidence les risques liés aux traitements de données à caractère personnel,
- d'évaluer leur probabilité d'occurrence,
- de documenter les modalités et démarches de réduction de ces risques,
- in fine, de décider d'accepter les risques résiduels.

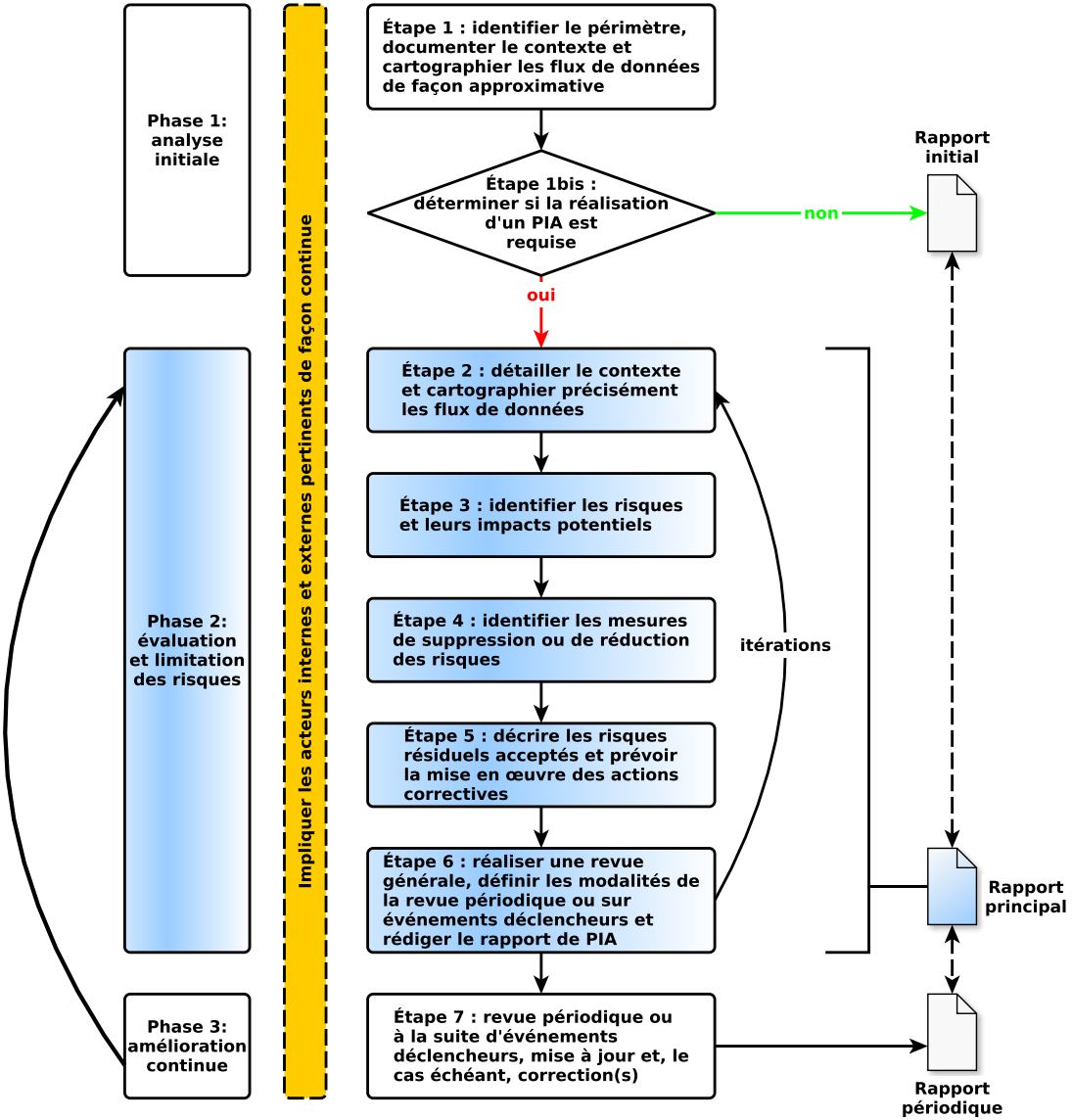
Quels avantages et bénéfices pour les organisations ?

- une visibilité sur la conformité règlementaire 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 PIA très tôt dès la conception des traitements,
- une maturité plus forte dans la gouvernance des risques.

PARTIE IV - DESCRIPTION D'UNE MÉTHODOLOGIE D'ANALYSE D'IMPACT

1. PRÉSENTATION

Le schéma qui suit décrit les étapes « idéales » d'une analyse d'impact, telles qu'elles ont pu être discutées dans le cadre du groupe de travail. Ces étapes s'appuient principalement sur des éléments décrits dans la version initiale de la proposition de RGPD ainsi que dans celle du Parlement.



PARTIE IV - DESCRIPTION D'UNE MÉTHODOLOGIE D'ANALYSE D'IMPACT

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

1. Phase initiale :
   - elle décrit « à grands traits » le contexte et le périmètre de l'application et propose une première cartographie des flux de données,
   - sur la base de ces informations, elle détermine le besoin de réaliser ou non une analyse d'impact et se conclut par la rédaction d'un rapport initial.

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 flux de données,
   - elle identifie les menaces sur la vie privée, évalue leur probabilité d'occurence et la gravité des événements redoutés,
   - elle documente les mesures possibles pour supprimer ou réduire les risques,
   - 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 de PIA.

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 personnelles.

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.

2. DESCRIPTION DÉTAILLÉE

La suite de ce chapitre détaille les différentes étapes.

2.1 Impliquer et consulter les acteurs internes et externes pertinents de manière continue

Dans l'idéal, l'analyse d'impact ne devrait pas être un exercice solitaire. Au contraire, 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, il est cependant intéressant de remarquer que le Parlement et le Conseil proposent de supprimer de l'article 33 l'obligation de consultation des personnes concernées[73].

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 informatique qui sera en charge d'héberger le traitement, de le maintenir,
- 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,
- le service juridique,
- les services en charge de la gestion des risques en général et informatiques en particulier,
- la direction qui devra faire les nécessaires arbitrages.
- etc.

Comme évoqué plus haut, le rôle du délégué à la protection des données dans la conduite de l'analyse d'impact n'a pas encore été arrêté. Celui-ci pourra être plus ou moins impliqué dans le processus d'analyse d'impact.

[73] Résolution législative du Parlement européen du 12-3-2014, art. 33 ; Note from the President of the Council of the European Union dated 30-6-2014, art. 33.

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.

2.2 Identifier le périmètre, documenter le contexte et cartographier les flux de données de façon approximative

Cette étape est la première de la « phase d'analyse 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 1bis » qui suit, si ce traitement doit ou non faire l'objet d'un PIA. 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 :

Entité juridique (Organisme) Responsable (coordonnées du contact)	
Personne ou entité chargée de la mise en oeuvre du traitement	Responsable, service ou prestataire extérieur manipulant les données
Nom du traitement (de l'application)	
Finalités du traitement	Objectifs et finalités
Formalités (à accomplir ou accomplies)	Par exemple normes simplifiées, etc.
Catégories de données traitées	Liste des données à caractère personnel traitées
Données sensibles	Par exemple données de santé
Zone de libre commentaire (ZLC)	Oui/Non
Encadrement ZLC	Audit de l'application, charte, sensibilisation des utilisateurs
Personnes concernées	Toutes les catégories de personnes dont les données sont traitées : salariés, clients, utilisateurs, etc.
Type de collecte	Directe/indirecte
Information des personnes concernées	Modalités prévues ou existantes
Durées de conservation	Politique pour les durées de conservation
Destinataires des données	Internes et/ou externes
Interconnexion	Lien avec d'autres fichiers de données à caractère personnel dont les finalités sont différentes
Flux transfrontières (FT)	Oui/Non, pays concernés
Encadrement des FT	Modalités
Sécurité	Mesures en place ou à prévoir
Droits des personnes	Processus de gestion des demandes d'accès, d'interrogation, de rectification ou d'opposition

Le travail ainsi réalisé sera directement utile au Cil ou 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 ».

PARTIE IV - DESCRIPTION D'UNE MÉTHODOLOGIE D'ANALYSE D'IMPACT

Le cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données, rédigé par des entreprises du secteur puis approuvé par le G29[74], fournit un exemple de formalisation pour les applications qui utilisent des technologies RFID. Il précise que « l'exploitant d'application RFID doit intégrer, le cas échéant, les informations ci-dessous au rapport [d'Etude d'Impact sur la Vie Privée] »[75] :

- Exploitant d'application RFID
    - Nom et localisation de l'entité juridique
    - Personne ou bureau responsable du respect du calendrier d'EIVP
    - Point(s) de contact et marche à suivre pour poser des questions à l'exploitant
- Présentation générale de l'application RFID
    - Nom de l'application RFID
    - Objectif(s) de la/des application(s) RFID
    - Scénarios d'utilisation de base de l'application RFID
    - Composants de l'application RFID et technologies utilisées (c'est-à-dire fréquences, etc.) • Portée géographique de l'application RFID
    - Types d'utilisateurs/de personnes sur lesquels l'application RFID a une incidence
    - Accès individuel et contrôle
- Numéro du rapport d'EIVP
    - Numéro de version du rapport d'EIVP (permettant de reconnaître une nouvelle EIVP ou de simples modifications mineures)
    - Date de la dernière modification apportée au rapport d'EIVP
- Traitement des données RFID
    - Liste des types de données traitées
    - Présence d'informations sensibles dans les données traitées (par ex. concernant la santé)
- Stockage des données RFID
    - Liste des types de données stockées • Durée du stockage
- Transfert interne de données RFID (le cas échéant)
    - Description ou diagrammes portant sur les flux de données dans le cadre des opérations internes concernant des données RFID
    - Objectif(s) d'un transfert des données à caractère personnel
- Transfert externe de données RFID (le cas échéant)
    - Type de destinataire(s) des données
    - Objectif(s) du transfert ou de l'accès en général
    - Données à caractère personnel identifiées et/ou identifiables concernées par le transfert (ou niveau de ces données)
    - Transferts en dehors de l'Espace économique européen (EEE)

[74] 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.

[75] 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, p. 13.

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

2.3 Déterminer si la réalisation d'un PIA est requise

Cette étape « 1bis » clôt la « phase d'analyse initiale ». Pour faciliter la prise de décision, le groupe de travail a élaboré des « arbres de décision » sur la base des différentes versions de l'article 33, entre la proposition initiale de RGPD et ses versions amendées par le Parlement et le Conseil.

Ces arbres de décision ont été présentés au Chapitre 2.3 du présent livre blanc. Un mode d'emploi est proposé en annexe 2 tandis que les études de cas du Chapitre 5 fournissent des exemples complets d'utilisation.

Dans une perspective de traçabilité et « d'accountability », l'ensemble de cette première phase pourra être formalisée dans un rapport de PIA initial regroupant les informations du tableau proposé au Chapitre 4.2.2, la cartographie des flux et les résultats significatifs obtenus en parcourant les arbres de décision. Si la réalisation d'un PIA est requise, alors se rapport initial pourra constituer la première partie du rapport principal attendu à la fin 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.

2.4 Détailler le contexte et cartographier précisément 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,
- objectifs 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 personnelles directes et déduites,
- personnes ayant accès aux données,
- etc.

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.

De même, afin de faciliter le déroulement du process 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.

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[76] (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 personnelles 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

[76] La maîtrise du cycle de vie des données personnelles 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 données.

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[77] 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 ?

Si les réponses sont affirmatives, un cadre de confiance s'applique naturellement à la maîtrise des données personnelles. Dans le cas contraire, une démarche de mise en place de ces processus de gestion documentaires et d'archivage devrait être entreprise en parallèle ou suite de l'analyse d'impact.

2.5 Identifier les risques et leurs impacts potentiels

Dans le cadre de cette deuxième 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 personnelles 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 personnelles, il existe des risques sur la vie privée.

[77] 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 oeuvre 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 responsabilité, quel impact, quelles contraintes réglementaires, etc.

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 intéressant de noter que, bien que l'article 33 de la proposition de RGPD mentionne la conduite d'une analyse d'impact relative à la protection des données, cet article précise au §(3) qu'il convient d'évaluer plus largement les risques « pour les droits et libertés des personnes concernées » et de prendre en compte les « droits et intérêts légitimes des personnes concernées par les données et des autres personnes touchées ». La résolution du Parlement fait ainsi référence à l'« impact des traitements envisagés sur les droits et les libertés des personnes concernées, en particulier leur droit à la protection des données à caractère personnel »[78].

Dans le cadre de la conduite d'une analyse d'impact, il convient donc d'identifier de manière systématique tous les risques susceptibles d'affecter le respect de la vie privée. Et en cas d'application transfrontalière, 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.

[78] *Résolution législative du Parlement européen du 12-3-2014, art. 33 §(1).*

2.5.1 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) ».

À ce stade, il est important de bien distinguer « analyse de risques » et « analyse d'impact ». L'analyse de risques est une méthodologie complète qui consiste à identifier la nature des risques puis à les « mesurer ». L'analyse d'impact, quant à elle, est un exercice complémentaire à l'analyse de risques mais qui consiste à simuler un risque (destruction, altération d'une donnée à caractère personnel) pour en mesurer les différents « impacts » sur l'activité et les personnes concernées. Assimiler « analyse de risques » et « analyse d'impact », c'est faire l'hypothèse implicite que les risques considérés dans l'analyse d'impact sont « avérés » ; c'est-à-dire que leur probabilité d'occurrence est égale à 1, ce qui n'est jamais le cas sauf quand le risque s'est réalisé ! Ainsi, l'analyse d'impact a toute son importance pour identifier les risques dont les impacts sont les plus critiques. En revanche, elle ne permet pas de « déterminer » la nature des protections requises. C'est là le rôle de l'analyse de risques.

La gravité des évènements redoutés (l'impact) est appréciée au regard du caractère identifiant des données personnelles (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 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 »[79].

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

[79] *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, p. 10.*

2.5.2 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.).

2.5.3 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'expert 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 contentieux souvent gérée par les départements juridiques permet aussi d'identifier l'occurrence (par exemple, nombre 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 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.

2.6 Identifier les mesures de suppression ou de réduction des risques

Cette troisième 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 fournit 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[80] ? le degré de maturité acquis par l'organisation est-il de nature à limiter les risques ? etc.). Les mesures proposées sont principalement des dispositifs de prévention et de détection d'incidents.

[80] *Confidentialité, intégrité, disponibilité, conformité, fiabilité.*

À titre d'exemple, la Cnil a listé des bonnes pratiques et des mesures visant à traiter des risques sur les libertés et la vie privée dont le tableau de synthèse est repris ci-dessous[81].

MESURES	PRINCIPAUX CHAPITRES CORRESPONDANTS DANS L'[ISO-27002]
1. Minimiser les DCP	15. Conformité
2. Gérer les durées de conservation des DCP	15. Conformité
3. Informer les personnes concernées	15. Conformité
4. Obtenir le consentement des personnes concernées	15. Conformité
5. Permettre l'exercice du droit d'opposition	15. Conformité
6. Permettre l'exercice du droit d'accès direct	15. Conformité
7. Permettre l'exercice du droit de rectification	15. Conformité
8. Cloisonner les DCP	10 Gestion de l'exploitation et des télécommunications
9. Chiffrer les DCP	10 Gestion de l'exploitation et des télécommunications
10. Anonymiser les DCP	15. Conformité
11. Sauvegarder les DCP	10. Gestion de l'exploitation et des télécommunications
12. Protéger les archives de DCP	10. Gestion de l'exploitation et des télécommunications
13. Contrôler l'intégrité des DCP	10. Gestion de l'exploitation et des télécommunications
14. Tracer l'activité sur le système informatique	10. Gestion de l'exploitation et des télécommunications
15. Gérer les violations de DCP	13. Gestion des incidents liés à la sécurité de l'information 14. Gestion du plan de continuité de l'activité
16. S'éloigner des sources de risques	9. Sécurité physique et environnementale
17. Marquer les documents contenant des DCP	7. Gestion des biens
18. Gérer les personnes internes qui ont un accès légitime	6. Organisation de la sécurité de l'information 8. Sécurité liée aux ressources humaines
19. Contrôler l'accès logique des personnes	11. Contrôle d'accès
20. Gérer les tiers qui ont un accès légitime aux DCP	6. Organisation de la sécurité de l'information
21. Lutter contre les codes malveillants	10. Gestion de l'exploitation et des télécommunications
22. Contrôler l'accès physique des personnes	9. Sécurité physique et environnementale
23. Se protéger contre les sources de risques non humaines	9. Sécurité physique et environnementale
24. Réduire les vulnérabilités des logiciels	10. Gestion de l'exploitation et des télécommunications 11. Contrôle d'accès 12. Acquisition, développement et maintenance des systèmes d'information
25. Réduire les vulnérabilités des matériels	7. Gestion des biens 9. Sécurité physique et environnementale 10. Gestion de l'exploitation et des télécommunications 11. Contrôle d'accès
26. Réduire les vulnérabilités des canaux informatiques	10. Gestion de l'exploitation et des télécommunications 11. Contrôle d'accès
27. Réduire les vulnérabilités des personnes	8. Sécurité liée aux ressources humaines
28. Réduire les vulnérabilités des documents papier	7. Gestion des biens
29. Réduire les vulnérabilités des canaux papier	7. Gestion des biens

30. Gérer l'organisation de protection de la vie privée	6. Organisation de la sécurité de l'information
31. Gérer les risques sur la vie privée	6. Organisation de la sécurité de l'information
32. Gérer la politique de protection de la vie privée	5. Politique de sécurité
33. Intégrer la protection de la vie privée dans les projets	12. Acquisition, développement et maintenance des systèmes d'information
34. Superviser la protection de la vie privée	15. Conformité

[81] *Guide mesures pour traiter les risques sur les libertés et la vie privée Cnil 6-2012, p. 84.*

Pour finir, les mesures identifiées doivent être introduites dans l'analyse pour ré-évaluer 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.

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.

2.8 Réaliser une revue générale, définir les modalités de la revue périodique ou sur événements déclencheurs et rédiger le rapport de PIA

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.

PARTIE IV - DESCRIPTION D'UNE MÉTHODOLOGIE D'ANALYSE D'IMPACT

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 pré-déterminés, 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 de PIA 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,
- 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.

Le rapport de PIA principal 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. 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.

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 la méthode de PIA « idéal » 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 de PIA précédent et d'identifier les variations et leurs éventuelles conséquences.

En l'absence de tout changement, le rapport de PIA 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 de PIA 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 de PIA 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.

PARTIE V - ETUDE DE CAS

1. CAS N° 1 « ASSOCIATION VISANT À RÉALISER UNE ACTIVITÉ DE LOISIR EXCEPTIONNELLE AU BÉNÉFICE DE PERSONNES ATTEINTES PAR UNE MALADIE GRAVE »

Il s'agit du cas fictif d'une association française à but non lucratif proposant des activités de loisir exceptionnelles, encadrées par des bénévoles, à des personnes, y compris des enfants, atteintes par une maladie grave. Cette association fait partie d'un réseau international d'associations d'aide aux familles touchées par la maladie qui sont fédérées par une association « mère » dont le siège se trouve en Australie. Les activités de loisir exceptionnelles proposées peuvent être pratiquées individuellement ou en famille lorsque le bénéficiaire est un enfant.

Pour l'organisation de ses activités et la gestion de son fonctionnement interne, l'association française utilise un logiciel de type « Customer Relationship Management » (CRM) fournit en mode « Software as a Service » (SaaS) par l'association mère australienne qui bénéficie d'un don d'un partenaire industriel. Cette application permet ainsi de gérer les demandes des bénéficiaires des activités et de suivre leur mise en œuvre. Les données traitées par le CRM concernent notamment l'identification des demandeurs d'activités, la famille des demandeurs lorsqu'il s'agit d'enfants, le type d'activité, l'identification des intervenants autres que le ou les bénéficiaires (bénévoles y compris des professionnels de santé, sponsors pour les dons affectés à la réalisation d'une activité spécifique, etc.), la gestion des collectes de fonds, la gestion du fonctionnement de l'association.

La présente étude de cas se focalise sur le traitement dont la finalité est d'identifier précisément le bénéficiaire d'une activité de loisir – ainsi que sa famille lorsqu'il s'agit d'un enfant –, la dite activité et le suivi de sa mise en œuvre avec l'équipe de bénévoles qui y est affectée. Dans cette perspective, un premier tableau décrit le contexte du traitement et en propose une cartographie avec une représentation des flux de données. Ensuite, les schémas correspondants aux trois versions de l'article 33 étudié dans ce livre blanc sont parcourus pour déterminer si cette application doit, ou non, faire l'objet d'un PIA. Enfin, une brève analyse d'impact et des recommandations sont formulées en fonction des résultats obtenus.

1.1 Analyse du contexte et cartographie des traitements mis en œuvre dans le cas n°1

Le tableau ci-dessous présente la cartographie des traitements mis en œuvre par l'association.

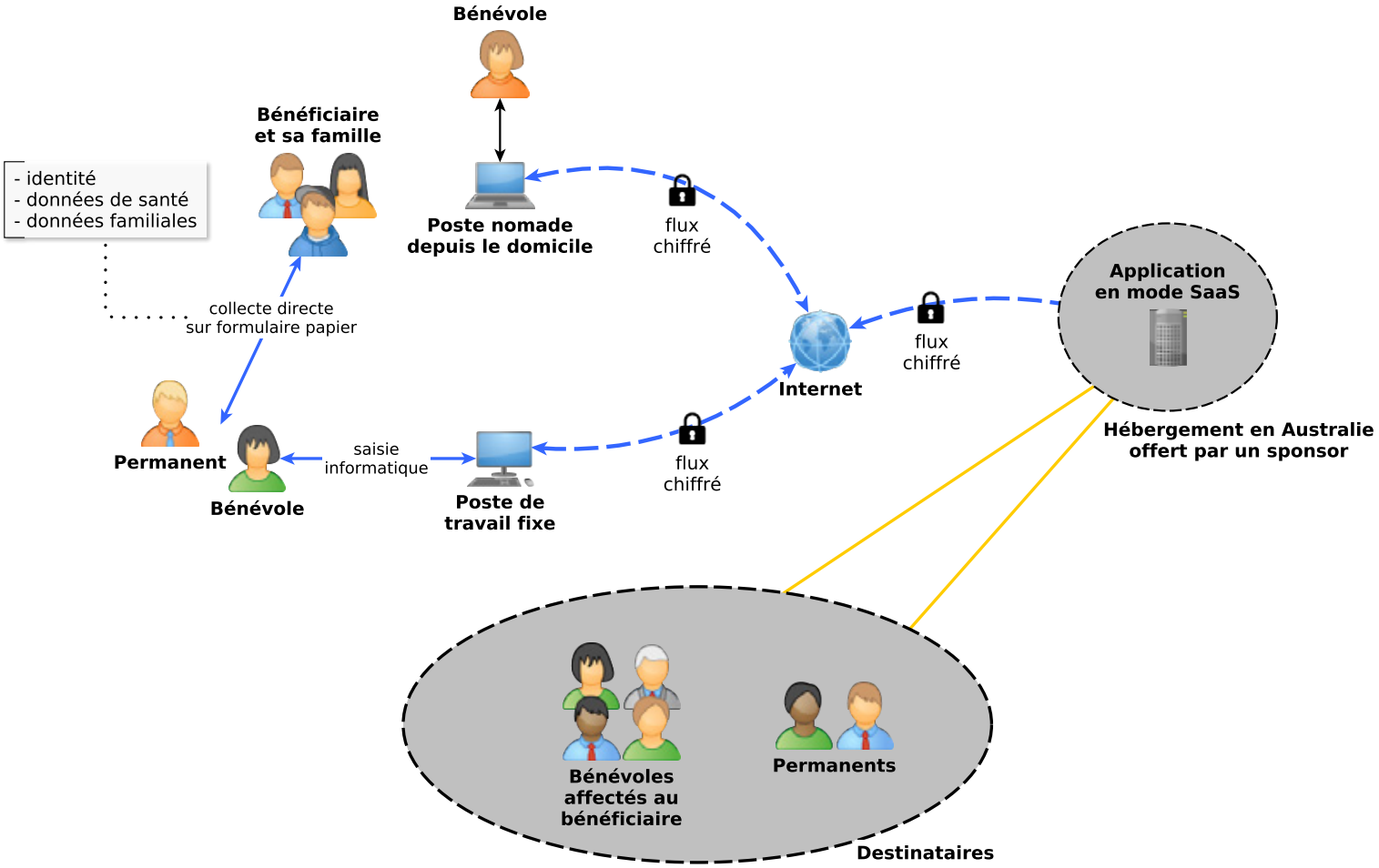
Nom de l'application	**CRM**
Finalité du traitement	Gestion des demandes d'activités de loisir exceptionnelles de personnes malades adultes ou mineures.
Formalités	Le traitement n'a fait l'objet d'aucune formalité auprès de la Cnil. La désignation d'un Correspondant Informatique et Libertés (Cil) est envisagée.

Catégories de données traitées	- état civil et autres données d'identification ; - vie personnelle (composition de la famille) ; - vie professionnelle (le cas échéant) ; - santé : précautions et équipements ; - préférences diverses : régime alimentaire, etc. - date de décès du malade (le cas échéant) ; - identités des bénévoles affectés à chaque projet ; - données financières relatives à chaque projet ; - photos et vidéos relatives à la réalisation de l'activité de loisir exceptionnelle.
Données sensibles	- données de santé relatives aux malades (diagnostic, médecin, service traitant, hôpital, etc.). - données relatives au régime alimentaire du demandeur pouvant faire éventuellement apparaître ses croyances religieuses. - données relatives à la famille pouvant faire apparaître sa structure et, éventuellement, révéler des orientations sexuelles.
Personnes concernées par la collecte	Demandeur de l'activité et sa famille dans le cas de mineurs. Bénévoles affectés à la réalisation des activités de loisir exceptionnelles. Tiers impliqués dans les activités de loisirs exceptionnelles.
Type de collecte	Les données sont directement collectées auprès de la ou des personnes concernées lorsque c'est possible. Les données relatives à l'état de santé du malade ou au service traitant, peuvent être collectées par le biais du médecin traitant après autorisation du malade ou de la famille.

Information des personnes concernées	Les personnes concernées sont informées du traitement mis en œuvre par l'association au moment de la collecte. Il en est de même pour les droits d'accès et de rectification. Un consentement est aussi demandé pour la transmission ou le recueil des données de santé nécessaires à la réalisation de l'activité lorsqu'il y a nécessité de s'adresser à l'équipe soignante du bénéficiaire.
Durées de conservation	Le système ne permet pas de définir des durées de conservation et l'association ne dispose d'aucune procédure à cet effet.
Destinataires	- deux administrateurs de l'association (accès à l'intégralité des données, avec pouvoir de modification). - les permanents de l'association (accès à l'intégralité des données, avec pouvoir de modification). - certains bénévoles avec des fonctions administratives (accès à l'intégralité des données, avec pouvoir de modification). - les bénévoles en charge de l'organisation des activités (accès aux informations suivantes, uniquement en consultation : nom du malade et des membres de la famille, nature de la demande). - les bénévoles travaillant sur la collecte des dons affectés à un bénéficiaire particulier (accès aux informations suivantes, uniquement en consultation : nom du malade et nature de sa demande).
Droits des personnes	L'association ne dispose d'aucune procédure écrite pour la gestion des demandes de droit d'accès, de rectification ou d'opposition.

Sécurité	- les locaux de l'association sont privatifs et équipés d'un dispositif de contrôle d'accès par badges réservés à certains bénévoles et au personnel permanent. - l'accès aux postes de travail situés dans les locaux de l'association nécessite un identifiant et un mot de passe. - l'accès à l'application CRM se fait grâce à un identifiant et un mot de passe. Les utilisateurs bénévoles, qui ne sont pas autorisés à faire des modifications, disposent d'un identifiant qui n'est pas nominatif. - l'accès aux données est restreint sur la base de profils pré-définis. - les accès à l'application et toutes les actions effectuées sur les données sont enregistrées dans le journal de l'application. - l'accès à l'application s'effectue via Internet, en utilisant un protocole sécurisé de type HTTPS. - les bénévoles concernés par l'utilisation du CRM signent un engagement de confidentialité. - l'association n'a pas de charte informatique.
Zones de libre commentaire (ZLC)	Le système dispose de ZLC pour recueillir des informations utiles pour la réalisation de l'activité en fonction de la maladie du demandeur. Il peut y être précisé, par exemple, les contraintes de mobilité ou les régimes alimentaires spécifiques.
Encadrement de l'utilisation des ZLC	Aucun.
Interconnexion de fichiers	Aucun.
Flux transfrontière (FT)	Oui. L'application est utilisée en mode SaaS et est hébergée sur des serveurs situés en Australie.
Encadrement des FT	Aucun.
Divers	L'application CRM est mise à disposition par un sponsor industriel qui assure également son hébergement et sa maintenance. La convention de don est le seul élément contractuel qui lie l'association au sponsor/hébergeur.

Un schéma simplifié des flux de données complète le tableau précédent. Les flèches en bleu représentent les flux de données. Les flèches en orange indiquent des destinataires.

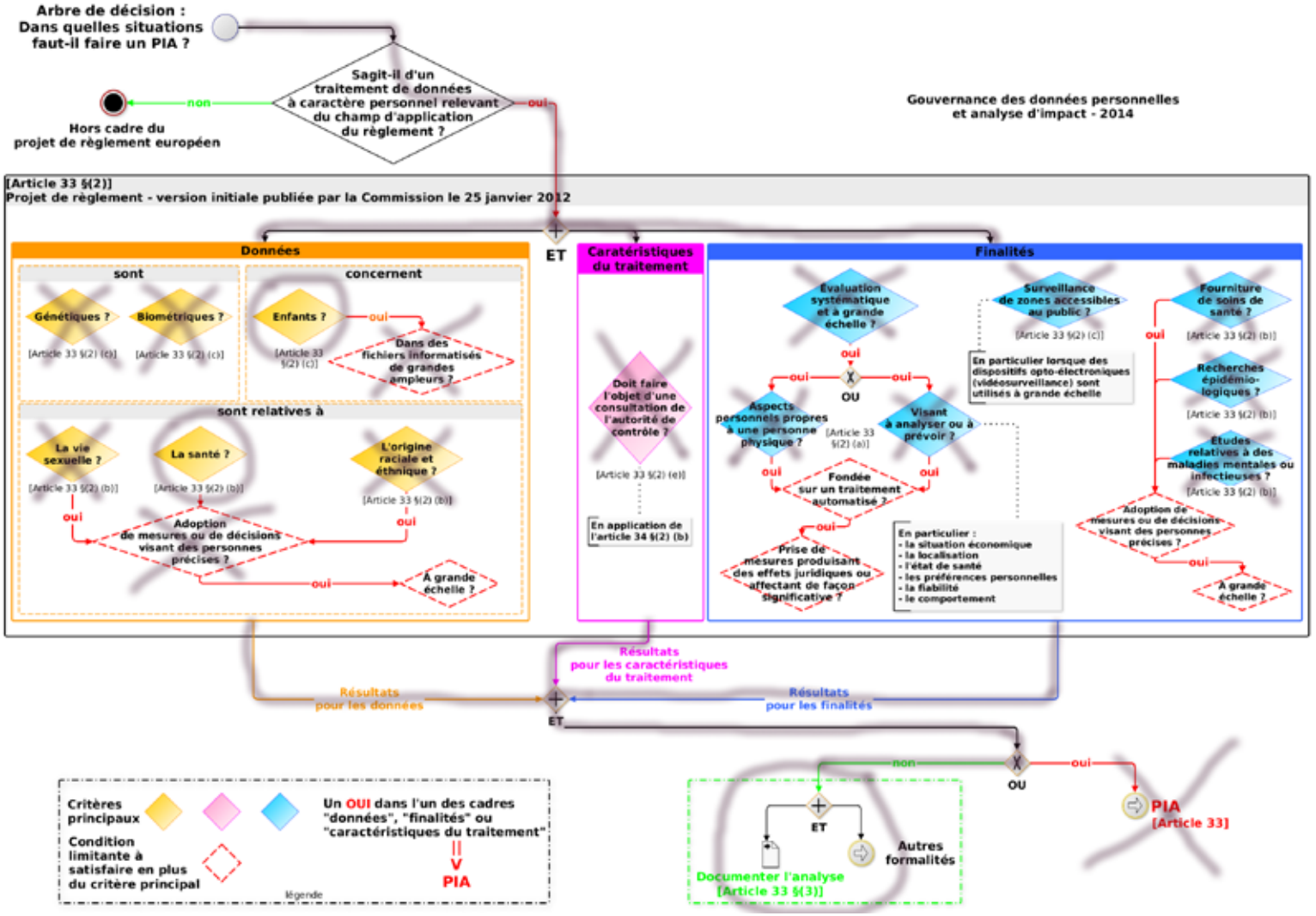


1.2 Analyse des arbres de décision concernant le cas n°1

En suivant la méthode présentée en Annexe 2, les schémas correspondants aux trois versions de l'article 33 étudié dans ce livre blanc ont été utilisés pour identifier les situations pouvant conduire à la réalisation d'un PIA.

Article 33 dans sa version initiale proposée par la Commission

Le schéma qui résulte de l'analyse est présenté ci-dessous.

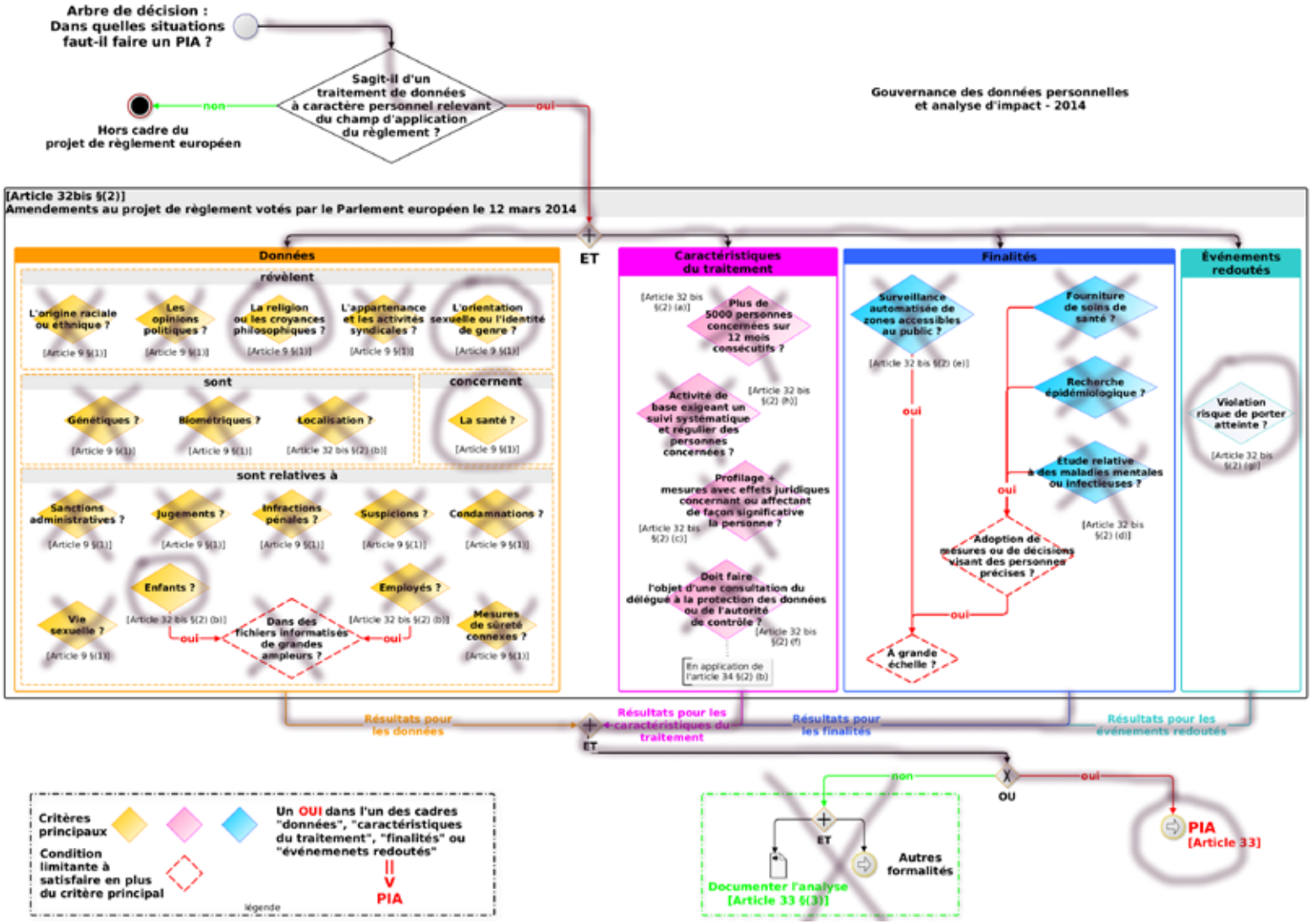


Comme on peut le constater, il ne conduit pas à la réalisation d'un PIA. Deux « critères principaux » ont été entourés mais ils ont ensuite été invalidés pas les « conditions limitantes » qui les suivent.

Critère principal / condition limitante	Explications
Données	
1 – Les données concernent-elles des enfants ?	**Oui.** L'association peut organiser des activités de loisirs pour des adultes comme des mineurs. L'application CRM peut donc contenir des données qui « concernent » explicitement des enfants.
1.1 – Ces données sont-elles contenues dans des fichiers informatisés de grande ampleur ?	**Non.** Même si comme cela a déjà été évoqué, la notion de « grande ampleur » reste floue, il a été considéré que la centaine de noms contenus dans le fichier de l'association ne constituait pas un fichier de grande ampleur.
2 – Les données sont-elles relatives à la santé ?	**Oui.** L'objectif de l'association est de permettre à des personnes malades de participer à une activité de loisir. Les données traitées par l'application concernent donc, en partie, l'état de santé de ces personnes afin de pouvoir les accueillir en tenant compte de leur situation individuelle.
2.1 – Ces données sont-elles traitées afin d'adopter des mesures ou des décisions qui visent des personnes précises ?	**Non.** Les données de santé de chaque malade ne sont pas utilisées en vue de prendre des décisions ou des mesures de portée large et qui visent des personnes précises mais uniquement à prendre en compte la particularité de chacun pour la réalisation de l'activité de loisir exceptionnelle. En effet, cette condition limitante est associée à la condition de « grande échelle ». Elle semble ainsi viser les processus de décision ou d'adoption de mesures à partir d'informations relatives à la santé des personnes, ayant une portée large et visant des individus déterminés. Elle pourrait faire référence notamment à l'adoption de politiques publiques dans le domaine de la santé, ce qui n'est manifestement pas le cas de l'association. En conséquence, cette « condition limitante » ne peut pas être considérée comme satisfaite.

Article 32bis dans sa version votée par le Parlement en mars 2014

Le schéma qui résulte de l'analyse est présenté ci-dessous.



PARTIE V - ETUDE DE CAS

Comme il a déjà été indiqué, l'article 32bis, qui résulte des amendements votés par le Parlement en mars 2014, contient beaucoup plus de critères propres à déclencher la réalisation d'un PIA que les autres versions. Cette remarque est parfaitement illustrée ici, puisque seule l'application de ce cadre réglementaire conduit l'association à devoir réaliser un PIA. Quatre « critères principaux » sont déclencheurs tandis que l'action d'un cinquième est annulée par une « condition limitante ».

Critère principal / condition limitante	Explications
Données	
1 – Les données révèlent-elles la religion ou les croyances philosophiques ?	**Oui.** Dans certaines situations, les informations relatives à des régimes alimentaires particuliers (kasher, halal, etc.) peuvent conduire à révéler la religion de la personne concernée voir de sa famille.
2 – Les données révèlent-elles l'orientation sexuelle ou l'identité de genre ?	**Oui.** Dans le cas des mineurs, l'association collecte des informations sur l'ensemble de la famille (frère(s), sœur(s), père(s), mére(s)). L'analyse de la structure familiale peut conduire à révéler l'orientation sexuelle des parents, voire d'autres membres de la famille.
3 – Les données concernent-elles la santé ?	**Oui.** L'objectif de l'association est de permettre à des personnes malades de participer à une activité de loisir. Les données traitées par l'application concernent donc en partie l'état de santé de ces personnes afin de pouvoir les accueillir en tenant compte de leur situation individuelle.
4 – Les données sont-elles relatives à des enfants ?	**Oui.** L'association peut organiser des activités de loisirs pour des adultes comme des mineurs. L'application CRM peut donc contenir des données qui sont explicitement « relatives » à des enfants.
4.1 - Ces données sont-elles contenues dans des fichiers informatisés de grande ampleur ?	**Non.** Même si comme cela a déjà été évoqué, la notion de « grande ampleur » reste floue, il a été considéré que la centaine de nom contenu dans le fichier de l'association ne constituait pas un fichier de grande ampleur.

Événement redouté	
5 – Une violation des données risque-t-elle de porter atteinte à la protection des données à caractère personnel, de la vie privée, des droits ou des intérêts légitimes de la personne concernée ?	**Oui.** Cette formulation est très générique et autorise des interprétations très larges. Dans le cas étudié, à l'évidence, compte tenu de la catégorie de personne concernée (malades et, le cas échéant, leur famille) et de la nature des données collectées, une divulgation accidentelle des données à des personnes non-autorisées ou pire à un large public pourrait porter atteinte aux personnes concernées et à leur famille.

L'analyse révèle que l'article 32bis met l'accent sur les données traitées et leur sensibilité ce qui place indiscutablement l'association en position de devoir réaliser un PIA.

Dans une démarche d'analyse de risques et de conception qui prend en compte la protection de la vie privée dès le commencement, il convient d'abord de s'interroger sur la nécessité et sur l'adéquation des données collectées par rapport à la finalité du traitement. Toutes les données sont- elles nécessaires ? Est-il possible d'en supprimer ? Est-il possible d'en remplacer certaines par d'autres qui seraient moins sensibles ? Etc. Le schéma et le tableau précédent font apparaître des données susceptibles de révéler indirectement des informations nouvelles. Il convient alors de s'interroger sur les conditions qui peuvent conduire à la révélation de ces nouvelles informations, ainsi que sur les moyens de les limiter ou, mieux, de les supprimer.

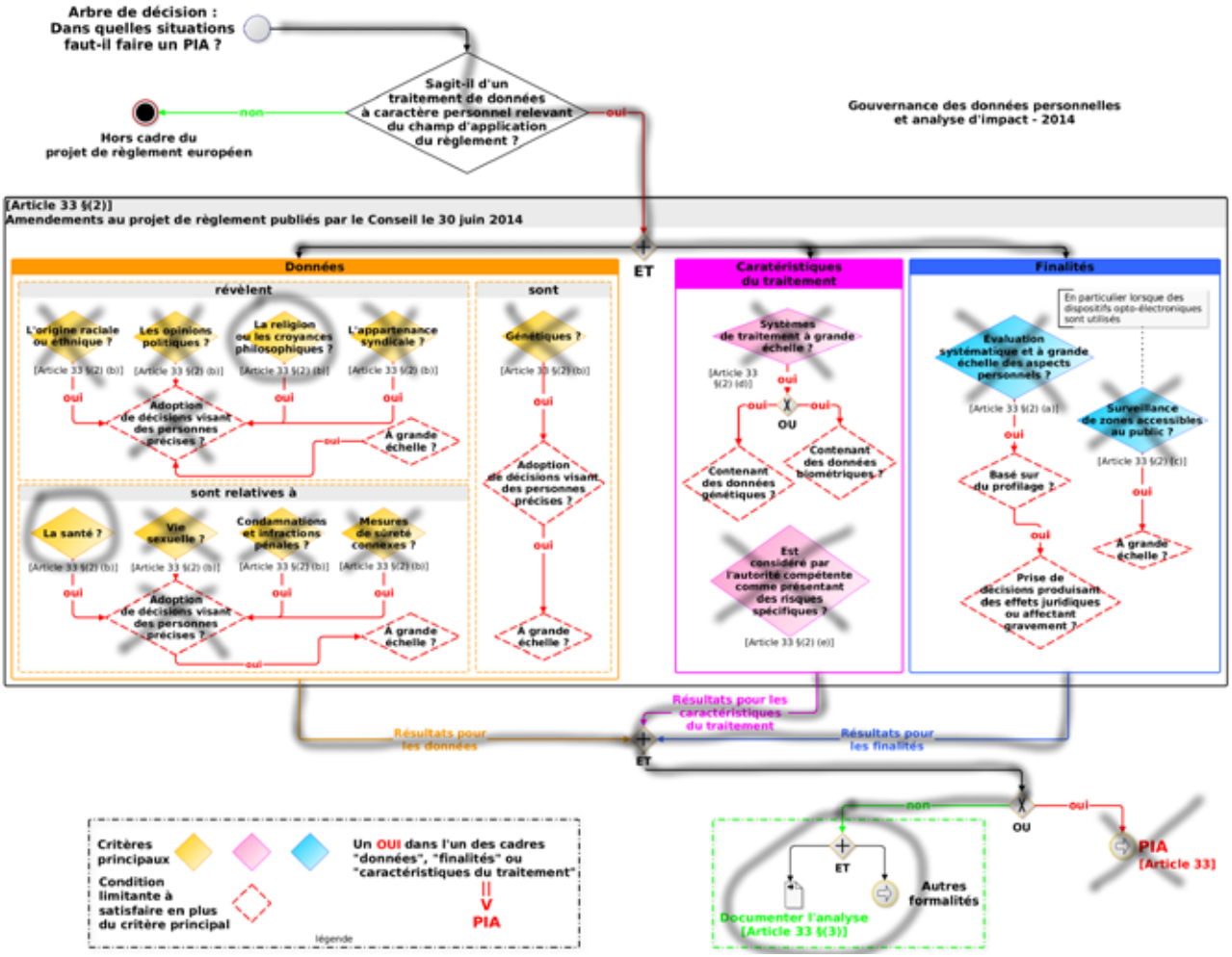
Après rationalisation des données utilisées, il convient de s'intéresser à leur protection. En effet, un autre risque concerne la divulgation à des tiers non-autorisés de façon intentionnelle ou accidentelle. Il est nécessaire d'identifier toutes les situations qui peuvent conduire à un tel résultat, en les hiérarchisant par rapport à leur vraisemblance et à leur impact. Ensuite, il faudra identifier les solutions susceptibles de supprimer ou sinon de réduire ces situations. L'analyse du contexte a notamment fait apparaître un déficit organisationnel quant à la gestion des ressources humaines susceptibles d'accéder aux ressources informatiques et éventuellement à l'application CRM :

- pas de verrouillage automatique des postes de travail,
- pas de politique de gestion des comptes sur l'application CRM (même si toutes les informations ne sont pas accessibles à tous les intervenants, bénévoles ou permanents),
- pas de formation des utilisateurs et notamment des bénévoles (hormis 1/2 journée consacrée au maniement de l'application CRM),
- pas de charte informatique,
- etc.

PARTIE V - ETUDE DE CAS

La fin de vie des données devra aussi être traitée. En effet, l'analyse du contexte a fait ressortir que l'application ne permet pas de traiter les durées de conservation. Au-delà de l'obligation légale, c'est aussi une source de risques supplémentaires. En l'absence de solution technique, le responsable de traitement (l'association) peut a minima mettre en œuvre des solutions organisationnelles qui instaurent des procédures pour la révision régulière des fiches et leur purge lorsqu'elles ne sont plus utiles.
Toutes les situations à risques brièvement indiquées ici doivent être mise en liste et traitées individuellement jusqu'à suppression des risques ou réduction dans des proportions compatibles avec la finalité visée.

Article 33 dans sa version publiée par le Conseil en juin 2014
Le schéma qui résulte de l'analyse est présenté ci-dessous.



Comme dans la première situation, cette troisième analyse ne conduit pas à la réalisation d'un PIA. Ici, seuls deux « critères principaux » ont été entourés, mais leur effet a été immédiatement annulé par les « conditions limitantes » qui les suivent.

Critère principal / condition limitante	**Explications**
Données	
1 – Les données révèlent-elles la religion ou les croyances philosophiques ?	**Oui.** Dans certaines situations, les informations relatives à des régimes alimentaires particuliers (kasher, halal, etc.) peuvent conduire à révéler la religion de la personne concernée voir de sa famille.
1.1 – Ces données sont-elles traitées afin d'adopter des décisions qui visent des personnes précises ?	**Non.** La finalité du traitement n'est pas de révéler la religion d'une personne ou de sa famille, en vue de prendre des décisions de portée large visant des personnes précises. Les données permettant de révéler la religion de personnes sont uniquement traitées afin de prendre en compte les éventuelles spécificités du régime alimentaire d'une personne, dans le cadre de la réalisation de l'activité de loisir exceptionnelle. En effet, cette condition limitante est associée à la condition de «grande échelle». Elle semble ainsi viser les processus de décision à partir d'informations révélant la religion ou les croyances philosophiques de personnes, ayant une portée large et visant des individus déterminés. Elle pourrait faire référence notamment à l'adoption de politiques générales stigmatisant (de manière favorable ou défavorable) des populations spécifiques, ce qui n'est manifestement pas le cas de l'association. En conséquence, cette « condition limitante » ne peut pas être considérée comme satisfaite.

2 – Les données concernent-elles la santé ?	**Oui.** L'objectif de l'association est de permettre à des personnes malades de participer à une activité de loisir. Les données traitées par l'application concernent donc en partie l'état de santé de ces personnes afin de pouvoir les accueillir en tenant compte de leur situation individuelle.
Critère principal / condition limitante	**Explications**
2.1 – Ces données sont-elles traitées afin d'adopter des décisions qui visent des personnes précises ?	**Non.** Les données de santé de chaque malade ne sont pas utilisées en vue de prendre des décisions de portée large et qui visent des personnes précises mais uniquement à prendre en compte la particularité de chacun pour la réalisation de l'activité de loisir exceptionnelle. En effet, cette condition limitante est associée à la condition de « grande échelle »). Elle semble ainsi viser les processus de décision à partir d'informations concernant la santé de personnes, ayant une portée large et visant des individus déterminés. Elle pourrait faire référence notamment à l'adoption de politiques publiques dans le domaine de la santé, ce qui n'est manifestement pas le cas de l'association. En conséquence, cette « condition limitante » ne peut pas être considérée comme satisfaite.

1.3 Analyse d'impact

Nom de l'application	**CRM**
Finalités du traitement	Suivi et gestion de la réalisation d'une activité de loisir exceptionnelle au bénéfice de personnes atteintes d'une maladie grave.

Rappel des fonctionnalités	- collecte des informations d'identification des bénéficiaires de l'activité de loisir exceptionnelle et de leur famille dans le cas des mineurs en particulier. - collecte des informations de santé relatives aux bénéficiaires qui sont utiles pour la réalisation de l'activité de loisir exceptionnelle. - identification des intervenants en charge de la réalisation de l'activité de loisir exceptionnelle et gestion d'une liste de contacts. - description de l'activité de loisir exceptionnelle demandée par le bénéficiaire. - estimation du coût et affectation des ressources. - suivi de la progression de la réalisation de l'activité de loisir exceptionnelle.
Données à protéger	- données identifiantes des bénéficiaires, de leur famille, des bénévoles affectés à la réalisation des activités de loisir exceptionnelles. - les données de santé des bénéficiaires. - les données relatives aux activités de loisir exceptionnelles lorsque celles-ci impliquent des tiers (personnalités, invités, etc.) dont les données sont également collectées. - photos et vidéos réalisées au moment des activités de loisir exceptionnelles.
Supports à protéger	- formulaires de recueil d'information. - formulaires de recueil de consentement. - canaux de transmission entre les postes de travail et le serveur de l'application. - les exportations de la base de données. - le serveur de l'application.
Sources de risques pertinentes	- les bénévoles. - les permanents. - le sponsor hébergeur. - des tiers pouvant accéder aux locaux de l'association.

Mesures de sécurité existantes	- engagement de confidentialité signé par les permanents et les bénévoles. - contrôle d'accès aux locaux de l'association. - contrôle d'accès non-nominatif à l'application CRM. - traçabilité des opérations effectuées dans l'application CRM. - sauvegarde irrégulière de la base de données. - stockage des supports papier en armoire forte. - transmissions via internet sécurisées en utilisant e protocole HTTPS.
Lacunes	- pas de charte informatique. - pas d'accès nominatif à l'application CRM. - pas de politique de gestion des habilitations ni de révocation des accès à l'application CRM à la suite du départ d'une personne. - pas de sensibilisation des permanents sur les obligations légales concernant les données à caractère personnel traitées. - pas de sensibilisation des bénévoles sur les obligations légales concernant les données à caractère personnel traitées. - pas de politique pour l'adaptation de la collecte à la nature du cas traité. - pas de politique pour l'encadrement des zones de libre commentaire. - pas de contrôle d'accès aux postes de travail fixes. - pas de verrouillage des postes de travail après un certain temps d'inactivité. - pas de déconnexion automatique de l'application CRM après un certain temps d'inactivité. - pas de procédure pour la gestion des demandes de droit d'accès, rectification, suppression.

	- pas de chiffrement des sauvegardes de la base de données. - pas de stockage redondant des sauvegardes de la base de données. - pas de politique de gestion des durées de conservation. - pas de procédure pour la sauvegarde régulière de la base de données. - pas de contrat de sous-traitance avec le sponsor/ hébergeur qui emporte de nombreuses incertitudes concernant la sécurité de l'hébergement, la sauvegarde des données, leur confidentialité, etc. - pas de réalisation de formalité auprès de la Cnil.

1.4 Tableau synthétique des risques

Le tableau qui suit présente quelques risques parmi ceux qui ont été identifiés comme maximums ou importants. Ils concernent des impacts possibles sur les personnes et les obligations de sécurités qui incombent au responsable de traitement.

Identification	**Commentaires**
R1 - Collecte excessive	Ce risque est maximum en raison de l'absence de sensibilisation des personnels, bénévoles ou permanents, affectés à la collecte des informations associé à l'utilisation d'un logiciel conçu pour être très générique sans intégrer le principe de « minimisation » de la collecte.
R2 – Accès non-autorisés	Ce risque est maximum en raison de la diffusion des identifiants pour la connexion aux CRM (ceux qui ne permettent que l'accès aux données d'identification des personnes concernées) et de la possibilité de se connecter depuis n'importe quel terminal relié à internet.
R3 – Perte de contrôle de l'application chez le sponsor/ hébergeur	Ce risque est maximum en l'absence d'un contrat de sous-traitance concernant l'application CRM avec le sponsor/hébergeur. L'association se retrouve dans l'incapacité de garantir la sécurité et la confidentialité des données hébergées en Australie. Elle ne maîtrise pas non plus les opérations de maintenance et d'évolution de l'application.

R4 – Atteinte aux droits des personnes concernées	Ce risque est important en raison du risque R2 précédent qui peut conduire des personnes mal intentionnées à utiliser des informations pour porter préjudice à des bénéficiaires ou à leur famille.
R5 – Perte de données	Ce risque est important en raison de l'absence de contrôle sur la réalisation de sauvegardes régulières du côté du sponsor/hébergeur, de l'absence de mise en place de procédures de sauvegardes régulières et du fait que les sauvegardes effectuées de façon irrégulières ne sont pas conservées de manière redondante.

1.5 Conclusion

Selon le cadre réglementaire sélectionné, l'association échappe deux fois sur trois à la réalisation d'un PIA. Pourtant, compte tenu de ses objectifs et des données traitées, le devoir de réaliser une telle analyse ne surprend pas, car le traitement de données à caractère personnel concernant des enfants et la santé sont sensibles et semblent devoir nécessiter une vigilance renforcée pour en limiter les risques.

Dans le contexte de cette association, le PIA apparaît comme un outil précieux pour aider à diminuer les risques associés à un traitement de données à caractère personnel. Il offre une démarche systématique dont le niveau de granularité peut être ajusté en fonction des moyens et des objectifs visés. Tandis que l'arbre de décision proposé par l'article 32bis permet de mettre en lumière rapidement les points délicats.

2. CAS N°2 « PROGRAMME DE FIDÉLITÉ »

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 utilise sur une application à installer sur un smartphone et un site web dédié.

Le traitement vise en particulier à gérer :

- la collecte et mise à jour des données personnelles des clients (via l'application pour mobiles ou le site web dédié),
- 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.),
- 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.

2.1 Analyse du contexte et cartographie des traitements mis en œuvre dans le cas n°2

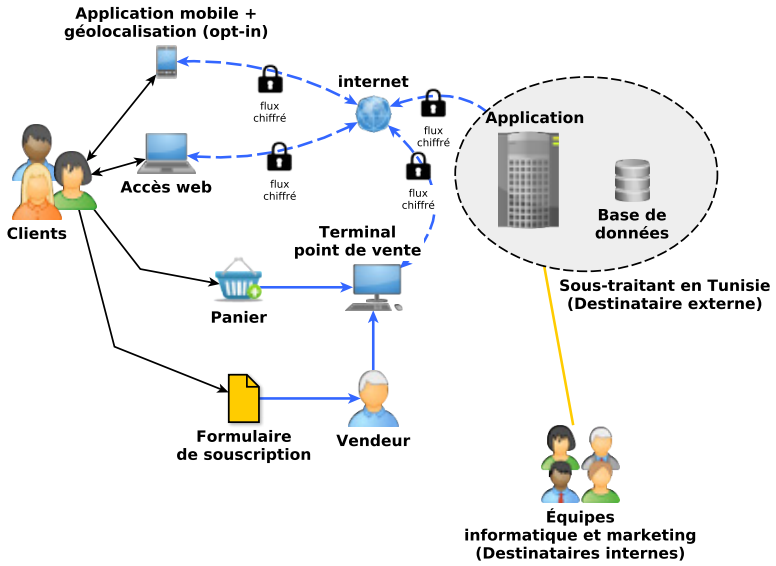
Nom de l'application	**Gestion d'un programme de fidélité.**
Finalités du traitement	Gestion et suivi d'un programme de fidélité avec production de statistiques anonymes.
Formalités	Une déclaration normale a été effectuée auprès de la Cnil (il n'y a pas encore de Cil).

Catégories de données traitées	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).
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.).
Personnes concernées	Clients.
Type de collecte	Collecte directe.
Information des personnes	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.
Durées de conservation	Conservation des données pendant la durée nécessaire à la finalité du traitement

Destinataires	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)	Aucune.
Encadrement des ZLC	Sans objet.
Interconnexion de fichiers	Pas d'interconnexion avec une autre application, ou une base de données ou un fichier.
Flux transfrontière (FT)	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
Droits des personnes	Interface prévue dans l'application web pour l'exercice par l'utilisateur de ses droits.

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.

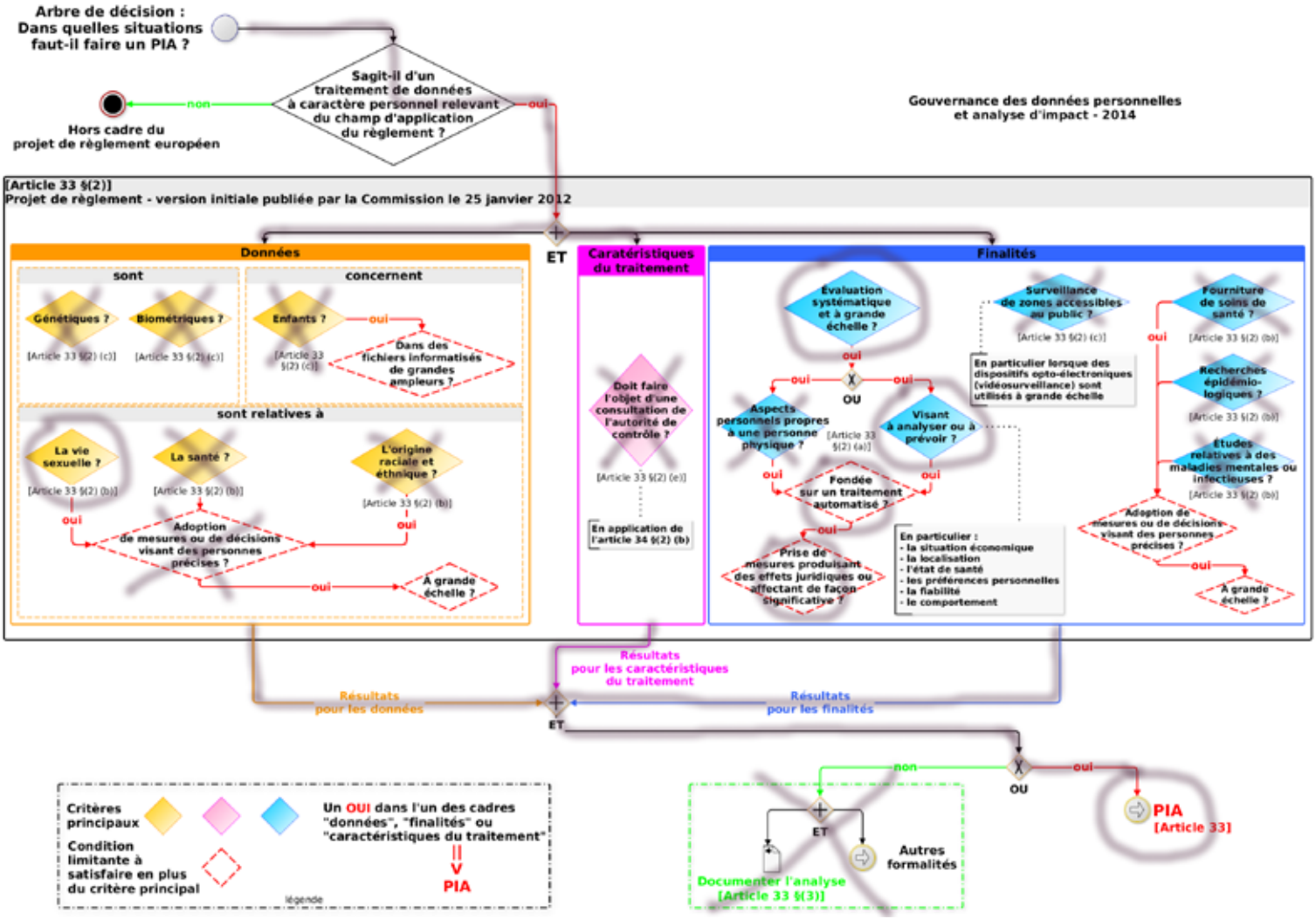


2.2 Analyse des arbres de décision concernant le cas n°2

En suivant la méthode présentée en Annexe 2, les schémas correspondants aux trois versions de l'article 33 étudié dans ce livre blanc ont été utilisés pour identifier les situations pouvant conduire à la réalisation d'un PIA. Quel que soit l'arbre de décision utilisé, tous conduisent au PIA, après l'activation d'un plus ou moins grand nombre de « critères principaux ».

Article 33 dans sa version initiale proposée par la Commission

Le schéma qui résulte de l'analyse est présenté ci-dessous.



L'analyse conduit à l'activation de « critère principaux » dans les catégories « données » et « finalités ». Cependant seuls ceux de la catégorie « finalités » conduisent à l'obligation de réaliser un PIA. En effet, pour la catégorie « données », l'action du « critère principal » est annulée par la « condition limitante » qui le suit.

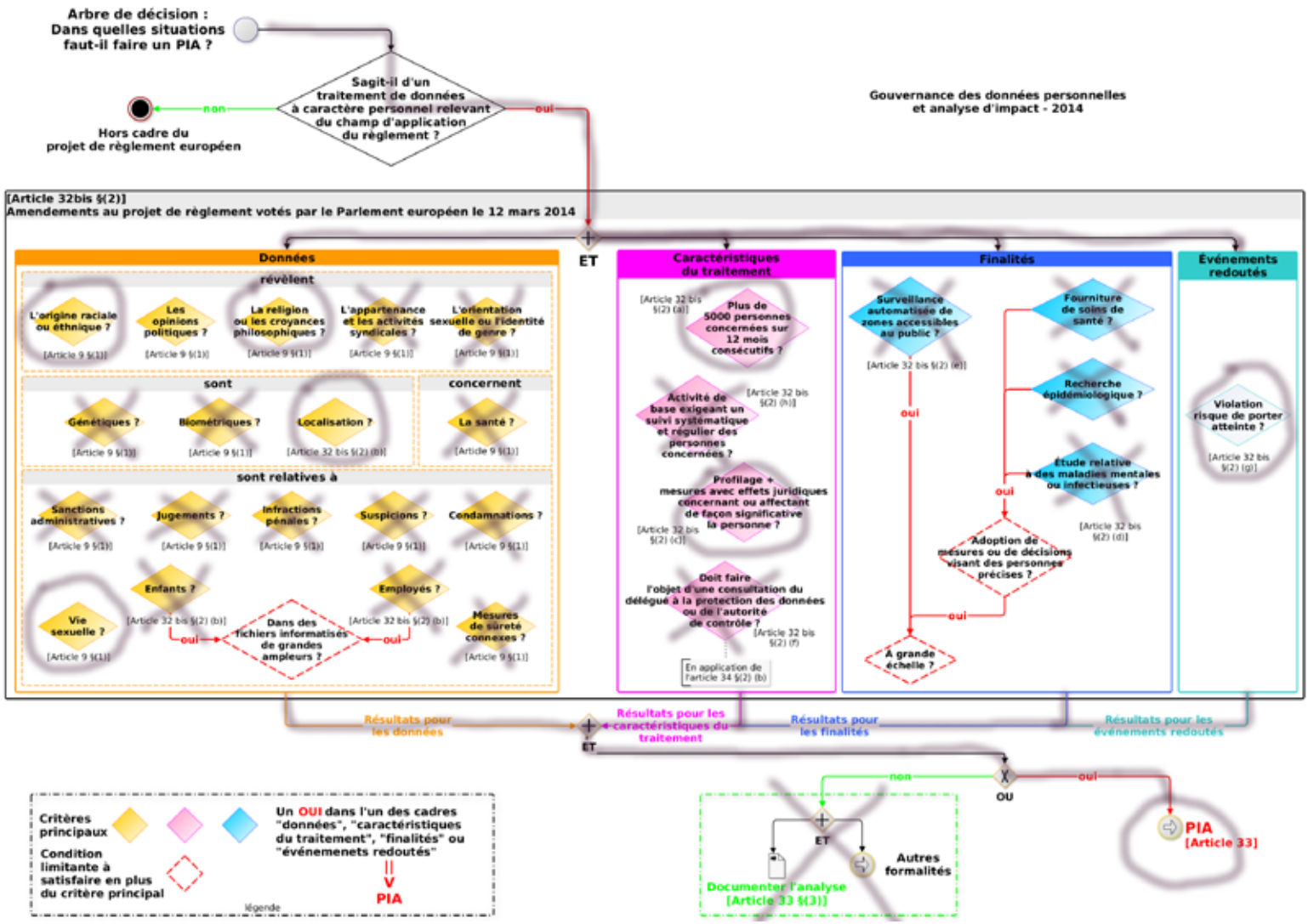
Critère principal / condition limitante	Explications
Données	
1 – Les données traitées sont-elles relatives à la vie sexuelle ?	**Oui.** Dans l'historique d'achat, certains produits (ex. : préservatifs) sont relatifs à la vie sexuelle.
1.1 – Ces données sont-elles traitées afin d'adopter des mesures ou des décisions qui visent des personnes précises ?	**Non.** Les données relatives à la vie sexuelle ne sont pas collectées en tant que telles, en vue de prendre des décisions ou des mesures de portée large visant des personnes précises mais uniquement afin de comprendre, analyser et éventuellement récompenser à une échelle individuelle l'achat de produits de l'enseigne de grande distribution. En effet, cette condition limitante est associée à la condition de « grande échelle ». Elle semble ainsi viser les processus de décision ou d'adoption de mesures à partir d'informations relatives à la vie sexuelle de personnes, ayant une portée large et visant des individus déterminés. Elle pourrait faire référence notamment à l'adoption de politiques générales stigmatisant (de manière favorable ou défavorable) des populations spécifiques, ce qui n'est manifestement pas le cas en l'espèce. En conséquence, cette « condition limitante » ne peut pas être considérée comme satisfaite.
Finalités	
2 – Le traitement a-t-il pour finalité une évaluation systématique et à grande échelle ?	**Oui.** L'application de gestion d'un programme de fidélité est mise en oeuvre par une grande enseigne de la grande distribution qui est présente sur l'ensemble du territoire national. Cette application touche donc potentiellement un grand nombre de personnes dont, dès lors qu'elles ont adhéré au programme, les habitudes de consommation font l'objet d'une évaluation systématique.

3 – Le traitement a-t-il pour finalité d'analyser ou de prévoir ?	**Oui.** La finalité du traitement est effectivement d'analyser les comportements d'achats des clients de façon notamment à leur faire des offres promotionnelles adaptées à leurs besoins. Il y a donc aussi prévision.
3.1 – L'analyse et la prévision sont-elles fondées sur un traitement automatisé ?	**Oui.** L'attribution de points de fidélité, les offres promotionnelles, etc. sont réalisées de façon entièrement automatique en utilisant différents algorithmes d'analyse statistique.
3.2 – Le traitement conduit-il à la prise de mesures produisant des effets juridiques ou affectant de façon significative les personnes concernées ?	**Oui.** Le programme de fidélité est engagement de l'enseigne à offrir des avantages à ses clients. Il fait l'objet d'un descriptif dans les conditions générales d'utilisation qui sont opposables à l'enseigne. Ces avantages ne sont pas anecdotiques, ils peuvent donc affecter de façon significative le pouvoir d'achat de certains clients.

Le traitement mis en oeuvre par l'enseigne est, à l'évidence, un traitement dit de « profilage ». Pour la Commission ce type traitement peut présenter des risques particuliers au regard des droits et des libertés des personnes concernées comme l'indique le point a) du §(2) de l'article 33.

Article 32bis dans sa version votée par le Parlement en mars 2014

Le schéma qui résulte de l'analyse est présenté ci-dessous.



Dans ce cas aussi, l'analyse conduit à la nécessiter de réaliser un PIA. Sur les trois, c'est l'arbre de décision qui active le plus de « critères principaux » : sept dans trois catégories différentes.

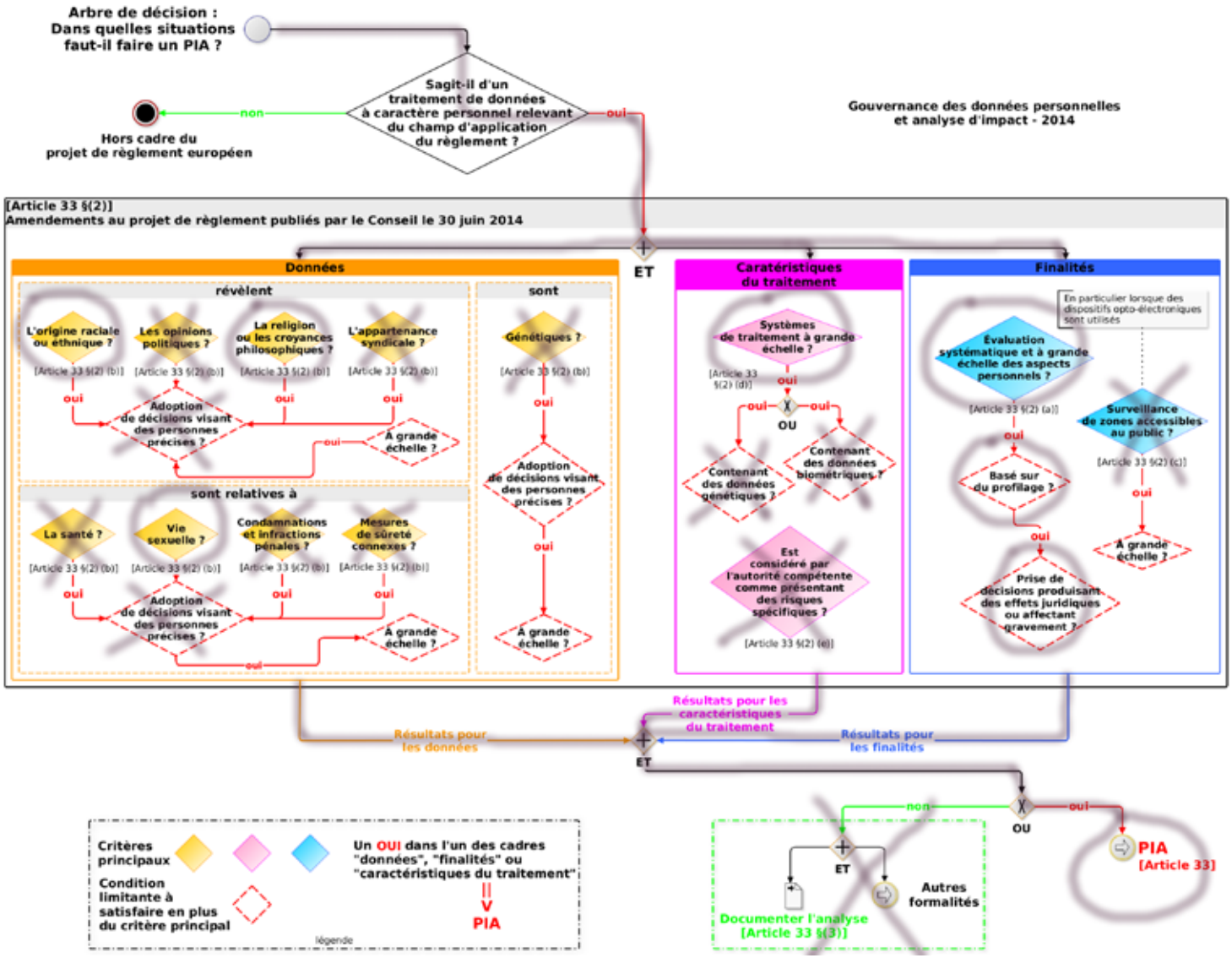
Critère principal / condition limitante	Explications
Données	
1 – Les données traitées révèlent-elles l'origine raciale ou ethnique ?	**Oui.** Dans l'historique d'achat, certains produits de beauté ciblés (ex. : solution pour défriser des cheveux crépus, crème pour éclaircir la peau, etc.) peuvent conduire à révéler des informations sur les origines raciales ou ethniques.
2 – Les données traitées révèlent-elles la religion ou les croyances philosophiques ?	**Oui.** Dans l'historique d'achat, certains produits alimentaires (ex. : halal, kasher, etc.) peuvent conduire à révéler des informations sur les croyances religieuses.
3 – Les données traitées sont-elles des données de localisation ?	**Oui.** L'application pour mobiles propose d'utiliser les coordonnées GPS pour indiquer le magasin le plus proche de l'utilisateur. Cette fonctionnalité est désactivée par défaut.
4 – Les données traitées sont-elles relatives à la vie sexuelle ?	**Oui.** Dans l'historique d'achat, certains produits (ex. : préservatifs) sont relatifs à la vie sexuelle.
Caractéristiques du traitement	
5 – Le traitement concerne t-il plus de 5000 personnes sur une période de 12 mois consécutifs ?	**Oui.** L'application de gestion d'un programme de fidélité est mise en oeuvre par une grande enseigne de la grande distribution qui est présente sur l'ensemble du territoire national. Cette application touche donc potentiellement un très grand nombre de personnes sans aucun doute supérieur à 5000 sur une période de 12 mois consécutifs.
6 – Le traitement inclut-il l'établissement de profils sur la base duquel sont prises des mesures produisant des effets juridiques concernant ou affectant de façon significative les personnes concernées ?	**Oui.** Le traitement utilise des algorithmes statistiques pour analyser les historiques d'achat de façon à identifier des comportements types chez les clients. Il s'agit bien de profilage. Ensuite, le programme de fidélité est un engagement de l'enseigne à offrir des avantages à ses clients. Il fait l'objet d'un descriptif dans les conditions générales d'utilisation qui sont opposables à l'enseigne. Ces avantages ne sont pas anecdotiques, ils peuvent donc affecter de façon significative le pouvoir d'achat de certains clients.

Événement redouté	
7 – Une violation des données à caractère personnel risque-t-elle de porter atteinte à la protection des données à caractère personnel, de la vie privée, des droits ou des intérêts légitimes de la personne concernée ?	**Oui.** Une violation des données du programme de fidélité pourrait porter atteinte aux personnes concernées en révélant des habitudes de consommation à des tiers à qui elles ne souhaitent pas donner ces informations. Elle pourrait aussi les priver des avantages auxquels elles peuvent légitimement prétendre.

Dans le cas de cet arbre de décision, l'analyse conduit à la réalisation d'un PIA avec sept « critères principaux » activés directement. Ce qui confirme le fait déjà souligné que l'article 32 bis proposé par le Parlement est le plus sensible aux risques potentiels posés par un traitement de données à caractère personnel.
Ici, l'analyse est sensible aux types de données traitées et à ce qu'elles peuvent révéler sur les personnes concernées en fonction des traitements qu'elles sont susceptibles de subir. Elle est également sensible à certaines caractéristiques du traitement et à ses conséquences en cas de faille.

Article 33 dans sa version publiée par le Conseil en juin 2014

Le schéma qui résulte de l'analyse est présenté ci-dessous.



Critère principal / condition limitante	Explications
Données	
1 – Les données traitées révèlent-elles l'origine raciale ou ethnique ?	**Oui.** Dans l'historique d'achat, certains produits de beauté ciblés (ex. : solution pour défriser des cheveux crépus, crème pour éclaircir la peau, etc.) peuvent conduire à révéler des informations sur les origines raciales ou ethniques.
2 – Les données traitées révèlent-elles la religion ou les croyances philosophiques ?	**Oui.** Dans l'historique d'achat, certains produits alimentaires (ex. : halal, kasher, etc.) peuvent conduire à révéler des informations sur les croyances religieuses.
1.1 et 2.1 – Le traitement de ces données vise-t-il à adopter des décisions visant des personnes précises ?	**Non.** La finalité du traitement n'est pas de révéler des origines raciales ou ethniques ou la religion d'une personne, en vue de prendre des décisions de portée large visant des personnes précises. Le traitement vise uniquement à comprendre, analyser et éventuellement récompenser à une échelle individuelle l'achat de produits de l'enseigne de grande distribution. En effet, cette condition limitante est associée à la condition de « grande échelle ». Elle semble ainsi viser les processus de décision à partir d'informations révélant l'origine raciale ou ethnique, la religion ou les croyances philosophiques de personnes, ayant une portée large et visant des individus déterminés. Elle pourrait faire référence notamment à l'adoption de politiques générales stigmatisant (de manière favorable ou défavorable) des populations spécifiques, ce qui n'est manifestement pas le cas en l'espèce. En conséquence, cette « condition limitante » ne peut pas être considérée comme satisfaite.
3 – Les données traitées sont-elles relatives à la vie sexuelle ?	**Oui.** Dans l'historique d'achat, certains produits (ex. : préservatifs) sont relatifs à la vie sexuelle.

3.1 – Ces données sont-elles traitées afin d'adopter des décisions qui visent des personnes précises ?	**Non.** Les données relatives à la vie sexuelle ne sont pas collectées en tant que telles, en vue de prendre des décisions ou des mesures de portée large visant des personnes précises mais uniquement afin de comprendre, analyser et éventuellement récompenser à une échelle individuelle l'achat de produits de l'enseigne de grande distribution. En effet, cette condition limitante est associée à la condition de « grande échelle ». Elle semble ainsi viser les processus de décision à partir d'informations relatives à la vie sexuelle, ayant une portée large et visant des individus déterminés. Elle pourrait faire référence notamment à l'adoption de politiques générales stigmatisant (de manière favorable ou défavorable) des populations spécifiques, ce qui n'est manifestement pas le cas en l'espèce. En conséquence, cette « condition limitante » ne peut pas être considérée comme satisfaite.
Caractéristiques du traitement	
4 – L'application est-elle un système de traitement de données à caractère personnel à grande échelle ?	**Oui.** Même si la notion de « grande échelle » doit être précisée, l'application de gestion d'un programme de fidélité est mise en oeuvre par une grande enseigne de la grande distribution qui est présente sur l'ensemble du territoire national. Cette application touche donc potentiellement un très grand nombre de personnes et ce « critère principal » peut être considéré comme satisfait.
4.1 – L'application contient-elle des données génétiques ?	**Non.**
4.2 – L'application contient-elle des données biométriques ?	**Non.**

Finalités	
5 – L'application a-t-elle pour finalité l'évaluation systématique et à grande échelle des aspects personnels propres à des personnes physiques ?	**Oui.** Le traitement utilise des algorithmes statistiques pour analyser les historiques d'achat de façon à identifier des comportements types chez les clients ce qui représente bien une « évaluation systématique » des aspects personnels propres à des personnes physiques. De plus, comme l'application de gestion d'un programme de fidélité est mise en oeuvre par une grande enseigne de la grande distribution qui est présente sur l'ensemble du territoire national, elle touche potentiellement un très grand nombre de personnes et ce « critère principal » peut donc être considéré comme satisfait.
5.1 – L'évaluation est-elle basée sur l'établissement de profils ?	**Oui.** Pour les raisons qui viennent d'être évoquées.
5.2 – Des décisions produisant des effets juridiques ou affectant gravement les personnes concernées sont-elles prises sur la base de cette évaluation ?	**Oui.** Le programme de fidélité est un engagement de l'enseigne à offrir des avantages à ses clients. Il fait l'objet d'un descriptif dans les conditions générales d'utilisation qui sont opposables à l'enseigne.

Dans cette dernière analyse, l'application de gestion d'un programme de fidélité doit faire l'objet d'un PIA en raison de sa finalité qui implique notamment du « profilage ». Quatre autres « critères principaux » ont été activés mais leur action a été annulée par les « conditions limitantes » qui les suivent.

2.3 Analyse d'impact

Nom de l'application	Gestion d'un programme de fidélité
Finalités du traitement	- gestion et suivi de programmes de fidélité en vue de la fidélisation clients - production de statistiques anonymes afin d'identifier des actions marketing
Rappel des fonctionnalités	- collecter et mettre à jour les données d'identification du client bénéficiaire du programme de fidélité auprès de l'enseigne de la grande distribution, grâce à une application pour mobile ou via un site web dédié. Le recueil des données lors de l'adhésion au programme de fidélité est réalisé sur support papier. Elles sont saisies dans l'application par le vendeur. Puis la mise à jour des données est opérée par le client. - collecter et synchroniser l'historique des achats effectués auprès de l'enseigne pour évaluer la fidélité du client (ex. : liste des produits achetés, prix, fréquence d'achat, etc.). - rétribuer la fidélité des clients sous forme de coupons d'achat, points de fidélité, cadeaux en fonction de critères tels que la fréquence des achats et les montants dépensés. - informer en temps réel les clients de leurs acquis au titre du programme de fidélité via des notifications push. - suivre les modalités de transformation des avantages fidélité acquis (conversion de points fidélité/produits). - établir des profils de clients, en fonction des habitudes de consommation, afin d'orienter le marketing produit et d'offrir des cadeaux rétribuant la fidélité correspondant aux habitudes d'achat. - établir des statistiques de consommation anonymes.

Éléments à protéger	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). Donnes issues du profilage (révélant la religion ou l'origine raciale ou relatives à la sexualité).
Supports à protéger	- formulaires d'adhésion au programme de fidélité, en papier, signés par les clients (conservés non-scannés dans les bureaux de chaque magasin, dans une armoire forte). - canaux de transmission internet depuis le serveur des magasins vers l'hébergeur et pour les accès aux données depuis le siège de l'enseigne. - canaux de transmission depuis la caisse vers le serveur du magasin (pas de Wifi ni de mémoire ni de données sur les caisses). - serveurs et back-up localisés en Tunisie. - restitution des statistiques d'achat une fois par mois sous excel par mail.
Exercice des droits	- information complète du client et obtention du consentement lors de la signature du contrat d'adhésion au programme de fidélité. - consentement pour les conditions générales d'utilisation de l'application et contrat d'acceptation distinct pour l'installation et l'utilisation de l'application pour mobiles. - espace client sur le site web du programme pour la mise à jour des données personnelles. - accès des clients à leur historique d'achats pour les 6 derniers mois. - possibilité de suppression complète du compte après résiliation de l'adhésion au programme de fidélité.
Sources de risques pertinentes	- salariés - prestataires - concurrents - clients

Mesures de sécurité existantes

Périmètres des données personnelles :
Stockage des formulaires d'adhésion signés dans une armoire forte située dans les bureaux de chaque point de vente, dont l'accès est restreint par badge.

Contrôle des accès côté responsable de traitement :
- les locaux du siège de l'enseigne 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 associé à un mot de passe.
- l'utilisation des systèmes d'information au sein de l'enseigne est encadrée par une Charte informatique pour l'ensemble des salariés ainsi que par une Charte « administrateur », spécifique à cette catégorie de salariés.

Contrôle des accès côté client :
- chaque client dispose d'un compte propre, associé à l'application qu'il a téléchargée sur son appareil mobile ou associée à son profil web. Les accès à l'application et les actions effectuées par le client sur les données sont enregistrés dans l'application (journal).
- l'accès à l'application est protégé par un mot de passe librement choisi par le client.
- les connexions internet sont sécurisées par un chiffrement de bout en bout.

Périmètre des moyens :
lieux de traitement des données (collecte, stockage, sauvegarde, archivage et restitution).
- zones géographiques concernées par les flux transfrontaliers : l'application est hébergée sur les serveurs d'un prestataire situé hors UE (Tunisie).

Périmètre des processus métiers :
- collecte initiale en magasin.
- saisie des données relatives à l'adhésion au programme de fidélité.
- gestion des accès à l'espace personnel et aux systèmes informatiques et aux données.
- gestion des encaissements/caisses (avec accès au seul n° d'adhérent).
- gestion des données des paniers d'achat (référence au seul n° d'adhérent).
- gestion de l'exploitation courante (y inclus sous tableur) et des évolutions de l'application.
- gestion des modalités de restitution et de diffusion.
- gestion de la rétention des données.

Périmètre des processus légaux :
- gestion des droits (information sur les droits, exercices des droits, etc.).
- modalités d'encadrement des droits.

2.4 Tableau synthétique des risques

La cartographie des risques a été établie pour les risques élevés à très élevés. Ces risques ont été appréciés tant en termes financiers qu'en termes d'image. Ils sont présentés dans le tableau qui suit.

Evénements redoutés jugés comme les plus graves	Caractère identifiant des DCP	Caractère préjudiciable des impacts potentiels (conséquence, importance des dommages)	Mesures réduisant la gravité	Gravité des évènements redoutés[82]
R1 – Détournement de finalité du traitement par le responsable de traitement, les équipes marketing ou informatique	4. Maximal très facile d'identifier les personnes au travers soit des données d'adhésion, soit du lien via le n° d'adhésion	4. Maximal très variable, mais possibilité d'atteinte morale durable	Aucune	4. Maximal
R2 – Accès illégitime aux données par le responsable de traitement, les personnels ou personnes non-autorisées, ex : caissiers sur le point de vente, services marketing, informatique, sous-traitant	4. Maximal idem	4. Maximal	Aucune	4. Maximal

[82] *Gravité : somme du caractère préjudiciable de la conséquence et du caractère identifiant des données à caractère personnel (dans le tableau « DCP »).*

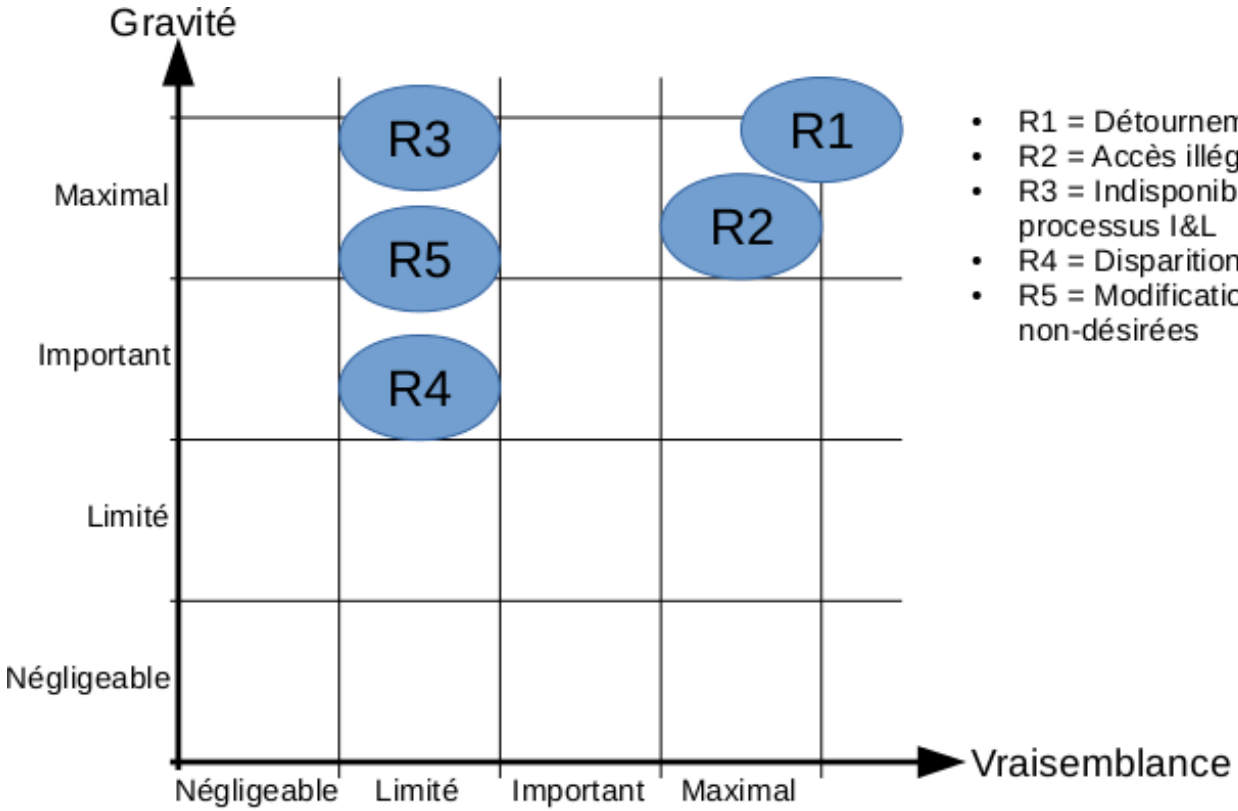
Menaces[83] jugées comme les plus vraisemblables[84]	Vulnérabilité des supports	Capacité des sources de risques (capacité à exploiter les vulnérabi-lités)	Mesures réduisant la vraisemblance	Vraisemblance maximale
Le responsable de traitement, les équipes marketing ou informatique, pourraient mettre en oeuvre un traitement de données visant notamment à corréler le fichier des données d'identification et celui des profils consommateurs par exemple dans le cadre d'une approche « big data »	4. Maximal dès lors qu'une personne dispose d'un accès aux deux types de fichiers (l'identifiant commun des deux fichiers étant le n° adhérent)	4. Maximal données de profilage sous excel	Aucune	4. Maximal
Toute personne ayant accès à l'emplacement où est archivé le fichier « physique » des données d'identification et ayant accès au fichier informatisé des profils de consommation pourrait prendre connaissance notamment d'informations relatives aux habitudes de consommation d'utilisateurs identifiables	4. Maximal dès lors qu'un membre du personnel dispose d'un accès aux deux types de fichiers	4. Maximal Le prestataire a des accès illimités +marketing peut accéder en lecture et mise à jour	- Existence d'un accès restreint aux données sur supports papiers (badge) - Existence d'un accès sécurisé aux postes de travail/applications (identifiant mot de passe) - Cryptage des données et existence d'un contrat de sous-traitance incluant clauses de confidentialité et sécurité	4. Maximal, Un très grand nombre de personnes risque de voir leurs DCP dévoilées

[83] Menaces listées pour chaque événement redouté, de gravités non négligeables et non limitées.
[84] Vraisemblance : somme de la vulnérabilité des supports et des capacités des sources de risques (après prise en compte des mesures de réduction).

R3 – Indisponibilité des processus requis par la loi Informatique & Libertés (ex : absence d'information des utilisateurs sur l'exercice de leurs droits, absence de consentement, etc.)	4. Maximal	4. Maximal	Aucune	4. Maximal
R4 – Disparition des données	4. Maximal	2. Limité	Aucune	3. Important
R5 – Modification non désirée des données	4. Maximal	4. Maximal	Aucune	4. Maximal

L'application ou l'Espace utilisateur du site web se bloque, faisant obstacle par exemple à la possibilité pour l'utilisateur de supprimer ses données	2. Limité dès lors que les processus sont automatisés principalement via l'application ou l'interface utilisateur du site web	3. Important (disponibilité des systèmes assurée par le sous-traitant et évolution régulière des versions de l'application)	Aucune	2. Limité
Par exemple, en cas de : - dysfonctionnement de l'application, ou de l'Espace Utilisateur - problème de sauvegarde sur les serveurs du sous-traitant	4. Maximale	1. Négligeable (seul le sous-traitant est intervenant dans le processus d'exploitation)	Aucune	2. Limité
Par exemple, en cas de : - dysfonctionnement de l'application, ou de l'Espace Utilisateur - problème de sauvegarde sur les serveurs du sous-traitant	4. Maximal dès lors qu'une personne dispose d'un accès aux fichiers concernés	1. Négligeable	Encadrement de l'utilisation des systèmes d'information par une charte	2. Limité

La matrice qui suit résume les principaux résultats :



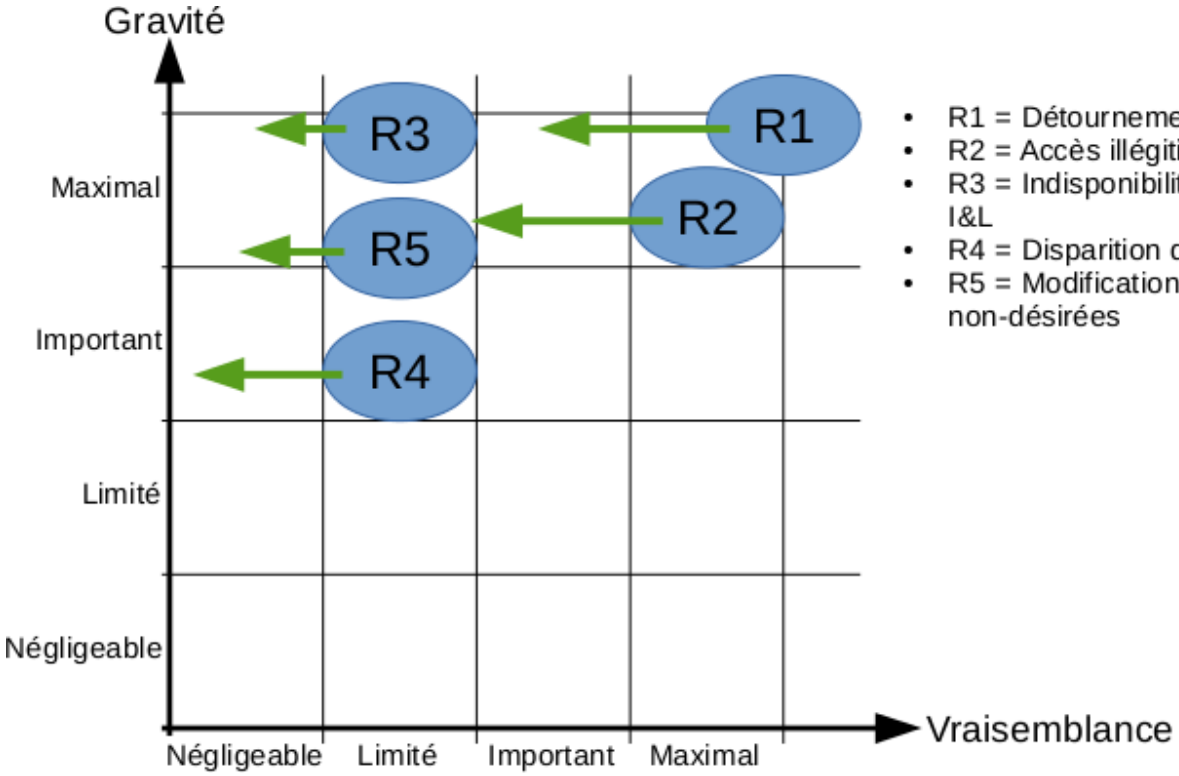
- R1 = Détournement de finalités
- R2 = Accès illégitime
- R3 = Indisponibilité des processus I&L
- R4 = Disparition des données
- R5 = Modification des données non-désirées

2.5 Proposition de mesures permettant de limiter les risques

Pour supprimer ou limiter les risques qui viennent d'être identifiés, voici quelques mesures qui pourraient être mises en place :

Risque	Mesures
R0 – Générique	• nomination d'un Cil ou d'un DPO
R1 – Détournement de finalités du traitement par le personnel interne.	• suppression des possibilités d'exportation des données pour réaliser des analyses non-prévues dans l'application de gestion d'un programme de fidélité. • externalisation des mailings personnalisés. • mise en place d'une Charte de bonne conduite dédiée aux équipes marketing.
R2 – Accès illégitime aux données par du personnel interne ou du sous-traitant.	• chiffrement des données. • limitation des accès aux fichiers sur la base de profils ayant une durée de vie limitée.
R3 – Indisponibilité des processus requis par la loi Informatique & Libertés.	• mise en place d'un système d'alerte permettant de signaler tout dysfonctionnement.
R4 – Disparition des données.	• mise en place de sauvegardes redondantes et séparées géographiquement. • conservation des documents papier dans des armoires fortes.
R5 – Modification des données non-désirées.	• mise en place d'un dispositif d'alerte sur la base d'enregistrements témoins signalant les accès aux fichiers et les tentatives de modifications.

La matrice qui suit résume la cartographie des risques résiduels après mise en place des mesures précédentes :



- R1 = Détournement de finalités
- R2 = Accès illégitime
- R3 = Indisponibilité des processus I&L
- R4 = Disparition des données
- R5 = Modification des données non-désirées

ANNEXE 1 : TABLEAU COMPARATIF DES DIFFÉRENTES VERSIONS DE L'ARTICLE 33 DE LA PROPOSITION DE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES[85]

Propositions du Parlement européen (mars 2014)	Proposition initiale de la Commission européenne (janvier 2012)	Propositions issues du Conseil de l'Union européenne (juin 2014)[86]
Article 32 bis Prise en compte des risques		
1. Le responsable du traitement ou, le cas échéant, le sous-traitant, réalise 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.		
2. Les traitements susceptibles de présenter des risques spécifiques sont les suivants:		
2 (a) le traitement de données à caractère personnel de plus de 5 000 personnes concernées sur une période de douze mois consécutifs ;		
2 (b) le traitement des catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1[87], des données de localisation, ou des données relatives à des enfants ou des employés dans des fichiers informatisés de grande ampleur ;		
2 (c) l'établissement de profils sur la base desquels sont prises des mesures produisant des effets juridiques concernant ou affectant de manière tout aussi significative ladite personne ;		
2 (d) le traitement de données à caractère personnel destinées à la fourniture de soins de santé, à des recherches épidémiologiques ou à des études relatives à des maladies mentales ou infectieuses, lorsque les données sont traitées aux fins de l'adoption de mesures ou de décisions à grande échelle visant des personnes précises ;		
2 (e) la surveillance automatisée à grande échelle de zones accessibles au public ;		
2 (f) les autres traitements pour lesquels la consultation du délégué à la protection des données ou de l'autorité de contrôle est requise en application à l'article 34, paragraphe 2, point b)[88] ;		

[85] Le texte en italique correspond aux ajouts ou modifications apportés au texte de la Commission européenne. Les parties de texte supprimées sont indiquées comme suit : (...).

[86] Traduction libre par le cabinet ALAIN BENSOUSSAN AVOCATS.

[87] Il s'agit des « données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances philosophiques , l'orientation sexuelle ou l'identité de genre, l' appartenance et les activités syndicales , ainsi que le traitement des données génétiques ou biométriques ou des données concernant la santé ou relatives à la vie sexuelle, aux sanctions administratives, aux jugements, à des infractions pénales ou à des suspicions, à des condamnations, ou encore à des mesures de sûreté connexes ».

[88] Il s'agit des cas dans lesquels « le délégué à la protection des données ou l'autorité de contrôle estime nécessaire de procéder à une consultation préalable au sujet de traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées, du fait de leur nature, de leur portée et/ou de leurs finalités (...) ».

2 (g) lorsqu'une violation des données à caractère personnel risque de porter atteinte à la protection des données à caractère personnel, de la vie privée, des droits ou des intérêts légitimes de la personne concernée ;		
2 (h) les activités de base du responsable du traitement ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées ;		
[...]		
3. En fonction des résultats de l'analyse du risque:		
[...]		
3 (c) lorsqu'il est procédé à l'un quelconque des traitements visés aux points a), b), c), d), e), f), g) ou h) du paragraphe 2, le responsable du traitement ou le sous-traitant agissant pour le compte du responsable du traitement procède à une analyse d'impact relative à la protection des données, conformément à l'article 33;		
[...]		
4. L'analyse des risques est révisée au plus tard après un an, ou immédiatement si la nature, la portée ou les finalités des traitements sont sensiblement modifiées. Lorsqu'en application du point c) du paragraphe 3, le responsable du traitement n'est pas tenu de procéder à une analyse d'impact relative à la protection des données, l'analyse des risques est documentée.		
Article 33 Analyse d'impact relative à la protection des données		
1. Lorsque *les dispositions de l'article 32 bis, paragraphe 3, point c) l'exigent* , le responsable du traitement ou le sous-traitant agissant pour le compte du responsable du traitement effectuent une analyse de l'impact des traitements envisagés *sur les droits et les libertés des personnes concernées, en particulier leur droit à* la protection des données à caractère personnel. *Une seule analyse suffit à examiner un ensemble de traitements similaires qui présentent des risques similaires.*	1 Lorsque les traitements présentent des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités, le responsable du traitement ou le sous-traitant agissant pour le compte du responsable du traitement effectuent une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel.	1. Lorsque *le traitement, compte tenu de sa nature, de sa portée ou de ses finalités, est susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées*, le responsable du traitement (...) effectue, *préalablement au traitement*, une analyse de l'impact des traitements envisagés sur la protection des données à caractère personnel. *Le sous-traitant, sur demande, aide le responsable du traitement à réaliser l'analyse d'impact relative à la protection des données.*
		1bis. Le responsable du traitement consulte le délégué à la protection des données, le cas échéant, lors de la réalisation de l'analyse d'impact relative à la protection des données.

		1bis. Le responsable du traitement consulte le délégué à la protection des données, le cas échéant, lors de la réalisation de l'analyse d'impact relative à la protection des données.
Supprimé	2. Les traitements présentant les risques particuliers visés au paragraphe 1 sont notamment les suivants :	2. Les traitements présentant les risques particuliers visés au paragraphe 1 sont (...) les suivants :
Supprimé	2 (a) l'évaluation systématique et à grande échelle des aspects personnels propres à une personne physique ou visant à analyser ou à prévoir, en particulier, la situation économique de ladite personne physique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement, qui est fondée sur un traitement automatisé et sur la base de laquelle sont prises des mesures produisant des effets juridiques concernant ou affectant de manière significative ladite personne;	2 (a) l'évaluation systématique et à grande échelle des aspects personnels propres à *des* personnes physiques (...), qui est fondée sur *l'établissement de profils* et sur la base de laquelle sont prises des *décisions* produisant des effets juridiques concernant *les personnes concernées* ou affectant gravement *les personnes concernées ;*
Supprimé	2 (b) le traitement d'informations relatives à la vie sexuelle, à la santé, à l'origine raciale et ethnique ou destinées à la fourniture de soins de santé, à des recherches épidémiologiques ou à des études relatives à des maladies mentales ou infectieuses, lorsque les données sont traitées aux fins de l'adoption de mesures ou de décisions à grande échelle visant des personnes précises;	2 (b) le traitement *de données qui révèlent* l'origine raciale ou ethnique, *les opinions politiques, la religion ou les croyances philosophiques, l'appartenance syndicale, ainsi que le traitement de données génétiques ou de données relatives à la santé* ou à la vie sexuelle *ou aux condamnations, aux infractions ou aux mesures de sûreté connexes*, lorsque les données sont traitées aux fins de l'adoption de (...) décisions à grande échelle visant des personnes précises ;
Supprimé	2 (c) la surveillance de zones accessibles au public, en particulier lorsque des dispositifs opto-électroniques (vidéosurveillance) sont utilisés à grande échelle;	2 (c) la surveillance de zones accessibles au public *à grande échelle*, en particulier lorsque des dispositifs opto-électroniques (...) sont utilisés ;
Supprimé	2 (d) le traitement de données à caractère personnel dans des fichiers informatisés de grande ampleur concernant des enfants, ou le traitement de données génétiques ou biométriques;	2 (c) le traitement de données à caractère personnel dans des *systèmes de traitements* de grande ampleur (...) *contenant des données* génétiques ou biométriques.
Supprimé	2 (e) les autres traitements pour lesquels la consultation de l'autorité de contrôle est requise en application à l'article 34, paragraphe 2, point b).	2 (e) les autres traitements *lorsque l'autorité de contrôle compétente estime que le traitement est susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées.*
		2bis. L'autorité de contrôle établit et publie une liste des types de traitements soumis à l'exigence d'une analyse d'impact relative à la protection des données au titre du paragraphe 2, point e). L'autorité de contrôle communique cette liste au Comité européen de la protection des données.

		2ter. Avant d'adopter cette liste, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence prévu à l'article 57 lorsque la liste prévue au paragraphe 2bis comprend des traitements qui sont liés à l'offre de biens ou services à des personnes concernées ou à l'observation de leur comportement dans plusieurs États membres, ou qui sont susceptibles d'affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.
3. L'analyse porte sur la gestion de la totalité du cycle de vie des données à caractère personnel, de la collecte à la suppression, en passant par le traitement. Elle contient au moins: *a) une description systématique des traitements envisagés, les finalités du traitement et, le cas échéant, les intérêts légitimes poursuivis par le responsable du traitement;* *b) une évaluation de la nécessité et de la proportionnalité des traitements au regard des finalités;* *c) une évaluation des risques pour les droits et libertés des personnes concernées, notamment du risque de discrimination inhérent au traitement ou que celui-ci pourrait accentuer;* *d) une description des mesures envisagées pour faire face aux risques et réduire au maximum le volume de données à caractère personnel traité;* *e) une liste des garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel, comme la pseudonymisation, et à apporter la preuve de la conformité avec le présent règlement, en tenant compte des droits et intérêts légitimes des personnes concernées par les données et des autres personnes touchées;* *f) une indication générale des délais impartis pour l'effacement des différentes catégories de données; g) une explication des pratiques de protection des données dès la conception et par défaut visées à l'article 23*[89] *qui ont été mises en oeuvre;* *h) une liste des destinataires ou des catégories de destinataires des données à caractère personnel;* *i) le cas échéant, une liste des transferts de données prévus vers un pays tiers ou une organisation internationale, y compris le nom de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 44, paragraphe 1, point h), les documents attestant l'existence de garanties appropriées;* *j) une évaluation du contexte du traitement des données.*	3. L'analyse contient au moins une description générale des traitements envisagés, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face aux risques, les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité avec le présent règlement, en tenant compte des droits et intérêts légitimes des personnes concernées par les données et des autres personnes touchées.	3. L'analyse contient au moins une description générale des traitements envisagés, une évaluation des risques pour[90] les droits et libertés des personnes concernées, les mesures envisagées pour faire face aux risques, les garanties, mesures de sécurité et mécanismes visant à assurer la protection des données à caractère personnel et à apporter la preuve de la conformité avec le présent règlement, en tenant compte des droits et intérêts légitimes des personnes concernées par les données et des autres personnes touchées.
3 bis. Si le responsable du traitement ou le sous-traitant a désigné un délégué à la protection des données, ce dernier est associé à la procédure d'analyse d'impact.		

[89] *L'article 23 prévoit ainsi, notamment, que « compte étant tenu des techniques les plus récentes, des connaissances techniques actuelles, des meilleures pratiques internationales et des risques représentés par le traitement des données , le responsable du traitement et le sous-traitant éventuel appliquent , tant lors de la définition des objectifs et des moyens de traitement que lors du traitement proprement dit, des mesures et procédures techniques et organisationnelles appropriées et proportionnées, de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée [...] ».*

[90] *Dans la version anglaise du texte, le terme « for » a été remplacé par le terme « to ».*

3 ter. L'analyse est documentée et établit un calendrier des examens périodiques de la conformité de la protection des données, au titre de l'article 33 bis, paragraphe 1. L'analyse est mise à jour sans retard indu si les résultats de l'examen de la conformité de la protection des données visé à l'article 33 bis font apparaître des lacunes. Le responsable du traitement et le sous-traitant ainsi que, le cas échéant, le représentant du responsable du traitement mettent l'analyse à la disposition de l'autorité de contrôle, à la demande de celle-ci.		
Supprimé	4. Le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ni de la sécurité des traitements.	Supprimé
Supprimé	5. Lorsque le responsable du traitement est une autorité ou un organisme publics, et lorsque le traitement est effectué en exécution d'une obligation légale conforme à l'article 6, paragraphe 1, point c), prévoyant des règles et des procédures relatives aux traitements et réglementées par le droit de l'Union, les paragraphes 1 à 4 ne s'appliquent pas, sauf si les États membres estiment qu'une telle analyse est nécessaire avant le traitement.	5. Lorsque le responsable du traitement est une autorité ou un organisme public et lorsque le traitement *conformément à l'article 6, paragraphe 1, point c) ou e) a un fondement légal en vertu du droit de l'Union ou de la législation de l'Etat membre dont relève le responsable du traitement, les paragraphes 1 à 3* ne s'appliquent pas, sauf si les États membres estiment qu'une telle analyse est nécessaire avant le traitement.
Supprimé	6. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères et conditions applicables aux traitements susceptibles de présenter les risques particuliers visés aux paragraphes 1 et 2, ainsi que les exigences applicables à l'analyse prévue au paragraphe 3, y compris les conditions de modularité, de vérification et d'auditabilité. Ce faisant, la Commission envisage des mesures spécifiques pour les micro, petites et moyennes entreprises.	Supprimé
Supprimé	7. La Commission peut définir des normes et procédures pour la réalisation, la vérification et l'audit de l'analyse visée au paragraphe 3. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2.	Supprimé

Article 33 bis Examen de la conformité de la protection des données		
1. Deux ans au plus tard après avoir effectué une analyse d'impact conformément à l'article 33, paragraphe 1, le responsable du traitement ou le sous-traitant agissant pour le compte de ce dernier procède à un examen de conformité. Celui-ci démontre que le traitement des données à caractère personnel est effectué conformément à l'analyse d'impact relative à la protection des données.		
2. L'examen de conformité est réalisé périodiquement, au moins tous les deux ans, ou immédiatement si un changement intervient dans les risques spécifiques présentés par les traitements.		
3. Lorsque les résultats de l'examen de conformité font apparaître des lacunes, l'examen de conformité comporte des recommandations pour y remédier.		
4. L'examen de conformité et ses recommandations sont documentés. Le responsable du traitement et le sous-traitant ainsi que, le cas échéant, le représentant du responsable du traitement mettent l'examen de conformité à la disposition de l'autorité de contrôle, à la demande de celle-ci.		
5. Si le responsable du traitement ou le sous-traitant a désigné un délégué à la protection des données, ce dernier est associé à la procédure d'examen de la conformité.		

ANNEXE 2 : COMMENT UTILISER LES ARBRES DE DÉCISIONS

Les arbres de décisions proposés au Chapitre 2.3 ont été construits pour être imprimés et annotés un crayon à la main. Il s'agit de les parcourir en partant de la question « Quand faire un PIA ? » pour ensuite entourer les propositions qui sont vraies et barrer celles qui sont fausses. Des exemples d'utilisation, en contexte, sont présentés avec les deux études de cas proposées au Chapitre 4.

1. REMARQUES INTRODUCTIVES

Les critères posés par le §(2) de l'article 33 ou le §(2) de l'article 32bis ont été regroupés en trois ou quatre grandes catégories –selon l'article étudié– pour en faciliter la compréhension : « données », « caractéristiques du traitement » et « finalités », dans le cas de l'article 33, auxquels s'ajoute « évènements redoutés », dans le cas du 32bis. Seule la catégorie « données » est sub-divisée en sous-catégories qui sont différenciées en fonction du « verbe » utilisé lorsqu'il est fait référence aux données traitées, à savoir : « sont », « concernent », « révèlent » et « sont relatives à », selon les cas.

Les « losanges » pleins, en couleur, représentent les « critères principaux » qui doivent être satisfaits pour conduire à la réalisation d'un PIA. Les losanges en « pointillés rouges » représentent des « conditions limitantes » qui doivent être satisfaites en complément d'un critère principal.

Dans ce contexte, la lecture visuelle des trois schémas est, en elle-même, éclairante.

En effet, le schéma correspondant au §(2) de l'article 32bis est celui qui contient le plus de catégories, le plus de critères et le moins de « conditions limitantes ». Autrement dit, c'est celui qui décrit le plus de situations conduisant directement à la réalisation d'un PIA.

Ensuite, le schéma correspondant au §(2) de l'article 33, dans sa version initiale proposée par la Commission, propose une vision intermédiaire dans laquelle, seuls trois critères principaux conduisent directement à la réalisation d'un PIA.
Enfin, dans la version du Conseil, tous les critères principaux sauf un sont assortis d'une ou plusieurs conditions limitantes. Cette proposition vise donc, à l'évidence, à limiter les situations nécessitant la réalisation d'un PIA et à éviter le plus possible cette formalité qui peut s'avérer contraignante.

2. EXEMPLE D'UTILISATION

En prenant comme exemple le schéma correspondant au §(2) de l'article 33 dans sa version initiale proposée par la Commission, la première question à se poser concerne l'applicabilité du règlement au regard des articles 2 (champ d'application matériel) et 3 (champ d'application territorial)91. Si le règlement est applicable, il faut continuer à parcourir l'arbre décision. Dans le cas contraire, l'analyse s'arrête là. Le règlement n'est pas applicable au traitement étudié, il n'y a donc pas de PIA à réaliser.

Ensuite, l'arbre de décision conduit aux trois grandes catégories (« données », « caractéristiques du traitement », « finalités ») qui doivent toutes être parcourues, de même que l'ensemble des critères principaux qu'elles contiennent. Ainsi dans la catégorie « données », les questions peuvent être formulées comme indiqué ci-après.

- **Les données traitées « sont »-elles :**
  - « génétiques » ?
  - « biométriques » ?

Si la réponse est positive, alors il faut entourer le critère correspondant, alors qu'une réponse négative conduit à le barrer. En l'absence de critère limitant dans cette sous-catégorie, nous pouvons passer à la sous-catégorie suivante.

- **Les données traitées « concernent »-elles des :**
  - « enfants » ?

Dans l'affirmative, il faut entourer ce critère puis passer à l'évaluation de la « condition limitante » qui le suit :

- les données traitées, sont-elles contenues dans des fichiers informatisés de grande ampleur ?

À ce stade, la notion de « grande ampleur » n'est pas explicitement définie et le législateur européen devra sans doute apporter des précisions. S'agit-il de la population d'une nation, d'une région, d'une ville ? Si ce critère limitant n'est manifestement pas satisfait dans le cas étudié, alors il faut le barrer et passer à la suite.

À la fin de l'analyse, tous les critères principaux de l'arbre de décision doivent être soit entourés soit barrés. Trois situations peuvent alors se présenter :

1. Tous les critères principaux sont barrés.

Alors le traitement étudié ne nécessite pas de réaliser un PIA. Dans ce cas, la case « PIA » rouge (en bas à droite de l'arbre de décision) peut elle-même être barrée. Seule reste alors comme possibilité le groupe « autres formalités » qui peut être entouré et qui correspond au résultat de cette analyse.

2. Un ou plusieurs critères principaux sont entourés.

Cette condition seule n'est pas suffisante. Il faut en complément que les critères principaux concernés soient « isolés » ou que toutes les « conditions limitantes » qui les suivent soient également entourées pour que le traitement étudié nécessite la réalisation d'un PIA. Dans ce cas, le « PIA » rouge (en bas à droite de l'arbre de décision) peut lui-même être entouré et le groupe « autres formalités » peut quant à lui être barré. Ici, le résultat de l'analyse est donc la réalisation d'un PIA (il pourra être suivi d'autres formalités).

3. Dans toutes les autres situations, un PIA n'est pas requis et la case « PIA » rouge (en bas à droite de l'arbre de décision) peut être barrée. Seule reste alors comme possibilité le groupe « autres formalités » qui peut être entouré et qui correspond au résultat de cette analyse.

GLOSSAIRE

Le tableau ci-dessous reprend les définitions issues de la proposition initiale de règlement général sur la protection des données, des propositions d'amendements du Parlement européen et du texte issu du Conseil de l'Union européenne[92].

Terme	Propositions du Parlement européen (mars 2014) [93]	Propositions de la Commission européenne (janvier 2012) [94]	Propositions issues du Conseil de l'Union européenne (juin 2014) [95]
Autorité de contrôle	Identique à la proposition de la Commission européenne	Une autorité publique qui est instituée par un État membre conformément aux dispositions de l'article 46 de la proposition de règlement général sur la protection des données.	Une autorité publique *indépendante qui* est instituée par un Etat membre *en application de* l'article 46 de la proposition de règlement général sur la protection des données.
Consentement de la personne concernée	Identique à la proposition de la Commission européenne	Toute manifestation de volonté, libre, spécifique, informée et explicite par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement.	Toute manifestation de volonté, libre, spécifique et informée (...) par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement.
Destinataire	Identique à la proposition de la Commission européenne	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel.	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme *autre que la personne concernée, le responsable du traitement ou le sous-traitant*, qui reçoit communication de données à caractère personnel ; *cependant, les organismes de réglementation et les autorités susceptibles de recevoir des données à caractère personnel dans l'exercice de leurs fonctions officielles ne sont pas considérés comme des destinataires.*
Donnée à caractère personnel	Toute information se rapportant à *une personne physique identifiée ou identifiable (la «personne* concernée»); *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, par exemple à un nom, à un numéro d'identification, à des données de localisation, à un identifiant unique ou à un ou plusieurs éléments spécifiques, propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle, sociale ou de genre de cette personne.*	Toute information se rapportant à une personne concernée.	Toute information se rapportant à *une personne physique identifiée ou identifiable* (la « personne concernée ») ; *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, (...), notamment par référence à un identifiant, par exemple à un nom, à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne.*

[92] Le texte en italique correspond aux ajouts ou modifications apportés au texte de la Commission européenne. Les parties de texte supprimées sont indiquées comme suit : (...).
[93] Résolution législative du Parlement européen du 12-3-2014.
[94] Proposition Règl. CE du 25-1-2012 art. 4.
[95] Note from the President of the Council of the European Union dated 30-6-2014. Traduction libre par le cabinet ALAIN BENSOUSSAN AVOCATS.

Données biométriques	Toutes les données à caractère personnel relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques.	Toutes les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques.	Toutes 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* l'identification unique *de cette personne physique*, telle que des images faciales ou des données dactyloscopiques.
Données concernant la santé	*Toutes données à caractère personnel* relatives à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne.	Toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne.	*Données liées* à la santé physique ou mentale d'un individu, *qui révèlent des informations concernant son état de santé.*
Données génétiques	Toutes les données *à caractère personnel liées aux* caractéristiques génétiques d'une personne physique qui sont héréditaires ou *ont été* acquises, *résultant d'une analyse d'un échantillon biologique de la personne en question, notamment par une analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou d'une analyse de tout autre élément permettant d'obtenir des informations équivalentes.*	Toutes les données, de quelque nature que ce soit, concernant les caractéristiques d'une personne physique qui sont héréditaires ou acquises à un stade précoce de son développement prénatal.	Toutes les données *à caractère personnel liées aux* caractéristiques *génétiques* d'une personne physique qui sont héréditaires ou *ont été acquises, résultant d'une analyse d'un échantillon biologique de la personne en question.*
Données pseudonymes	*Données à caractère personnel qui ne peuvent pas être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que de telles informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution.*		
Données cryptées	*Données à caractère personnel qui sont rendues inintelligibles par des mesures de protection technologique pour toute personne qui n'est pas autorisée à y avoir accès.*		
Enfant	Identique à la proposition de la Commission européenne	Toute personne âgée de moins de dix-huit ans.	Supprimé
Entreprise	Identique à la proposition de la Commission européenne	Toute entité exerçant une activité économique, quelle que soit sa forme juridique, y compris, notamment, les personnes physiques et morales, les sociétés de personnes ou les associations qui exercent régulièrement une activité économique.	Toute *personne physique ou morale* exerçant une activité économique, quelle que soit sa forme juridique (...) y compris (...) les sociétés de personnes ou les associations qui exercent régulièrement une activité économique.

Etablissement principal	Le lieu de l'établissement *de l'entreprise ou du groupe d'entreprises* dans l'Union, *qu'il s'agisse du responsable du traitement ou du sous-traitant*, où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement de données à caractère personnel. *Il peut être notamment tenu compte des critères objectifs suivants: la localisation du siège du responsable du traitement ou du sous-traitant; la localisation de l'entité au sein du groupe d'entreprises qui est la mieux placée en termes de fonctions de direction et de responsabilités administratives pour s'occuper des règles exposées dans le présent règlement et les faire appliquer; la localisation où les activités effectives et réelles de direction sont exercées, et qui déterminent le traitement des données dans le cadre d'une installation stable.*	- En ce qui concerne le responsable du traitement, le lieu de son établissement dans l'Union où sont prises les principales décisions quant aux finalités, aux conditions et aux moyens du traitement de données à caractère personnel ; si aucune décision de ce type n'est prise dans l'Union, l'établissement principal est le lieu où sont exercées les principales activités de traitement dans le cadre des activités d'un établissement d'un responsable du traitement dans l'Union ; - En ce qui concerne le sous-traitant, on entend par «établissement principal» le lieu de son administration centrale dans l'Union.	- En ce qui concerne un responsable du traitement *disposant d'établissements dans plus d'un État membre*, le lieu de son *administration centrale* dans l'Union, à moins que les (...) décisions quant aux finalités (...) et aux moyens du traitement de données à caractère personnel *ne soient prises dans un autre établissement du responsable du traitement dans l'Union. Dans ce cas, l'établissement ayant pris ces décisions est considéré comme établissement principal.* Si aucune décision de ce type n'est prise dans l'Union, (...) l'établissement du responsable du traitement dans l'Union où sont exercées les principales activités de traitement (...) ; - En ce qui concerne *un* sous-traitant *disposant d'établissements dans plus d'un État membre*, le lieu de son administration centrale dans l'Union européenne, *et, s'il n'a pas d'administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où sont exercées les principales activités de traitement dans le cadre des activités d'un établissement d'un sous-traitant ;* *- Lorsque le responsable du traitement exerce également des activités en tant que sous-traitant, l'établissement principal du responsable du traitement est considéré comme l'établissement principal pour le contrôle des activités de traitement.* *- Lorsque le traitement est effectuée par un groupe d'entreprises, l'établissement principal de l'entreprise qui exerce le contrôle est considéré comme l'établissement principal du groupe d'entreprises, à moins que les décisions quant aux finalités et aux moyens du traitement ne soient prises par une autre entreprise.*
Fichier	Identique à la proposition de la Commission européenne	Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.	Identique à la proposition de la Commission européenne

GLOSSAIRE

Groupe d'entreprises	Identique à la proposition de la Commission européenne	Une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle.	Identique à la proposition de la Commission européenne
Limitation du traitement			*Le marquage de données à caractère personnel mises en mémoire, en vue de limiter leur traitement futur.*
Personne concernée	Identique à la proposition de la Commission européenne	Personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.	Identique à la proposition de la Commission européenne
Profil			*Ensemble de données qui caractérise une catégorie de personnes physiques et qui est destiné à être appliqué à une personne physique.*
Profilage	*Toute forme de traitement automatisé de données à caractère personnel destiné à évaluer certains aspects personnels propres à une personne physique ou à analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement.*		*Une forme de traitement automatisé de données à caractère personnel destiné à utiliser un profil pour évaluer les aspects personnels propres à une personne physique, en particulier pour analyser et prévoir des aspects concernant le rendement professionnel de celle-ci, sa situation économique, son état de santé, ses préférences personnelles, ou ses centres d'intérêts, sa fiabilité ou son comportement, sa localisation ou ses déplacements.*
Pseudonymisation			*Le traitement de données à caractère personnel de manière à ce que les données ne puissent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que de telles informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution.*

Règles d'entreprise contraignantes	Identique à la proposition de la Commission européenne	Les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre de l'Union, aux transferts ou à un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises;	Les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre de l'Union, aux transferts ou à un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises *ou un groupe d'entreprises exerçant une activité économique commune*.
Représentant	Toute personne physique ou morale établie dans l'Union expressément désignée par le responsable du traitement, qui représente ce dernier, en ce qui concerne les obligations du responsable du traitement en vertu du présent règlement.	Toute personne physique ou morale établie dans l'Union expressément désignée par le responsable du traitement, qui agit en lieu et place de ce dernier et peut être contactée à sa place par les autorités de contrôle et d'autres entités dans l'Union, en ce qui concerne les obligations du responsable du traitement en vertu du présent règlement.	Toute personne physique ou morale établie dans l'Union, (...) désignée *par écrit* par le responsable du traitement *conformément à l'article 25*, qui *représente* ce dernier en ce qui concerne les obligations du responsable du traitement en vertu du présent règlement (...).
Responsable du traitement	Identique à la proposition de la Commission européenne	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités, les conditions et les moyens du traitement de données à caractère personnel ; lorsque les finalités, les conditions et les moyens du traitement sont déterminés par le droit de l'Union ou la législation d'un État membre, le responsable du traitement peut être désigné, ou les critères spécifiques applicables pour le désigner peuvent être fixés, par le droit de l'Union ou par la législation d'un État membre.	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités (...) et les moyens du traitement de données à caractère personnel ; lorsque les finalités (...) et les moyens du traitement sont déterminés par le droit de l'Union ou la législation d'un Etat membre, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit de l'Union ou par la législation d'un Etat membre.
Sous-traitant	Identique à la proposition de la Commission européenne	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.	Identique à la proposition de la Commission européenne

Tiers	*Toute personne physique ou morale, autorité publique, service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données.*		
Traitement de données à caractère personnel	Identique à la proposition de la Commission européenne	Toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et appliquée(s) à des données à caractère personnel, telle(s) 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, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que l'effacement ou la destruction.	Toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et appliquée(s) à des données à caractère personnel, telle(s) 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 (...) ainsi que l'effacement.
Violation de données à caractère personnel	La destruction, la perte, l'altération, la divulgation ou la consultation non autorisées, de manière accidentelle ou illicite, de données à caractère personnel transmises, conservées ou traitées d'une autre manière	Une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière.	Identique à la proposition de la Commission européenne

BIBLIOGRAPHIE INDICATIVE

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 oeuvre 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).

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.

BIBLIOGRAPHIE INDICATIVE

3. TRAVAUX DES AUTORITÉS DE PROTECTION DES DONNÉES

- Guide gérer les risques sur les libertés et la vie privée Cnil 6-2012.

- 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.

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.

- Report from the Cabinet Office of the United Kingdom's Government dated 6-2008 regarding Data Handling Proc dures in Government.

- www.piawatch.eu

L'Académie est une initiative de l'Ordre des Experts-Comptables

GOUVERNANCE DES DONNEES PERSONNELLES ET ANALYSE D'IMPACT

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

Nicole POWILEWICZ
Directeur Délégué
npowilewicz@lacademie.info

Marie-Claude PICARD
Chargée de Mission
mcpicard@lacademie.info