SIMONT
BRAUN

GENERAL DATA PROTECTION REGULATION 2016

Quelles obligations prévoit le projet de règlement européen sur les données personnelles (GDPR) ?

Par Benjamin Docquir, associé, Simont Braun

Au sein de l'Union européenne, les règles sur le traitement des données à caractère personnel étaient régies par la directive 1995/46/CE. Conçue à une époque antérieure à celle des réseaux sociaux, du *big data* et de l'Internet des objets, cette réglementation était souvent incomprise et mal appliquée par les entreprises et les organisations. Sa révision était à l'ordre du jour depuis 2012. Après plusieurs années d'intenses discussions, un texte final a enfin été adopté en décembre 2015 [1] et il devrait être voté par le législateur de l'Union puis publié au Journal Officiel dans les prochaines semaines.

La modernisation du régime de la protection des données à caractère personnel, devrait avoir des conséquences pratiques importantes pour la plupart des entreprises et des organisations. En particulier, ceux qui, au sein de ces organisations, sont chargés de veiller au respect de la réglementation, se verront confrontés à des défis nouveaux présentant de multiples facettes. Il ne s'agit pas uniquement d'appliquer de nouvelles dispositions légales, d'effectuer de nouvelles démarches administratives voire d'adapter la formulation de certaines clauses de conditions générales ou de politiques de confidentialité. Les exigences du règlement, principalement à travers la notion dite de « *accountability* » qui sera examinée ci-après, vont bien au-delà.

Dans ce document, nous tentons de donner un aperçu suffisamment complet de ces nouvelles obligations, mais aussi des pouvoirs nouveaux qui seront attribués au régulateur, au plan national et au plan européen, pouvoirs qui pourront se traduire par des enquêtes et des mesures d'investigation, des injonctions positives et même des amendes administratives d'un niveau potentiellement assez élevé.

Pour illustrer les ambitions que suscite cette réforme, je reprends le propos de deux contributeurs lors d'un récent colloque sur le sujet : « *peering into the future of privacy does not only mean complying with the forthcoming EU legal framework, it means moving from a data controller's'wait and see' compliance to a proactive and creative accountability that puts users at the centre of their own digital experience* »[2]. Et les

[1] Le 15 décembre 2015, un accord a été trouvé au sein des institutions européennes sur un texte de compromis qui devrait être soumis au vote du Parlement et publié au début de l'année 2016. Ce texte est disponible à l'adresse suivante : http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf.
[2] F. Lhemery, M.C. Roques-Bonnet, « Peering into the future of privacy », in a. Grosjean (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2014, pp. 429-440.

auteurs de ces lignes ne sont pas membres d'un régulateur : ils sont respectivement *Senior Director Public Policy* et *Director of EMEA privacy policy* chez Microsoft EMEA. C'est dire à quel point l'on appelle à une transformation de la façon dont les règles de protection des données personnelles sont perçues et appliquées généralement par les entreprises et les organisations.

En résumé, il s'agit de faire de la protection des données personnelles une préoccupation de même nature que celle du respect de l'environnement ou de la promotion du commerce équitable, en d'autres termes l'un des éléments de la responsabilité sociale de l'entreprise[3]. Satisfaire aux exigences du règlement sur la protection des données demandera dès lors un effort interdisciplinaire, nécessitera de mobiliser différents profils à travers une grande variété de fonctions au sein de l'entreprise.

Le règlement européen tend en effet à aborder la protection des données personnelles non plus seulement sous un angle strictement juridique ou administratif (à travers les déclarations préalables), mais également en tenant compte de l'impact concret que des décisions stratégiques, opérationnelles et en matière de sécurité peuvent avoir pour la protection des données au sein d'une entreprise ou d'une organisation.

Nous examinerons d'abord brièvement le processus d'adoption du règlement (1). Nous poursuivrons avec un aperçu des mécanismes de contrôle et de sanction que ce règlement consacrera (2), et qui par le renforcement des pouvoirs des autorités de contrôle indépendantes auront un impact significatif pour les entreprises. Nous insisterons ensuite sur la notion nouvelle de responsabilité ou « accountability », qui est au cœur des nouvelles obligations imposées par le règlement et qui implique notamment une évaluation des risques liés aux traitements de données en fonction des circonstances concrètes (3). Nous pourrons ensuite étudier quelques-unes des nouvelles obligations substantielles qui s'imposent au responsable du traitement ainsi qu'aux sous-traitants dans le régime mis en place par le futur règlement (4).

1. Statut du règlement et de son adoption

Jusqu'à l'adoption d'un texte de compromis le 15 décembre 2015[4], le processus d'élaboration du règlement européen a été jalonné par trois étapes importantes : (i) adoption de la proposition de la Commission en janvier 2012, (ii) vote par le Parlement, en première lecture, le 12 mars 2014, du rapport de la Commission Libertés civiles, Justice et Affaires intérieures, et enfin (iii) adoption par le Conseil d'une « approche générale » le 11 juin 2015[5]. Dans les lignes qui suivent, nous nous appuyons essentiellement sur cette « approche générale », qui prend certaines distances avec la proposition de la Commission et les amendements du Parlement. Nous indiquerons ici et là, sans exhaustivité, certains des points qui ont fait l'objet d'un arbitrage dans le texte de compromis disponible depuis ce 16 décembre 2015.

Le 25 janvier 2012, la Commission publiait officiellement sa proposition de règlement du Parlement européen et du conseil concernant la protection des individus à l'égard du traitement de données à caractère personnel et la libre circulation de ces données[6]. Cette proposition ambitieuse, composée de 138 considérants et de 91 articles, était le résultat d'un long travail d'évaluation de la directive 95/46. Celle-ci, bien qu'elle avait le mérite indéniable de consacrer un certain nombre de principes essentiels pour la

[3] G. Lommel, « Company's liability regarding new technologies », in A. Grosjean (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2014, pp. 373-378 ; L. Moerel, *Binding Corporate Rules*, *Corporate Self-Regulation of Global Data Transfers*, Oxford University Press, 2012, spéc. chap. 9, pp. 175-227.
[4] Voy. note 1 ci-avant.
[5] Nous invitons le lecteur à consulter la page suivante : https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/Consultation/Reform_package, où il aura accès à ces trois textes intermédiaire, ainsi qu'à des outils de comparaison entre les différentes versions.
[6] COM(2012) 11 final - 2012/0011 (COD), 25 janvier 2012.

protection des données, était généralement considérée comme insuffisante au regard des développements technologiques récentes, et elle faisait par ailleurs l'objet de critiques en raison du niveau d'harmonisation jugé faible auquel elle était parvenue. Les Etats membres avaient en effet procédé à une harmonisation qui, sur bien des points, différait sensiblement d'un pays à l'autre, en particulier en ce qui concerne les mécanismes de contrôle et de sanction.

Après un intense travail législatif et le dépôt de très nombreux amendements, le Parlement européen adoptait, le 12 mars 2014, le rapport de la Commission Libertés civiles, Justice et Affaires intérieures qui avait été voté en commission le 21 octobre 2013.

Parallèlement, depuis le dépôt de la proposition de la Commission, le Conseil avait développé sa propre approche de la réforme. Ceci a culminé dans l'adoption, le 15 juin 2015, d'une « approche générale ». Celle-ci ne constituait pas encore la position formelle du Conseil, mais plutôt un document informel qui a servi de base à des négociations avec le Parlement et l'assistance de la Commission.

Dans le respect des dispositions du traité, cette approche générale, après adoption d'un texte de compromis entre les institutions concernées, fera l'objet d'une adoption en première lecture par le Conseil puis d'une adoption en seconde lecture par le Parlement, avant l'adoption formelle et définitive du règlement, dans les premiers mois de 2016.

Ce processus d'élaboration explique que le statut de certaines dispositions du règlement est demeuré incertain tout au long du processus de discussion du texte. En effet, alors que le Parlement a adopté des amendements sur la base du texte de la Commission, l'approche générale adoptée par le Conseil prend, elle aussi, pour base le texte de la Commission, sans tenir compte des amendements adoptés par le Parlement. Dès lors, sur un certain nombre de questions, parfois fort importantes, on est demeuré dans l'expectative jusqu'à l'adoption du texte de compromis de décembre 2015.

Il en va notamment ainsi de la question des données pseudonymes. En effet, le Parlement avait proposé d'alléger certaines obligations en cas de traitement de données qui ne permettent pas l'identification directe des individus, lorsque les garanties appropriées sont mises en œuvre pour empêcher cette identification. L'approche générale du Conseil ne s'inscrivait pas dans la même démarche mais proposait d'autres voies et moyens. Il demeurait donc de nombreuses incertitudes quant au contenu des futures règles applicables dans des contextes de *data mining* ou *big data*, et globalement de *business intelligence* au sein des entreprises. Il semble que dans le texte de compromis du 15 décembre 2015, ce soit l'approche du Conseil qui prévale : le profilage en tant que tel, qui implique une possibilité de prendre de façon automatisée des décisions affectant les individus, fait l'objet d'une interdiction spécifique, sauf l'accord des personnes concernées (article 20).

Tel est aussi le cas, par exemple, en ce qui concerne l'exigence d'un consentement par écrit. Alors que la Commission et le Parlement semblaient insister sur la nécessité que le consentement de la personne concernée soit toujours exprimé par écrit, le Conseil renonçait à cette exigence dans son approche générale, tout en veillant à préserver autrement les droits des individus concernés. Le texte de compromis du 15 décembre maintient cette exigence d'un consentement « non ambigu » sans imposer un accord explicite dans tous les cas (hors le cas des données sensibles).

Un autre exemple concerne le statut du détaché à la protection des données. Alors que le texte adopté par la Commission ainsi que par le Parlement prennent chacun position de façon claire sur le seuil minimum qui déclenche l'obligation de désigner un détaché à la protection des données, l'approche générale du Conseil de juin 2015 s'en tenait à une prudence diplomatique et se contentait de prévoir que le responsable du

traitement est obligé de désigner un détaché à la protection des données « lorsque le droit de l'Union ou le droit d'un Etat membre l'impose ». Les compétences et connaissances dont devrait disposer ce détaché à la protection des données ne sont pas davantage fixées, en dépit de la tentative du Parlement d'imposer un « profil de fonction » particulièrement exigeant[7].

En définitive, dans le texte de compromis du 15 décembre 2015, l'obligation de désigner un détaché à la protection des données s'impose aux autorités publiques et aux situations dans lesquelles les « activités principales » (*« core activities* ») du responsable ou du sous-traitant requièrent, en raison de leur nature, de leur portée ou de leurs finalités, une « surveillance » (« *monitoring* ») régulière et systématique des personnes concernées à grande échelle, ou impliquent le traitement à grande échelle de données sensibles[8].

Le règlement deviendra applicable deux ans après la date de son entrée en vigueur, qui dépendra de celle de sa publication au journal officiel de l'Union européenne[9].

Les entreprises et organisations devront donc dans ce délai prendre des mesures pour se conformer à la réglementation future, tout en veillant à continuer à se conformer au cadre juridique issu de la directive 95/46.

Dans les lignes qui suivent, nous nous appuierons essentiellement sur le contenu du texte de compromis de décembre 2015, tout en faisant écho, lorsque cela nous paraît nécessaire ou utile, aux positions exprimées antérieurement dans la proposition de la Commission, dans les amendements adoptés par le Parlement européen ou dans l'approche générale du Conseil.

2. Des principes (1995) … à leur mise en œuvre concrète (2015)

En dépit des incertitudes liées au processus d'élaboration du texte, l'une des inspirations fondamentales du règlement européen tient à la volonté de ses auteurs de mettre en place des règles permettant d'assurer une plus grande effectivité de la protection des données personnelles.

Cette effectivité accrue passe certes par un renforcement du contrôle de la part des autorités de régulation, qui disposeront de compétences élargies. La Charte des droits fondamentaux de l'Union européenne dispose en effet en son article 8 que le respect des règles de protection des données personnelles doit être « *soumis au contrôle d'une autorité indépendante* ».

Mais elle nécessite également que des sanctions puissent être prononcées et que des recours puissent être exercés contre les responsables de traitement ne se conformant pas au règlement. En définissant à cet égard des règles uniformes, le règlement réalise un niveau élevé d'harmonisation du droit et crée les conditions de possibilité de mécanismes de sanction et de contrôle effectifs.

Pour autant, l'on aurait tort d'envisager le règlement uniquement comme un nouvel instrument de contrôle, un arsenal de mesures contraignantes au service de futurs « gendarmes de la vie privée » que seraient les autorités de contrôle. En effet, l'exigence d'un contrôle indépendant ne va pas nécessairement de pair avec une vision antagoniste des rôles respectifs du contrôleur (CPVP, CBP, CNIL, etc.) et du contrôlé (le responsable du traitement et, bientôt, le sous-traitant également).

[7] Voy. le considérant 75a du texte adopté par le Parlement.
[8] Voy. l'article 35 du texte de compromis.
[9] Voy. l'article 91 du texte de compromis.

A l'instar de l'approche développée par plusieurs autorités nationales de contrôle, dont la Commission belge de la protection de la vie privée ces dernières années, il est en effet possible de voir la « compliance » comme étant non pas une gestion préventive du risque lié à la non-conformité, mais plutôt un dialogue constructif et évolutif entre le régulateur et les acteurs du secteur[10]. En un sens, le règlement invite à un tel dialogue : s'il conduit les entreprises et organisations à s'impliquer davantage de façon active dans la définition et la mise en œuvre de mesures concrètes pour renforcer la protection des données, il confie aussi aux autorités de contrôle des responsabilités et des pouvoirs importants, dont l'exercice imposera de comprendre et d'identifier les contraintes liées à des situations ou des secteurs spécifiques, pour définir, dans l'échange et le dialogue, les outils de mise en conformité les plus appropriés.

On ne peut en tout cas qu'espérer que dans la pratique, la recherche de la *compliance* s'apparente, fût-ce de loin, à un tel cercle vertueux…

Avant d'examiner plus en détail les dispositions du futur règlement consacrées aux autorités de contrôle et à leurs pouvoirs, il n'est pas inutile de rappeler brièvement l'état du droit belge à cet égard.

2.1. Les carences de la situation actuelle en Belgique

La directive 95/46 envisageait la question du contrôle et des sanctions en cas de non-respect de ses dispositions, à travers deux mécanismes distincts : d'une part, des recours juridictionnels devant les tribunaux nationaux et, d'autre part, la consécration dans le chef d'une autorité de contrôle indépendante, d'un certain nombre de pouvoirs d'investigation, d'intervention et d'action en justice.

Les Etats membres étaient ainsi tenus de mettre en œuvre des recours juridictionnels en cas de violation des droits garantis par les dispositions nationales transposant la directive (article 22). Ils devaient également permettre à toute personne ayant subi un dommage en raison d'un traitement illicite ou d'une action non conforme aux dispositions de la directive, d'obtenir du responsable du traitement la réparation du préjudice subi (article 23). Enfin, les Etats membres devaient prendre les mesures appropriées et déterminer notamment les sanctions à appliquer en cas de violation des dispositions de la directive (article 24).

En outre, les Etats membres devaient consacrer l'existence d'une autorité de contrôle indépendante, chargée de surveiller l'application, sur leur territoire, des dispositions transposant la directive (article 28). Outre un rôle consultatif lors de l'élaboration de mesures réglementaires ou administratives en la matière, ces autorités de contrôle devaient notamment disposer de pouvoirs d'investigation, de « *pouvoirs effectifs d'intervention* » et du pouvoir soit d'intenter elles-mêmes une action justice en cas de violation des dispositions nationales de transposition de la directive, soit de porter ces violations la connaissance de l'autorité judiciaire.

En ce qui concerne les pouvoirs dont est dotée la Commission pour la protection de la vie privée en Belgique, force est de constater que le législateur avait opté pour une transposition *a minima* de l'article 28. Tout d'abord, si elle dispose en théorie des pouvoirs d'investigation relativement étendus prévus à l'article 32 de la loi du 8 décembre 1992, la Commission n'en fait pas un usage très régulier ni très poussé dans la pratique. Plus fondamentalement, alors que cette possibilité est expressément envisagée par le texte de la directive, la Commission belge n'a pas le pouvoir effectif d'intervenir préalablement à la mise en œuvre d'un traitement, ni d'ordonner « *le verrouillage, l'effacement ou la destruction de données* » ni encore « *d'interdire temporairement ou définitivement un traitement* » (article 28 (3), de la directive 95/46). Contrairement à

[10] S. Nerbonne, « Le nouveau rôle des autorités de contrôle », in A. Grosjean (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2014, pp. 379-394.

d'autres Etats membres, le droit belge ne permet pas non plus à la Commission de la protection de la vie privée d'imposer des sanctions administratives ou financières aux responsables de traitement.

La faiblesse relative des moyens dont se voit dotée l'autorité belge de contrôle de la protection des données, a d'ailleurs été plusieurs fois dénoncée par la doctrine.

2.2. Les nouveaux pouvoirs de contrôle et de sanction dans le futur règlement

Devant un tel état de fait, nul doute que l'entrée en vigueur du règlement entraînera en Belgique une nécessaire adaptation des pratiques de bien des entreprises et organisations. Celles-ci seront en effet confrontées à une nouvelle autorité de contrôle, dotée de pouvoirs plus importants, et à un corps de règles uniformisées sur le plan européen et assorties de sanctions très concrètes.

2.2.1. Les nouvelles autorités de contrôle et leurs pouvoirs

A. Généralités

Selon l'article 46 du règlement, chaque Etat membre doit désigner une ou plusieurs autorités publiques indépendantes, chargées de surveiller l'application du règlement et de veiller à l'application cohérente de ces règles à travers l'Union européenne. Lorsqu'un Etat membre désigne plusieurs autorités de contrôle, seule l'une d'entre elles devra être habilitée à représenter les autres au sein du conseil européen de la protection des données, et les mécanismes nécessaires devront être mis en œuvre en droit interne pour veiller au respect, par les autres autorités, des règles de coopération visées à l'article 57 du règlement (voyez ci-après). Chaque Etat membre doit, aux plus tard deux ans après l'entrée en vigueur du règlement, informer la Commission des dispositions de droit national adoptées à ce sujet.

Le règlement consacre par ailleurs le principe d'indépendance des autorités de contrôle, réglemente les conditions d'éligibilité de leurs membres et précise les règles essentielles de leur fonctionnement. Il entérine également le principe du secret professionnel (article 47 à 50).

L'article 47 du règlement, relatif à l'indépendance de l'autorité de contrôle, ne consacre pas uniquement le principe en des termes généraux. Il dispose que l'autorité de contrôle doit agir avec une complète indépendance dans l'exercice de ses devoirs et de ses compétences, et que les membres de cette autorité doivent demeurer libres de toute influence extérieure directe ou indirecte et qu'ils ne peuvent ni rechercher ni recevoir des instructions de quiconque. Mais en outre, le règlement oblige les Etats membres à faire en sorte que chaque autorité de contrôle dispose des moyens humains, techniques et financiers ainsi que des locaux et de l'infrastructure nécessaires pour pouvoir exercer effectivement leurs devoirs et leurs compétences, qu'elle soit dotée d'une équipe propre soumise à la direction des membres de l'autorité de contrôle et que chaque autorité de contrôle soit directement soumise à un contrôle financier qui ne mette pas à mal son indépendance. Les Etats membres devront ainsi s'assurer que chaque autorité de contrôle dispose d'un budget annuel distinct, public et qui peut faire partie du budget national ou fédéral. La proposition du Parlement précisait que chaque Etat membre devait faire en sorte que l'autorité de contrôle soit responsable envers le Parlement national pour des raisons de contrôle budgétaire. Le texte de compromis ne reprend pas cette précision, qui ne figurait pas non plus dans la proposition de la Commission.

Les membres de chaque autorité de contrôle devront être désignés au moyen d'une procédure transparente soit par le parlement, le gouvernement ou le chef d'un Etat membre, soit par un organisme indépendant chargé en vertu du droit national de procéder à cette désignation. (Cette dernière possibilité a été ajoutée au stade de l'approche générale du Conseil et reprise dans le texte de compromis). Les membres de l'autorité de contrôle doivent disposer des qualifications, de l'expérience et des connaissances nécessaires pour exercer leurs missions. Les devoirs des membres de l'autorité prendront fin à l'expiration de leur mandat, en cas de démission ou de retraite obligatoire en vertu du droit national. Les membres peuvent également être révoqués ou privés de leur droit à une pension ou à d'autres avantages par un tribunal national compétent, s'ils ne remplissent plus les conditions requises pour l'exercice de leurs devoirs ou s'ils se rendent coupables de malversations sérieuses. Le membre dont le mandat arrive à échéance ou qui démissionne de ses fonctions, continuera à exercer ses fonctions jusqu'à la désignation d'un nouveau membre. Les membres et le personnel de chaque autorité de contrôle seront, conformément au droit de l'Union ou de l'Etat membre concerné, soumis au secret professionnel, et ce aussi bien pendant qu'après l'expiration de leur mandat, à l'égard de toute information confidentielle dont ils ont pris connaissance à l'occasion de l'exercice de leurs devoirs et dans l'exercice de leurs compétences.

Chaque Etat membre devra en outre prévoir dans son droit interne le principe de l'établissement de chaque autorité de contrôle, et réglementer un ensemble de questions : les qualifications requises pour exercer les fonctions de membre de l'autorité de contrôle, les règles et procédures applicables pour la désignation des membres, la durée des mandats et le nombre possible de renouvellement le cas échéant, ainsi que l'ensemble des obligations incombant aux membres et aux personnels de l'autorité de contrôle, les règles d'incompatibilité et les règles régissant la résiliation de leur contrat. On notera que le mandat des membres de l'autorité de contrôle ne peut être d'une durée inférieure à quatre ans (sauf lors de leur premier mandat après l'entrée en vigueur du règlement si cela est nécessaire pour protéger l'indépendance de l'autorité de contrôle au moyen d'une procédure de désignation par étapes).

B. Tâches des autorités de contrôle

Les tâches dévolues aux autorités de contrôle, énumérées à l'article 52 du règlement, sont nombreuses et variées. On peut notamment distinguer, à côté de certaines tâches générales, le traitement et la gestion des plaintes et l'exécution d'un certain nombre de dispositions du règlement.

On remarquera que selon l'article 53 (5) du règlement (position du Conseil en juin 2015), l'exercice des tâches dévolues aux autorités de contrôle ne peut entraîner de coûts à charge du de la personne concernée ni, le cas échéant, du détaché à la protection des données. Cette disposition a toutefois disparu du texte de compromis du 15 décembre 2015.

C. Tâches générales

Les autorités doivent notamment surveiller et veiller à l'application du règlement, promouvoir une meilleure connaissance et compréhension des risques, des règles, des mesures de précaution et des droits des individus à l'égard des traitements de données à caractère personnel. Elles doivent assister le législateur et les autres organismes publics quant aux mesures législatives et administratives concernant la protection des droits et libertés des individus à l'égard des traitements de données personnelles. Elles doivent promouvoir la connaissance par les responsables et le sous-traitant de leurs obligations en vertu du règlement. Elles doivent, sur requête, donner des informations aux individus en ce qui concerne l'exercice de leurs droits et, le cas échéant, coopérer à cette fin avec les autorités de contrôle dans d'autres Etats membres.

D'une manière générale, elles doivent coopérer avec les autres autorités de contrôle afin d'assurer l'application cohérente du règlement. Elles doivent mener des enquêtes sur l'application du règlement, notamment sur la base d'informations reçues d'autres autorités de contrôle ou d'autres organismes publics. Elles doivent surveiller les développements pertinents, notamment le développement des techniques d'information et de communication et des pratiques commerciales, qui peuvent avoir un impact sur la protection des données personnelles. Enfin, elles doivent participer aux activités du conseil européen de la protection des données et remplir toutes les autres tâches qui concernent la protection des données à caractère personnel.

D. Traitement des plaintes

Les autorités de contrôle sont chargées de traiter les plaintes qui leur sont soumises par un individu, un organisme ou une association représentative (voy. ci-après : l'article 76[11] du règlement donne un droit d'action en justice à des associations constituées à cette fin) ; les autorités doivent instruire l'objet de la plainte et informer le plaignant de l'évolution de leurs investigations et de leurs résultats, dans un délai raisonnable, en particulier si des investigations complémentaires ou une coordination avec une autre autorité de contrôle s'avèrent nécessaires. Les autorités doivent faciliter le dépôt de plainte par les personnes concernées, notamment par l'établissement de formulaires types de plaintes, pouvant être complétés de façon électronique ou par tout autre moyen de communication.

E. Exécution de dispositions particulières du règlement

Les autorités de contrôle sont également chargées de l'exécution concrète d'un certain nombre de dispositions du règlement, notamment les clauses contractuelles standard entre le responsable et le sous-traitant (article 26 (2c)), les exigences minimales pour les études d'impact préalable (article 33 (2a) et (3a)), la consultation préalable à la mise en œuvre du traitement dans des cas présentant des risques particuliers (article 34), l'encadrement des mécanismes d'autorégulation (codes de conduite et mécanismes de certification ainsi que accréditation des organismes de contrôle fermé : articles 38 et 39), l'approbation des clauses contractuelles pour le transfert de données à l'étranger ainsi que des règles contraignantes d'entreprise en vertu des articles 42 et 43 du règlement.

Les Etats membres doivent prévoir que les autorités de contrôle disposent des compétences d'autorisation et d'avis qui sont nécessaires pour la mise en œuvre de ces différentes dispositions du règlement (article 53 (1c)).

F. Pouvoirs des autorités de contrôle

Comme cela était déjà le cas sous l'empire de la directive 95/46, chaque autorité de contrôle peut porter à la connaissance des autorités judiciaires les violations du règlement dont elle a connaissance et peut, en outre, ester en justice en vue d'assurer l'application des dispositions du règlement. Mais en outre, les autorités de contrôle détiendront désormais obligatoirement, directement en vertu du droit de l'Union, des pouvoirs d'investigation, d'injonction et d'amende.

Comme le précise l'article 53 (2), les autorités de contrôle devront exercer leurs pouvoirs dans le respect de la Charte des droits fondamentaux de l'Union européenne, ce qui implique notamment que leurs décisions pourront faire l'objet d'un recours en justice et qu'elles devront être prises dans le respect du droit au procès équitable.

[11] Dans le texte de compromis de décembre 2015. Article 73 dans l'approche générale du Conseil de juin 2015.

Parmi les pouvoirs d'enquête des autorités de contrôle, relevons notamment qu'elles pourront ordonner au responsable et au sous-traitant (et le cas échéant au représentant du responsable) de fournir toutes les informations requises pour l'exercice de leurs missions, effectuer des audits et revoir périodiquement les certifications délivrées conformément à l'article 39 (4) du règlement. Elles pourront avoir accès aux locaux du responsable et du sous-traitant, ainsi qu'à tous les équipements et moyens de traitement de données, conformément au droit de l'Union ou au droit procédural d'un Etat membre. Elles pourront obtenir du responsable et du sous-traitant un accès à toutes les données personnelles et à toutes les informations nécessaires pour l'exercice de leurs missions.

Plus remarquables encore sont les pouvoirs d'injonction et d'amende attribués aux autorités de contrôle. Celles-ci pourront ainsi, notamment, émettre des avertissements à l'attention du responsable comme du sous-traitant, leur ordonner de se conformer à une demande individuelle d'exercice des droits d'accès ou de rectification, ou encore leur enjoindre de mettre leurs opérations de traitement en conformité avec les exigences du règlement, en spécifiant de quelle manière et dans quel délai, et notamment par la correction, la restriction ou l'effacement de données avec l'obligation d'en informer les tiers qui ont eu accès à ces données. Les autorités peuvent encore limiter à titre temporaire ou définitif un traitement, ordonner la suspension de flux de données à un destinataire dans un pays tiers et imposer des amendes administratives conformément aux articles 79 et 79 (a), soit en plus des mesures d'injonction précitées, soit en lieu et place de celles-ci, en fonction des circonstances concrètes du cas d'espèce.

L'exercice de ces nouvelles compétences par les autorités de contrôle pourrait entraîner des conséquences pratiques assez contraignantes pour les entreprises telles que, notamment, l'obligation de suspendre ou de mettre fin à certaines activités impliquant un traitement de données non conforme à la loi, de restructurer certains systèmes informatiques, d'interrompre le déploiement d'une application, de redéfinir une stratégie de délégation de tâches à certaines filiales au sein d'un groupe de sociétés, etc. Il pourrait également en résulter d'autres obligations comme celle d'indemniser des clients ou des partenaires commerciaux ayant subi un dommage, de devoir réorienter certains investissements dans les systèmes ou des applications déterminées, sans compter les risques éventuels pour la réputation d'une entreprise ou d'une organisation.

2.2.2. Mécanismes de coopération et de cohésion des régulateurs

Le règlement maintient le principe de la compétence de chaque autorité nationale de contrôle à l'égard des traitements effectués sur son territoire. Cependant, les différentes autorités doivent agir de façon à assurer une application cohérente du règlement à travers le territoire de l'ensemble de l'Union européenne. À cette fin, un certain nombre de mécanismes de coopération et de cohésion sont prévus. Un conseil européen de la protection des données est également institué afin de veiller en particulier à cette préoccupation. Avant d'aborder ces différents mécanismes, il importe de préciser les règles de compétence territoriale de chaque autorité de contrôle.

A. Compétence territoriale

Chaque autorité de contrôle sera compétente pour exercer ses pouvoirs sur son propre territoire national. Seuls les traitements effectués par les cours et tribunaux dans l'exercice du pouvoir judiciaire échappent à la compétence de l'autorité de contrôle. Les traitements des autorités publiques ou des organismes de droits privé qui sont nécessaires pour se conformer à une obligation légale ou pour l'exercice d'une tâche d'intérêt général ou l'exercice de l'autorité publique (article 6 (1), (c) ou (d), du règlement), demeurent soumis à la compétence de l'autorité de contrôle nationale, mais échappent au mécanisme de répartition des compétences défini à l'article 51a du règlement.

Le règlement envisage la question des traitements qui ont un caractère transfrontière. Suivant la définition figurant à l'article 4 (19b) du règlement, il faut entendre par là un traitement qui se situe dans le contexte des activités des établissements du responsable ou du sous-traitant dans plus d'un Etat membre au sein de l'Union européenne, ou bien le traitement qui se situe dans le contexte des activités d'un seul établissement du responsable ou du sous-traitant mais qui affecte de manière substantielle les personnes concernées dans plus d'un Etat membre.

Dans son approche générale, le Conseil a souhaité régler la question de la compétence des autorités de contrôle dans de telles situations à travers un ensemble de règles de coopération et de cohésion. Le texte de compromis a largement repris cette approche.

En règle, et sans préjudice à l'article 51, c'est l'autorité de contrôle du lieu du principal établissement ou du seul établissement du responsable ou du sous-traitant qui est compétente en tant qu'autorité de contrôle principale (« lead authority ») pour ces traitements ayant un caractère transfrontière, et ce conformément à la procédure fixée à l'article 54a. Selon cet article 54a, l'autorité principale demeure le seul interlocuteur du responsable ou du sous-traitant pour les traitements présentant un caractère transfrontière (voy. aussi l'article 51a(3)).

Nonobstant ce qui précède, chaque autorité de contrôle demeure compétente pour traiter les plaintes dont elle est saisie, ainsi que les infractions au règlement qui soit ne relèvent que d'un établissement du responsable sur le territoire de leur Etat membre soit n'affectent les personnes concernées que sur le territoire de leur Etat membre. Un mécanisme de concertation est prévu entre les autorités nationales qui souhaitent se saisir d'une question et l'autorité du lieu du principal établissement du responsable ou du sous-traitant (appelée « autorité principale »). Une autorité nationale qui est saisie d'une plainte qui relève, selon elle, de sa seule compétence, doit en informer l'autorité principale sans délai. Dans les trois semaines, cette autorité principale peut décider d'évoquer le dossier conformément à l'article 54a. Si l'autorité principale choisit d'évoquer le dossier, la procédure prévue à l'article 54a s'applique. L'autorité nationale qui a informé l'autorité principale peut lui soumettre un projet de décision, dont cette dernière devra tenir dûment compte en préparant sa propre décision au sens de l'article 54a (2). Au contraire, lorsque l'autorité principale décide de ne pas traiter elle-même le dossier, l'autorité nationale agira seule, mais dans le respect des mécanismes de coopération visés aux articles 55 et 56.

B. Coopération

La compétence centralisée qui est dévolue à l'autorité principale (celle du principal établissement du responsable ou du sous-traitant) en cas de traitements présentant un caractère transfrontière, ne doit pas faire échec à cette nécessaire coopération entre les autorités de contrôle. Il s'agit non seulement d'assurer une application cohérente du règlement à travers l'ensemble du territoire de l'Union, mais également de prendre en charge de façon appropriée les plaintes qui peuvent avoir été déposées dans un ou plusieurs Etats membres autres que celui de l'autorité principale.

Dès lors, l'autorité principale est tenue d'agir en concertation avec les autres autorités de contrôle concernées, dans la recherche d'un consensus. Pour ce faire, l'autorité principale peut recourir aux mécanismes d'assistance mutuelle et d'opérations conjointes organisés par les articles 55 et 56 du règlement. L'autorité principale pourra solliciter des autres autorités nationales toutes les informations nécessaires, et veillera elle-même à leur transmettre les informations pertinentes concernant le dossier. Elle soumettra son projet de décision ou de mesure sans délai aux autres autorités concernées. Si l'une des autorités concernées élève une objection dans un délai de quatre semaines, et à défaut de consensus, l'autorité principale transmettra le dossier au conseil européen de la protection des données. Celui-ci

adoptera alors une décision conformément à l'article 57 du règlement (art. 54a(3) et (3a)). Si aucune objection n'est élevée dans ce délai, le pasage par le conseil européen de la protection des données n'est pas nécessaire et toutes les autorités de contrôle concernées sont liées par le projet de décision de l'autorité principale (article 54a(4)).

Lorsqu'une plainte est déposée auprès d'une autorité de contrôle, l'autorité principale doit notifier la décision qui est prise au principal établissement du responsable ou du sous-traitant, au conseil européen de la protection des données et aux autorités de contrôle concernées. Cependant, lorsqu'une plainte est rejetée, c'est l'autorité saisie de cette plainte qui adoptera la mesure et qui la notifiera au plaignant et en informera le responsable du traitement (articles 54a(4a) et (4b)).

Il peut aussi arriver qu'une plainte soit rejetée en partie et que, pour certains aspects, elle donne lieu à des mesures d'enquête ou de surveillance de la part de l'autorité de contrôle. Dans ce cas, l'autorité principale et les autorités concernées traiteront chacune un aspect de la plainte : l'autorité principale adoptera une décision en ce qui concerne les actions à prendre à l'égard du responsable et le notifiera au principal établissement de celui-ci ou du sous-traitant en même temps qu'elle en informera le plaignant ; l'autorité saisie de la plainte, elle, adoptera formellement la décision de rejet de la plainte et la notifiera au plaignant ainsi qu'au responsable ou au sous-traitant (article 54a(4bb)).

Dans tous les cas, le responsable ou le sous-traitant devront prendre les mesures nécessaires pour se conformer aux décisions des autorités de contrôle dans le contexte de tous leurs établissements dans l'Union européenne.

Le conseil européen de la protection des données établira des règles de procédure en vue de garantir une coopération efficace entre les autorités conformément à ce qui est prévu à l'article 54a du règlement.

Afin d'assurer une application cohérente du règlement, les autorités de contrôle doivent se porter une assistance mutuelle et mettre en place des mesures de coopération efficace entre elles. En particulier, elles doivent pouvoir échanger des informations et s'accorder sur des mesures de contrôle, comme par exemple des demandes d'autorisation préalable, des consultations, des enquêtes, etc. Par ailleurs, elles peuvent effectuer des opérations conjointes, sous le patronage du conseil européen de la protection des données. Le règlement précise un certain nombre de mesures concernant la communication de ces informations, les délais, les motifs de refus, etc., mais aussi le déroulement concret des opérations d'enquête ou de surveillance menée conjointement par plusieurs autorités dans plusieurs États membres, aux articles 55 et 56.

C. Cohérence (consistency)

Eu égard aux pouvoirs importants que le règlement attribue à chaque autorité de contrôle sur son propre territoire, il convient de veiller à l'application cohérente du règlement à travers l'ensemble de l'Union européenne. Des décisions divergentes des autorités de contrôle risquent en effet d'entraîner une fragmentation du droit de la protection des données selon le territoire où est situé l'établissement ou l'établissement principal du responsable du traitement. Ceci risquerait de mettre à mal l'un des objectifs principaux du règlement, qui est de parvenir à un degré d'harmonisation avancé du droit de la protection des données. Par conséquent, différents mécanismes sont prévus afin d'assurer l'interprétation uniforme des dispositions du règlement.

Tout d'abord, lorsqu'une autorité de contrôle envisage de prendre certaines catégories de décision, elle doit communiquer au conseil européen de la protection des données son projet de décision. Ce conseil pourra ainsi émettre une opinion, non contraignante *a priori*. Les catégories de décision concernées, visées à

l'article 58, portent sur la liste des opérations de traitement soumis à une analyse d'impact préalable, la conformité d'un projet de code de conduite, les critères d'accréditation d'un organisme de certification, les clauses standard de protection des données en cas de transferts internationaux ou l'autorisation de clauses contractuelles visées à l'article 42 (2) (d) ou encore l'approbation des règles contraignantes d'entreprise au sens de l'article 43.

Ensuite, le conseil européen de la protection des données est chargé d'adopter une décision contraignante lorsqu'il existe un désaccord entre l'une des autorités de contrôle concerné et l'autorité principale au sujet d'un projet de décision, lorsqu'il existe un conflit de compétences entre les autorités de contrôle concernées pour déterminer le principal établissement du responsable ou du sous-traitant, ou encore lorsqu'une autorité de contrôle concernée ne requiert pas l'avis du conseil européen de la protection des données alors qu'elle devait le faire, ou ne suit pas l'avis émis par le conseil européen de la protection des données en vertu de l'article 58 (voyez ci-après).

Enfin, toute autorité de contrôle, de même que le président du conseil européen de la protection des données ou la Commission, peuvent toujours demander qu'une question d'application générale ou produisant des effets dans plus d'un Etat membre, soit soumis au conseil européen de la protection des données en vue d'obtenir un avis, en particulier lorsqu'une autorité compétente ne se conforme pas à ses obligations en vertu des articles 55 (assistance mutuelle) et 56 (opérations conjointes).

Lorsqu'il est appelé à formuler un avis sur un projet de décision ou en cas de désaccord entre des autorités nationales, le conseil européen de la protection des données se prononce dans le mois, à la majorité simple de ses membres. Dans l'attente de sa décision, les autorités de contrôle concernées s'abstiendront de prendre une décision. L'avis du conseil européen de la protection des données sera communiqué aux autorités et à la Commission et sera rendu public. L'autorité compétente devra prendre dûment compte l'avis du conseil européen de la protection des données et, dans les deux semaines de la réception de cet avis, communiquera au président du conseil européen de la protection des données sa décision de maintenir ou d'amender son projet de décision. Si cette autorité choisit de ne pas suivre la position du conseil européen de la protection des données, ce dernier pourra alors adopter une décision contraignante.

Les décisions contraignantes du conseil européen de la protection des données lient toutes les autorités concernées et elles doivent être motivées. Elles doivent être adoptées dans le mois, à la majorité des deux tiers de ses membres. Cette période peut être prolongée d'un mois supplémentaire pour tenir compte de la complexité du dossier. Si, dans ce délai, le conseil ne parvient pas à une décision, la décision sera prise dans les deux semaines à la majorité simple des membres. En cas de parité des voix, le vote du président sera prépondérant. La décision du conseil européen de la protection des données sera ensuite communiquée à l'autorité principale et aux autorités concernées. Celles-ci devront alors prendre une décision définitive au plus tard dans le mois de la notification de la décision du conseil européen de la protection des données.

En principe, les autorités nationales de contrôle doivent suspendre toute décision dans l'attente du vote du conseil européen de la protection des données. Cependant, en cas d'urgence nécessitant une intervention immédiate pour protéger les droits et libertés des personnes concernées, l'autorité de contrôle peut adopter des mesures provisoires. Dans ce contexte, elle peut également demander dans l'urgence au conseil européen de la protection des données de rendre un avis ou une décision contraignante. L'initiative de ces mesures provisoires revient à l'autorité de contrôle compétente mais, si celle-ci demeure inactive, toute autorité de contrôle peut adopter les mêmes mesures. En cas d'urgence, le conseil européen de la protection des données doit statuer dans les deux semaines à la majorité simple de ses membres (article 61).

D. Conseil européen de la protection des données (« *European Data Protection Board* »)

Les articles 64 à 72 instituent le conseil européen de la protection des données, régissent ses attributions et organisent son fonctionnement.

Le conseil est composé du responsable de chaque autorité de contrôle national ainsi que du contrôleur européen de la protection des données. La Commission peut participer aux activités et réunions du conseil européen, sans droit de vote.

Le conseil agit de façon indépendante dans l'exercice de ses devoirs et responsabilités. Il est chargé d'assurer l'application cohérente du règlement, notamment à travers le mécanisme de résolution des différends visé à l'article 57, mais également en fournissant à la Commission des avis et en adoptant, d'initiative ou à la demande de la Commission ou de l'un de ses membres, des recommandations, des directives ou des bonnes pratiques en vue d'encourager l'application cohérente du règlement.

Le secrétariat du contrôleur européen de la protection des données (EDPS) devra également assurer le secrétariat du conseil européen de la protection des données. L'article 71 du règlement prévoit néanmoins une séparation fonctionnelle des membres des deux équipes et dispose que le secrétariat du conseil agira uniquement sous les instructions du président du conseil.

On observera que l'accès aux documents soumis aux membres du conseil européen de la protection des données sera régi par le règlement 1049/2001 sur l'accès aux documents administratifs.

2.2.3. Recours, sanctions et responsabilités

Les possibilités de recours, de sanctions et notamment d'amendes sont réglementées par les articles 73 à 79b du règlement.

Le règlement prévoit aux articles 73 à 75, en substance, que les personnes concernées ont le droit de déposer plainte auprès de l'autorité de contrôle, d'exercer un recours judiciaire contre une décision de cette autorité ainsi qu'un recours judiciaire à l'encontre d'un responsable ou d'un sous-traitant.

Pour l'exercice de ces droits, les personnes concernées peuvent se faire représenter par un organisme, une organisation ou une association à qui elles confèreront un mandat ; cet organisme, organisation ou association doit avoir été constitué conformément au droit d'un Etat membre et son objet légal doit inclure aux termes de la loi applicable la protection des droits et libertés des personnes concernées à l'égard des traitements de données à caractère personnel (article 76(1)).

Les Etats membres peuvent, en outre, prévoir que ces organismes, organisations ou associations pourront agir indépendamment du mandat qui leur est donné par un ou plusieurs individus, s'ils estiment que des droits subjectifs ont été violés à la suite d'un traitement de données à caractère personnel non conforme au règlement (article 76(2)).

A. Plaintes et recours auprès de l'autorité de contrôle

Chaque personne concernée doit avoir le droit de déposer plainte auprès d'une autorité de contrôle unique, en particulier celle de l'Etat membre où elle a son lieu habituel de résidence, son lieu de travail ou bien celle du lieu où l'infraction alléguée a été commise.

L'autorité de contrôle informera le plaignant de l'état d'avancement et du résultat de la plainte et l'avertira de la possibilité d'exercer un recours conformément à l'article 74.

Les décisions juridiquement contraignantes de l'autorité de contrôle qui concernent un individu doivent pouvoir faire l'objet d'un recours judiciaire effectif. De même, lorsque l'autorité de contrôle compétente ne traite pas une plainte ou n'informe pas la personne concernée dans les trois mois de l'état d'avancement ou du résultat de la plainte, un recours judiciaire semblable doit être disponible. La procédure de recours sera diligentée devant les tribunaux de l'Etat membre du lieu d'établissement de l'autorité de contrôle. Lorsque l'autorité de contrôle avait pris la décision contestée à la suite d'un avis ou d'une décision du conseil européen de la protection des données, elle transmettra au tribunal compétent l'avis ou la décision dudit conseil.

Ces possibilités de recours sont sans préjudice de tous autre recours administratifs ou non-judiciaires, aux termes des articles 74 (1) et (2) du règlement. Il appartiendra à chaque Etat membre de déterminer la nature et les conditions exactes d'un tel recours conformément au droit interne applicable.

B. Recours juridictionnels contre le responsable ou le sous-traitant

La personne qui estime être victime d'une atteinte à ses droits en vertu du règlement, du fait d'un traitement non-conforme à ce texte, doit pouvoir exercer un recours judiciaire effectif. Ce recours sera dirigé contre le responsable ou le sous-traitant. Le tribunal compétent sera celui du lieu d'établissement du responsable ou du sous-traitant, mais il pourra également être celui du lieu où la personne concernée possède sa résidence habituelle, sauf si le responsable ou le sous-traitant est une autorité publique qui agit dans l'exercice de ses pouvoirs. Ces règles de compétence s'appliquent également en cas d'action en indemnisation en vertu de l'article 77 du règlement (voyez ci-après).

L'article 76a prévoit que les tribunaux saisis de tels recours se tiendront mutuellement informés de l'existence de recours qui peuvent porter sur le même objet ou concerner les traitements effectués par le même responsable ou le même sous-traitant. Le tribunal saisi en second lieu peut choisir de suspendre les procédures ou se déclarer sans juridiction à condition que le tribunal premier saisi soit compétent et que le droit applicable permette de « consolider » les différents recours. Il conviendra sans doute de concilier ces règles avec celles qui gouvernent la compétence internationale et notamment les questions de litispendance et de connexité notamment.

L'article 77 du règlement accorde à toute personne qui a subi un dommage matériel ou immatériel à la suite d'opérations de traitement non conformes aux règlements, le droit d'obtenir une indemnisation de la part du responsable ou du sous-traitant. Le responsable qui est impliqué dans le traitement sera tenu d'indemniser le préjudice causé par le traitement non conforme au règlement. Quant au sous-traitant, il sera tenu d'indemniser le dommage causé par le traitement lorsqu'il ne s'est pas conformé aux obligations du règlement qui sont spécialement applicables aux sous-traitants ou lorsqu'il a agi sans instruction ou de façon contraire aux instructions légitimes du responsable du traitement.

Le responsable ou les sous-traitants seront exemptés de leur obligation d'analyser s'ils démontrent qu'ils ne sont pas responsables de l'événement qui a donné lieu au dommage.

Lorsque plus d'un responsable ou plus d'un sous-traitant ou un responsable et un sous-traitant sont ensemble impliqués dans le même traitement, et lorsqu'ils sont responsables en vertu de l'article 77 (2) et (3), ils seront chacun tenus de l'entièreté du dommage.

Le responsable ou le sous-traitant qui a effectué le règlement de l'intégralité du préjudice, peut réclamer aux autres responsables ou sous-traitants impliqués dans le même traitement une part de l'indemnité correspondant à leurs parts respectives de responsabilité dans le dommage survenu.

C. Amendes administratives et autres sanctions

Les autorités de contrôle peuvent imposer des amendes en cas d'infraction au règlement. Celles-ci doivent être, dans chaque cas individuel, efficaces, proportionnées et dissuasives. La décision d'imposer une amende doit être prise dans le respect des garanties procédurales conformes au droit de l'Union et de l'Etat membre concerné, en ce compris le droit à un recours juridictionnel et le droit au procès équitable.

Les Etats membres ont la liberté de choisir la voie des amendes administratives régies par le règlement ou, en application de l'article 79 (5), de prévoir des sanctions pénales dans leur droit national en s'assurant que celles-ci soient efficaces, proportionnées et dissuasives et en prenant en compte le niveau des amendes administratives prévues par le règlement. Les Etats membres notifieront dans ce cas à la Commission les dispositions pertinentes de leur droit pénal national.

Les autorités de contrôle devront tenir compte d'un ensemble de facteurs avant de prononcer des amendes administratives. Rappelons en effet qu'elles peuvent ordonner, plutôt qu'une amende, certaines des mesures visées à l'article 53 du règlement, à moins qu'elles ne prononcent à la fois une amende et une telle injonction. Dans tous les cas, les autorités de contrôle devront tenir compte des circonstances de fait pertinentes, énumérées à l'article 79(2a), telles que, notamment, la nature, la gravité et la durée de l'infraction, la nature, la portée et la finalité du traitement, le nombre d'individus concernés et la gravité du dommage subi, le caractère intentionnel ou non de l'infraction, les mesures prises par le responsable ou le sous-traitant pour atténuer le dommage, le degré de responsabilité respectif du responsable et du sous-traitant eu égard aux mesures techniques et organisationnelles mises en œuvre conformément aux articles 23 et 30, les cas éventuels de récidive, la manière dont l'autorité de contrôle a pris connaissance de l'infraction et notamment le fait que celle-ci ait été notifiée par le responsable ou le sous-traitant lui-même, l'existence de mesures d'injonction ou d'investigation antérieurement prononcées à l'encontre du responsable ou du sous-traitant relativement au même objet et le respect ou non de ces mesures par le responsable ou le sous-traitant, l'adhésion à des codes de conduite approuvés ou à des mécanismes de certification accrédités en vertu des articles 38 et 39, ainsi encore que tout autre circonstance aggravante ou atténuante propre aux circonstances du cas d'espèce.

Il appartient à chaque Etat membre de décider si les règles en matière d'amendes administratives peuvent donner lieu à l'imposition d'amendes aux autorités et organismes publics.

Le niveau des amendes administratives est fixé par l'article 79a du règlement. Ce niveau dépend notamment du type d'infraction commise. Il peut être de 10 ou de 20 millions d'euros ou, à l'égard d'une entreprise, de 2 % à 4 % de son chiffre d'affaires mondial de l'année précédente. Lorsqu'un responsable ou un sous-traitant se rend coupable de plusieurs violations des dispositions du règlement susceptibles d'être frappées d'une amende administrative, le montant total de l'amende ne peut excéder le montant prévu pour l'infraction la plus grave.

L'approche générale du Conseil de juin 2015 retenait trois niveaux distincts pour le montant des amendes (qui était de 250.000 à 1 million d'euros ou de 0,5 à 2% du chiffre d'affaires d'une entreprise) :

- Le premier niveau, le plus bas, concerne le responsable qui, intentionnellement ou par négligence, ne répond pas aux demandes de la personne concernée dans le délai visé à l'article 12 (2) du

règlement concernant le droit à l'information, ou qui, contrairement à l'article 12 (4), facture un coût pour la communication des informations à la personne concernée.

- Le deuxième niveau, intermédiaire, concerne un ensemble de manquements intentionnels ou par négligence aux dispositions en matière de droit à l'information (article 12 (3), 14 et 14a), de droit d'accès et de rectification (articles 15 et 16), de droit à l'effacement de données (article 17), de droit a la restriction du traitement (article 17a), de droit à une notification concernant la rectification, l'effacement ou la restriction de traitement (article 17*bis*), de droit à la portabilité des données (article 18), ou encore en matière d'objection à des décisions individuelles automatisées (article 19) et d'opposition au marketing direct (article 19 (2)) ; il s'agit encore des manquements aux obligations en matière de détermination de la responsabilité respective des contrôleurs conjoints (article 24) et en matière de documentation des traitements (articles 28 et 31 (4)).
- Le dernier niveau, le plus élevé, s'applique aux manquements intentionnels ou par négligence aux obligations de disposer d'une base légale pour le traitement et aux obligations en matière d'obtention du consentement en vertu des articles 6 à 9, ainsi qu'à la violation des règles en matière de décisions individualisées automatisées et notamment de profilage (article 20), de relations avec le sous-traitant (article 26) et de codes de conduite ou de certification (articles 38 et 39), et aux manquements à l'obligation de mettre en œuvre des mesures appropriées ou de pouvoir démontrer la conformité (articles 22 et 23), de désigner un représentant en vertu de l'article 2, de notifier une violation de données personnelles (article 31 et 32), d'effectuer une analyse d'impact préalable (article 33) ou une consultation préalable à certains traitements (article 34 (2)) ; ces amendes du niveau le plus élevé peuvent aussi être infligées à celui qui effectue un transfert de données vers un destinataire situé hors de l'Union européenne ou à une organisation internationale en violation des articles 41 à 44, à celui qui ne se donne pas suite à un ordre de restriction temporaire ou définitive du traitement ou de suspension de flux de données (article 53 (1b), ou enfin à celui qui ne fournit pas à l'autorité compétente l'accès aux informations requises en vertu de l'article 53 (1).

Dans le texte de compromis de décembre 2015, ne subsistent que deux niveaux :

- jusqu'à 10 millions EUR ou 2% du chiffre d'affaires mondial d'une entreprise en cas d'atteinte aux règles concernant les obligations du responsable et du sous-traitant (notifications individuelles, accountability, privacy impact assessment, etc.)

- jusqu'à 20 millions EUR ou 4 % du chiffre d'affaires mondial d'une entreprise en cas notamment d'atteinte aux principes fondamentaux repris aux articles 5 à 9, de violation des droits subjectifs des individus et de transferts internationaux illicites.

2.3. Mesures d'exécution et règles particulières

Comme on l'a vu ci-avant, un certain nombre de dispositions du règlement permettent aux autorités de contrôle, le cas échéant en concertation avec la Commission et à l'intermédiaire du conseil européen de la protection des données, de définir de manière plus concrète des exigences ou des règles particulières dans différents domaines : relations avec le sous-traitant, mécanismes d'autorégulation, transferts internationaux de données, mais aussi mesures préalables au traitement (étude d'impact et consultation préalable concernant les traitements présentant des risques particuliers, etc.).

On n'en donnera ici qu'un seul exemple, à propos des relations entre le responsable et le sous-traitant. Selon le projet de règlement, la Commission est habilitée à établir des clauses standard pour le problème de la sous-traitance en cascade et pour la relation contractuelle entre le responsable et le sous-traitant. Une autorité de contrôle peut par ailleurs adopter des clauses contractuelles standard. Dans de tels cas, et sans

préjudice à l'accord particulier conclu entre le responsable et le sous-traitant, l'exigence d'un accord entre ces deux opérateurs peut être satisfaite au moyen de ces clauses contractuelles standard ou de clauses du même type qui font partie d'un mécanisme de certification accrédité conformément à l'article 39 et 39 a du règlement. D'une manière générale, l'adhésion du sous-traitant à un code de conduite approuvé conformément à l'article 38, ou à un mécanisme de certification approuvé conformément à l'article 39, peuvent servir à démontrer que le sous-traitant présente les garanties suffisantes au sens article 26 (1) et 26 (2a) du règlement.

À travers l'adoption de ces mesures particulières, les autorités de contrôle et le conseil européen de la protection des données pourront sans nul doute imposer des obligations très concrètes aux entreprises et organisations, dans des secteurs particuliers ou pour des questions spécifiques. L'on y gagnera peut-être en sécurité juridique. Il apparaît en tout cas qu'un dialogue régulier entre les entreprises et autres organisations responsables du traitement, d'une part, et les autorités de contrôle, d'autre part, sera nécessaire.

Tel est d'ailleurs l'un des rôles attendus du détaché à la protection des données.

Enfin, un tel dialogue est probablement indispensable pour tenir dûment compte des exigences du principe dit de « accountability », dont il sera question ci-après, à travers une remise en question régulière des mesures et des politiques internes mises en œuvre par l'entreprise ou l'organisation pour se conformer à ses nombreuses obligations en matière de protection des données personnelles.

3. *Accountability*

3.1. Notion d' « accountability »

La notion d'accountability (pour reprendre le terme anglais difficile à bien traduire en français), n'est pas inconnue en droit international de la protection des données. Elle figurait déjà, en 1980, dans les principes directeurs adoptés par l'OCDE et elle a ensuite été reprise dans un certain nombre d'instruments de droit international ou dans des résolutions ou des bonnes pratiques non contraignantes. Avant la publication de la proposition de règlement de la Commission, la notion d'accountability avait aussi été mise en avant dans deux documents du Groupe de l'article 29 (Documents WP 168 et WP 173). Le Groupe 29 jugeait important de tenir compte de ce principe dans le cadre de la révision de la directive 95/46, en « *exigeant des responsables du traitement des données qu'ils mettent en œuvre des mesures appropriées et efficaces pour garantir le respect des principes et obligations en la matière, et qu'il démontre cette mise en conformité aux autorités qui le demandent. Ces mesures devraient favoriser la conformité aux principes et obligations en matière de protection des données tout en limitant les risques d'accès non autorisés, d'abus, de perte, etc. L'obligation de démontrer, sur demande, la mise en place des mesures requises devrait, pour les autorités chargées de la protection des données, se révéler un instrument utile qui les aidera dans leur mission de surveillance* » (WP 173, conclusion, point 74). Dans cette acception, la notion d'accountability regroupe essentiellement deux éléments : la mise en œuvre effective de mesures et de procédures pour assurer la protection des données, d'une part, et la capacité de démontrer le respect effectif de ces mesures et procédures, d'autre part.

La notion d'accountability n'est toutefois pas limitée au domaine de la protection des données. Il s'agit d'un concept que l'on retrouve à des degrés divers à travers plusieurs mécanismes et instruments de régulation dans certains secteurs dont le secteur financier ou dans le domaine de la responsabilité sociale des entreprises.

D'une manière générale, il s'agit de rendre les entreprises activement responsables de la mise en conformité, en encourageant la mise en place de structures de gouvernance interne, de pratiques de gestion et de cultures d'entreprise qui concourent ensemble à assurer la réalisation des objectifs de compliance.

D'après certaines recherches[12], cette approche globale impliquerait notamment d'encourager la publication par l'entreprise ou l'organisation de rapports dans des formats standardisés, afin de réaliser un certain niveau de transparence mais aussi de faciliter la comparaison entre organisations quant à leur niveau de conformité. Un autre aspect de cette approche porte sur l'évaluation permanente des efforts mis en œuvre par l'entreprise ou l'organisation, idéalement dans le contexte d'un dialogue ouvert avec le régulateur, qui est appelé à évaluer la performance de l'organisation en termes de compliance et à lui faire part de suggestions ou d'exemples de bonnes pratiques mises en œuvre par d'autres organisations. Enfin, l'approche basée sur l'accountability implique la mise en place d'un certain nombre d'incitants et de mécanismes de sanction encourageant les organisations à se comporter de façon proactive dans la définition et la mise en œuvre de programmes de mise en conformité. Parmi de nombreux exemples possibles, on peut citer à cet égard le fait de prendre en compte l'existence d'un programme de compliance dans la décision d'infliger une sanction ou une amende, ou dans l'appréciation de la décision d'entamer ou non des poursuites en cas de violation des règles applicables.

Dans le domaine de la protection des données, l'approche d'accountability a surtout été développée à propos des transferts internationaux de données, et plus spécialement des règles contraignantes d'entreprise[13]. Dans ce contexte, l'une des questions débattues est de savoir qui supporte la responsabilité envers les personnes concernées à l'égard de données qui font l'objet de transferts successifs : au-delà de la relation entre le responsable du traitement qui transfère des données hors de l'Union européenne et le sous-traitant, lorsque les données sont ensuite transférées à d'autres sous-traitants voire à des tiers, peut-on considérer que le responsable du traitement ou le sous-traitant principal soient et demeurent responsables du dommage même après que les données échappent à leur contrôle ? leur suffit-il de démontrer qu'ils ont mis en place des mesures appropriées pour protéger les données ?[14]

3.2. L' « accountability » dans le règlement européen

Dans l'exposé des motifs de sa proposition initiale, la Commission indiquait que l'article 22 du projet « *takes account of the debate on a 'principle of accountability' and describes in detail the obligations of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance* »[15]. Cet article disposait ce qui suit : « *The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation* ». Il énumérait ensuite les mesures à mettre en œuvre, en renvoyant à d'autres dispositions du règlement, telles que notamment tenir à jour une documentation sur les traitements, désigner un détaché à la protection des données, etc. Et il imposait au responsable du traitement de mettre en œuvre des mécanismes pour vérifier l'effectivité des mesures ainsi mises en œuvre.

Par ailleurs, l'article 5(f) de la proposition de règlement de la Commission disposait comme suit : « *Personal data must be (…) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation* ». Le texte adopté par le Parlement européen contient, lui, une évocation expresse du principe d'accountability : « *the*

[12] Voy. pour un résumé et de nombreuses références et exemples, L. Moerel, *Binding Corporate Rules. Corporate Self-Regulation of Global Data Transfers*, Oxford University Press, 2012, pp. 178-186.
[13] L. Moerel, *op. cit.*, chap. 6.2., pp. 101-105 et pp. 209-227 ; C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013, pp. 71-76.
[14] C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013, p. 75.
[15] Proposition de règlement de la Commission, Explanatory Memorandum, p. 10.

controller, who shall ensure and be able to demonstrate the compliance with the provisions of this Regulation (accountability) ».

Le texte de compromis de décembre 2015 reprend un article 5(2), qui dispose : « *The controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ('accountability')* ». La mention "accountability" a été insérée dans le texte de compromise et complète donc la formulation issue de l'approche générale du Conseil.

De plus, l'article 22(1) du texte de compromis dispose par ailleurs que le responsable du traitement doit « *mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement des données personnelles est effectué de façon conforme au règlement* », et ce en prenant en considération « *la nature, la portée, le contexte et les finalités du traitement ainsi que les différents niveaux de risque pour les droits et libertés individuelles et leur degré de gravité* », étant précisé que « *ces mesures doivent faire l'objet d'une révision régulière et être mises à jour si nécessaire* »[16].

L'idée d'accountability paraît donc bien inspirer et sous-tendre l'ensemble du règlement, comme le montrent également les articles 22(2a) et (2b) : les mesures à mettre en œuvre par le responsable du traitement peuvent inclure des « politiques de protection des données » appropriées ; de plus, l'adhésion à des codes de conduite approuvés ou à des mécanismes de certification accrédités conformément aux articles 38 et 39 peut être un moyen de démontrer que le responsable du traitement se conforme aux obligations du règlement. Par ailleurs, l'ensemble du texte de compromis repose en large partie sur l'idée que les mesures à prendre par le responsable du traitement et le sous-traitant doivent être définies en fonction du niveau de risque inhérent à chaque traitement (voy. notamment le considérant 60). Ceci est une autre caractéristique de la notion d'accountability. Enfin, nombre de dispositions qui sont maintenues voire renforcées dans l'approche générale du Conseil ou le texte de compromis sont directement inspirées par le principe d'accountability tel qu'il a été défini antérieurement dans le contexte soit des règles contraignantes d'entreprise, soit d'autres avis antérieurs du Groupe 29.

Il apparaît ainsi que l'intention des auteurs du texte serait bien d'ancrer d'une manière ou d'une autre ce principe d'accountability dans le droit de la protection des données. Reste cependant à définir sa portée et son contenu exacts, ainsi que ses conséquences précises sur le plan juridique.

La référence à la notion d'accountability dans les débats relatifs à la protection des données, et particulièrement dans le cadre de la réforme annoncée, n'est en effet pas neutre. Comme l'indique un auteur, « *it is no secret in the data protection community that some data controllers view accountability as a justification for them to be freed from such burdens* [parlant des lourdes démarches administratives de notification préalable aux autorités de contrôle] »[17]. Or, même si l'approche générale du Conseil et le texte de compromis sont globalement plus souples et moins contraignants pour les responsables du traitement, il n'en reste pas moins que le règlement dans sa version définitive devrait entraîner un relèvement global du niveau de diligence et d'attention attendus des responsables de traitement comme des sous-traitants.

Dans ce contexte, au-delà des différences de formulation à travers le processus d'adoption du texte, on peut raisonnablement penser que le droit européen de la protection des données comportera désormais pour le responsable du traitement une obligation de prendre des mesures positives afin de protéger les données, de devenir acteur à part entière du respect effectif des règles, et d'être comptable devant les autorités de contrôle ainsi que devant les personnes concernées des mesures mises en œuvre à cet égard.

[16] Notre traduction.
[17] C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013, p. 74.

4. Nouvelles obligations pour les responsables de traitement et les sous-traitants

L'analyse qui suit repose sur l'approche générale du Conseil et le texte de compromis, tout en indiquant çà et là en quoi cette approche diffère de celle promue par la Commission ou le Parlement. Elle est communiquée sous réserve de l'adoption du texte définitif tel que publié.

4.1. Concepts de base et principes fondamentaux

A. Introduction

Les fondements de la réglementation issue de la directive 95/46 sont peu ou prou repris par le règlement, même si celui-ci apporte des améliorations sur certains points. L'équilibre global reposant sur les principes de qualité des données, de légitimité des traitements et de proportionnalité de ceux-ci, n'est pas bouleversé de fond en comble.

Ainsi, en vertu de l'article 5, les données doivent être traitées loyalement, licitement et de façon transparente ; elles doivent être collectées pour des finalités spécifiques, explicites et légitimes ; elles doivent être adéquates, pertinentes et non excessives au regard des finalités poursuivies ; elles doivent être exactes et, si nécessaire, mises à jour ; et elles ne peuvent être conservées plus longtemps que nécessaire sous une forme qui permet l'identification des personnes concernées. Le règlement innove en précisant que les données doivent être traitées d'une façon qui assure une « sécurité appropriée », et que le responsable du traitement est tenu d'assurer le respect de ces dispositions concernant la qualité des données.

L'article 6 du règlement énumère quant à lui les bases légales susceptibles de justifier tout traitement : le consentement, la nécessité pour l'exécution d'un contrat, pour le respect d'une obligation légale, pour la protection des intérêts vitaux de l'intéressé ou d'un tiers, pour l'exécution d'une tâche d'intérêt général ou l'exercice de l'autorité publique et, enfin, pour les intérêts légitimes poursuivis par le responsable du traitement ou un tiers, à moins, dans ce cas, que ces intérêts légitimes ne soient contrebalancés par les intérêts et les droits et libertés fondamentaux de la personne concernée.

B. Consentement

Le règlement s'en tient à l'exigence d'un consentement « *non ambigu* », abandonnant l'idée d'un consentement explicite qui avait été proposée par la Commission et le Parlement. Dans le considérant 25, le règlement envisage la possibilité de donner son consentement par « *une forme d'action positive* » de la personne concernée, notamment le fait de cocher une case sur un site Internet, sélectionner les paramètres d'un service ou d'une application, ou encore toute autre déclaration ou tout comportement qui indiquent de façon claire et dans un contexte donné, l'acceptation par la personne concernée du traitement de ses données à caractère personnel. Le silence, les cases pré-cochées ou l'inaction de l'individu ne peut toutefois pas constituer un consentement. Pour que le consentement soit valablement donné, la personne concernée doit connaître au moins l'identité du responsable et les finalités du traitement (considérant 32).

Le considérant 25 précise aussi que lorsque plusieurs finalités distinctes sont poursuivies, un consentement distinct doit être obtenu pour chacune d'elles. Il appartient au responsable du traitement de pouvoir

démontrer que la personne concernée a donné son consentement. À cette fin, le considérant 32 insiste sur la nécessité de recourir à des formulations claires et aisément compréhensibles[18], et précise que le consentement ne peut être considéré comme libre lorsque la personne concernée n'a pas véritablement le choix de refuser ou de retirer son consentement sans subir un désavantage. De façon claire, le considérant 34 indique que le consentement ne sera pas jugé libre s'il n'est pas possible de consentir séparément à différentes opérations de traitement ou si l'exécution d'un contrat est conditionnée par le consentement alors que le traitement des données n'est pas nécessaire pour l'exécution de ce contrat et que la personne concernée peut raisonnablement obtenir des services équivalents auprès d'un tiers sans devoir consentir au traitement de ses données de la même manière.

Par ailleurs, l'article 7 du futur règlement dispose que le responsable du traitement doit être capable de démontrer que la personne concernée a donné son consentement non ambigu, ou son consentement explicite lorsqu'il s'agit du traitement de données sensibles. Lorsqu'un formulaire de consentement écrit est présenté à la personne concernée et que cette déclaration concerne plusieurs domaines, la demande de consentement doit être présentée d'une manière nettement distincte des autres sujets abordés dans le document, sous une forme intelligible et aisément accessible, en faisant usage d'une formulation claire et compréhensible. L'article 7 précise aussi que la personne concernée a le droit de retirer son consentement à tout moment, et qu'elle doit être informée de cette possibilité avant même de donner son consentement initial. Le retrait du consentement n'affectera pas la légitimité du traitement pour le passé. Il doit être aussi facile de retirer son consentement que de le donner, précise l'article 7(3).

L'article 8 précise les conditions particulières pour le consentement obtenu de la part d'un mineur d'âge en rapport avec des services de la société de l'information. Dans un tel contexte, le consentement doit être donné ou autorisé par les parents ou le détenteur de l'autorité parentale lorsque le mineur est âgé de moins de 16 ans, sauf si le droit d'un Etat membre prévoit un âge inférieur qui ne peut être de moins de 13 ans (article 8(1)). Le responsable du traitement doit « faire des efforts raisonnables » pour vérifier, en tenant compte de l'état de la technique disponible, que le consentement soit donné ou autorisé par le détenteur de l'autorité parentale (article 8(1a)). Les dispositions du règlement sont sans préjudice des dispositions du droit national concernant la validité, la conclusion et les effets d'un contrat conclu avec un mineur (article 8 (2)).

C. Intérêt légitime et traitement ultérieur pour des finalités compatibles

Lorsque le traitement repose sur la poursuite de l'intérêt légitime du responsable, l'appréciation de la balance des intérêts est un exercice toujours délicat. Les considérants 38 à 40 du texte de compromis contiennent un certain nombre de précisions utiles pour l'interprétation de cet équilibre. Ainsi, lorsqu'il existe une « *relation pertinente et appropriée* » entre le responsable et la personne concernée, par exemple lorsque la personne concernée est un client ou est au service du responsable, l'existence d'un intérêt légitime du responsable pourrait être établie. Il faut néanmoins tenir compte des attentes légitimes de la personne concernée au moment et dans le contexte de la collecte des données. La prévention de la fraude ou le marketing direct constituent également des intérêts qui peuvent être légitimes selon le considérant 38. Un autre type d'intérêts légitimes envisagés dans le considérant 38a concerne les groupes de sociétés. Enfin, le considérant 39 envisage comme légitimes certaines finalités dans le contexte de la sécurité des réseaux et de l'information.

[18] On relèvera aussi que le considérant 32 se réfère expressément à la directive 93/13/CE concernant les clauses abusives dans les contrats conclus avec les consommateurs, pour exiger que toute déclaration de consentement pré-remplie par le responsable du traitement, soit établie dans une forme intelligible et aisément accessible, en faisant usage d'un langage clair et compréhensible, et sans contenir de clauses abusives.

Une question étroitement liée à la précédente est celle de l'appréciation de la compatibilité entre les finalités du traitement initial et celles d'un traitement ultérieur. À cet égard, l'article 5 (1) (B) du règlement établit tout d'abord que le traitement ultérieur pour des finalités d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou pour des finalités statistiques, conformément à l'article 83, ne sera pas jugé incompatible avec les finalités initiales. L'article 6(3a) du règlement énumère aussi un certain nombre de critères qui peuvent être pris en compte pour apprécier cette compatibilité, tels que notamment le lien entre les finalités initiales et nouvelles, le contexte dans lequel les données ont été collectées, la nature des données, les conséquences possibles de l'utilisation ultérieure qui est envisagée et l'existence de mesures de précaution ou de sauvegarde appropriées.

4.2. Renforcement des droits individuels et profilage

A. Notifications individuelles

Le règlement opère un renforcement significatif des droits subjectifs des personnes concernées. Nous nous limiterons ici à quelques observations succinctes concernant les notifications individuelles aux personnes concernées et le profilage.

Tout d'abord, on remarquera que les informations qui doivent être communiquées lors de la collecte des données sont étendues par le règlement (article 14).

- au cas où le traitement est basé sur la poursuite de l'intérêt légitime du responsable conformément à l'article 6(1)(f), du règlement, l'indication des intérêts légitimes poursuivis par le responsable ou par le tiers auquel les données sont communiquées.
- Les destinataires ou catégories de destinataires des données.
- Le cas échéant, l'intention du responsable de transférer les données à un destinataire situé dans un pays tiers ou à une organisation internationale.
- La durée de conservation ou à tout le moins les critères de fixation de celle-ci.
- L'existence d'un droit de demander l'accès à et la rectification ou la suppression des données ou la restriction du traitement des données concernant la personne, et de s'opposer au traitement, ainsi que d'un droit à la portabilité des données.
- Lorsque le traitement est légitimé par le consentement de la personne, y compris pour les données sensibles, il faut notifier l'existence d'un droit de retirer le consentement à tout moment, sans que cela affecte la licéité du traitement basé sur le consentement avant le retrait de celui-ci.
- Le droit de déposer plainte auprès d'une autorité de contrôle.
- L'indication si la communication des données est une exigence légale ou contractuelle, ou un préalable nécessaire à la conclusion d'un contrat, ainsi que le caractère obligatoire ou non de la communication des données et les conséquences éventuelles d'une absence de communication de ces données par la personne concernée.
- L'existence d'un processus de décision automatisée, en ce compris le profilage visé à l'article 20 (1) et (3) et toute information concernant la logique sous-jacente ainsi que la signification et les conséquences possibles d'un tel traitement pour la personne concernée.
- Lorsque le responsable a l'intention de procéder à un traitement ultérieur pour une finalité autre que celle pour laquelle les données ont été collectées initialement, il doit aussi informer la personne concernée au préalable de la nouvelle finalité poursuivie et de toute autre information pertinente visée ci-avant.

Lorsque les données ne sont pas obtenues directement auprès de la personne concernée mais auprès d'une source externe ou d'un tiers, le responsable doit également communiquer les catégories de données concernées ainsi que l'indication de la source d'origine des données, sauf si celles-ci proviennent de sources publiquement accessibles.

B. Profilage

Le règlement clarifie également les obligations et les limites du profilage. Celui-ci est défini à l'article 4(3aa) comme toute forme de traitement automatisé consistant à utiliser des données pour évaluer des aspects personnelles d'un individu, en particulier pour analyser et prédire des aspects concernant sa performance au travail, sa situation économique, sa santé, ses préférences personnelles ou ses intérêts, sa fiabilité, ou son comportement, sa localisation ou ses déplacements. Le considérant 58 du projet de règlement donne deux exemples de profilage de nature à affecter de manière significative les personnes concernées : le refus automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans intervention humaine.

La question du profilage est régie à l'article 20 du règlement, qui donne à toute personne concernée le droit de ne pas être soumis à une décision basée uniquement sur un traitement automatisé, en ce compris le profilage, lorsqu'une telle décision produit des effets juridiques qui la concernent ou qui l'affectent de manière significative.

Le profilage (ou d'autres traitements du même type) ne pourra être autorisé que dans trois cas : s'il repose sur le consentement explicite de l'intéressé, s'il est autorisé en vertu du droit de l'Union ou du droit d'un Etat membre pour peu que celui-ci établisse également les mesures nécessaires pour préserver les droits et libertés et les intérêts légitimes de la personne concernée, ou s'il est nécessaire pour conclure ou exécuter un contrat entre la personne concernée et le responsable du traitement.

Le profilage ou les autres décisions automatisées ne peuvent généralement pas être basées sur des catégories de données sensibles. Lorsque le profilage est nécessaire pour la conclusion ou l'exécution d'un contrat ou lorsqu'il repose sur le consentement explicite de la personne concernée, le responsable doit mettre en œuvre des mesures adéquates pour préserver les droits et libertés et les intérêts légitimes de la personne concernée, et à tout le moins prévoir que celle-ci aura le droit d'obtenir une intervention humaine de la part du responsable du traitement, qu'elle pourra faire valoir son point de vue et contester la décision automatisée. Selon le considérant 58, afin d'assurer un traitement équitable et transparent à l'égard de la personne concernée, le responsable du traitement devrait recourir à des procédures mathématiques ou statistiques appropriées pour le profilage, mettre en œuvre des mesures techniques et organisationnelles adéquates pour s'assurer en particulier que les facteurs susceptibles d'entraîner des erreurs soient corrigés et que le risque d'erreur soit minimisé, et pour assurer la sécurité et l'intégrité des données et empêcher notamment la discrimination entre individus sur la base notamment de l'origine ethnique ou raciale, de l'opinion politique, religieuse ou philosophique, etc.

4.3. Nouvelles obligations à charge du responsable et du sous-traitant

4.3.1. Mesures appropriées au niveau de risque ; *data protection by design and by default*

En vertu de l'article 22 (1), on l'a vu, le responsable du traitement a l'obligation de démontrer que le traitement des données est effectué dans le respect du règlement, et de mettre en œuvre des mesures appropriées à

cette fin. Conformément à l'approche basée davantage sur le risque, cette obligation suppose d'apprécier de façon objective la probabilité et le degré de sérieux des risques encourus pour les droits et libertés des individus en raison du traitement, compte dûment tenu de la nature, de la portée, du contexte et des finalités de celui-ci. Le considérant 60b confirme le caractère objectif de cette appréciation du risque au regard du traitement et des implications de celui-ci pour les droits et libertés des individus.

Ainsi que le détaille le considérant 60a, les traitements de données peuvent impliquer des risques divers, présentant des degrés variables de probabilité et de gravité selon les situations. Il peut s'agir d'un risque de discrimination, de vol d'identité ou de fraude, d'atteinte à la réputation, etc. mais également de toute forme d'atteinte aux droits et libertés en raison notamment du traitement de données sensibles ou relatives à la santé, de l'évaluation d'aspects personnels tels que la performance au travail, la situation économique, la santé, les préférences personnelles, le comportement, la localisation ou les déplacements, en vue de créer des profils personnels. Le traitement des données de mineurs d'âge, ainsi que le traitement de vastes quantités de données susceptibles d'affecter un grand nombre d'individus font également partie des traitements qui présentent des risques particuliers. C'est donc en fonction de l'ensemble des circonstances particulières de chaque traitement, que le responsable est tenu d'apprécier les risques pour la vie privée et les droits et libertés des individus, et de définir des mesures appropriées de nature à garantir l'application des dispositions du règlement.

Afin de mieux assurer le respect des règles de protection des données, il peut s'avérer nécessaire de prendre en compte, dès le stade de la conception des produits ou services, certains impératifs liés à l'application du règlement, comme la minimisation des données ou la possibilité de rendre celles-ci anonymes ou pseudonymes. C'est pourquoi l'article 23 du règlement fait obligation au responsable de mettre en œuvre des mesures techniques et organisationnelles appropriées, en tenant compte de la nature et des risques liés au traitement ainsi que de ses objectifs. L'objectif est que le traitement réponde aux exigences du règlement et protège les droits des individus. Ces mesures peuvent inclure la minimisation des données et le fait de les rendre pseudonymes dès que possible, etc.

Plus précisément, le responsable devra mettre en œuvre des mesures pour s'assurer que, par défaut, seules les données nécessaires aux finalités du traitement soient traitées, y compris en ce qui concerne la quantité de données collectées, l'étendue de leur utilisation, la durée de conservation des données et leur accessibilité à des tiers. Ces mesures devront aussi garantir que, par défaut, des données ne peuvent être rendues accessibles à un nombre indéfini de personnes sans intervention humaine (sous réserve des mesures qui seront prises en droit national, conformément à l'article 80 du règlement, pour réconcilier le droit à la protection des données avec la liberté d'expression et le droit du public de recevoir des informations). Il s'agit là d'une obligation nouvelle, qui peut s'avérer particulièrement exigeante pour le responsable du traitement.

Le règlement dispose que les mécanismes de certification conformes à l'article 39 pourront être utilisés en vue d'établir que le responsable se conforme à ses obligations à cet égard.

Le considérant 61 envisage également d'encourager les producteurs d'applications, de produits et de services qui reposent sur le traitement de données ou qui traitent des données pour remplir leurs fonctions, à prendre en compte les règles de protection des données dès le stade du développement et de la conception de leurs produits et, en tenant dûment compte de l'état de l'art, de s'assurer que les responsables de traitement et les sous-traitants sont en mesure de remplir leurs obligations en termes de protection des données. Ceci ne se traduit toutefois pas dans le règlement par une obligation particulière à l'égard de ces producteurs en tant que tels.

4.3.2. Responsable et sous-traitant

Comme l'indique le considérant 62, la protection des droits et libertés des individus suppose que les responsabilités et les obligations découlant du règlement soient attribuées de façon claire, y compris pour permettre la surveillance et le contrôle des activités du responsable par les autorités de contrôle. Ceci est particulièrement vrai lorsque le responsable du traitement détermine les finalités et les moyens des opérations de façon conjointe avec d'autres responsables, ou lorsqu'un traitement est exécuté pour le compte du responsable par un sous-traitant. C'est pourquoi le règlement énumère une série d'obligations et apporte des précisions importantes concernant la responsabilité conjointe, les obligations du responsable établi hors de l'Union européenne et les obligations du sous-traitant ainsi que ses rapports avec le responsable.

A. Contrôle conjoint de deux ou plusieurs responsables.

L'article 24 du règlement consacre, à charge de ceux qui déterminent ensemble les finalités et les moyens du traitement, qualifiés de « responsables conjoints » (« *joint controllers* »), une certaine obligation de transparence envers les personnes concernées.

Ils doivent en effet déterminer leurs responsabilités respectives vis-à-vis des obligations découlant du règlement, en particulier en ce qui concerne l'exercice des droits des individus et la communication des informations visées aux articles 14 et 14a. Les responsables conjoints doivent conclure un accord, qui définira lequel d'entre eux intervient en tant que seul point de contact pour les individus. Cet accord doit refléter leurs rôles respectifs et leurs relations avec les personnes concernées, et le règlement prévoit que la substance de l'accord doit être rendue disponible aux personnes concernées. Par exception, les responsables conjoints ne doivent pas conclure un tel accord lorsque et dans la mesure où leurs responsabilités respectives sont déterminées par le droit de l'Union ou le droit d'un Etat membre.

L'article 24 (2), dispose que nonobstant les termes de l'accord entre les responsables conjoints, la personne concernée peut exercer ses droits en vertu du règlement à l'égard de l'un comme de l'autre des responsables conjoints. L'article 24 (3) fait cependant exception à cette règle, pour le cas où la personne concernée a été informée de façon transparente et non équivoque de l'identité du responsable parmi les responsables conjoints, sauf en cas de fraude à ses droits.

B. Représentant d'un responsable établi hors de l'Union européenne.

En vue de renforcer l'effectivité des droits des individus à l'égard de responsables du traitement établis en dehors de l'Union européenne et qui seraient soumis à l'application du règlement en vertu de son article 3 (2), l'article 25 établit l'obligation pour un tel responsable de désigner par écrit un représentant au sein de l'Union européenne.

Il n'existe que deux exceptions à cette règle, en faveur des personnes ou des autorités publiques, et en ce qui concerne les traitements qui présentent un caractère occasionnel et qui ne risquent pas d'entraîner un risque pour les droits et libertés des individus, tenant compte de la nature, du contexte, de la portée et des finalités du traitement.

Le représentant du responsable devra être établi dans l'un des Etats membres où résident les personnes dont les données sont traitées en relation avec l'offre de biens ou de services ou bien les personnes dont le comportement fait l'objet d'un suivi (*monitoring*) par le responsable.

Le représentant doit disposer d'un mandat du responsable dans ses relations avec les autorités de contrôle et les individus, pour tout ce qui concerne le traitement des données, et ce afin d'assurer l'application conforme du règlement.

La désignation d'un représentant n'enlève rien aux obligations du responsable et elle ne porte pas préjudice aux mesures qui peuvent être prises contre ce dernier par une autorité de contrôle ou une autre autorité compétente.

C. Relations avec le sous-traitant (article 26)

Comme dans le cadre de la directive, le responsable du traitement a l'obligation de ne faire appel qu'à des sous-traitants qui présentent des garanties suffisantes et qui mettront en œuvre des mesures appropriées sur les plans technique et organisationnel pour faire en sorte que le traitement réponde aux exigences du règlement. La relation avec le sous-traitant doit être encadrée par un contrat. Ce contrat doit décrire l'objet et la durée du traitement, la nature et la finalité de celui-ci, les types de données et les catégories de personnes concernées, les droits du responsable, etc.

L'accord avec le sous-traitant doit stipuler que les données ne pourront être traitées que sur instruction du responsable, sauf lorsque le traitement est imposé par le droit de l'Union ou d'un Etat membre, auquel cas le sous-traitant en informera le responsable au préalable.

Le contrat fera aussi obligation au sous-traitant :

- de prendre les mesures requises en vertu de l'article 30 (sécurité du traitement),
- de respecter les conditions pour faire lui-même appel à un autre sous-traitant, comme par exemple une autorisation préalable et spécifique de la part du responsable ;
- de porter assistance au responsable, compte tenu de la nature du traitement, pour répondre aux requêtes des individus exerçant leurs droits en vertu du chapitre III du règlement ;
- d'assister le responsable pour la mise en conformité aux obligations découlant des articles 30 à 34 du règlement (sécurité du traitement et analyse préalable d'impact) ;
- de restituer ou de supprimer les données, au choix du responsable, quand prennent fin les services confiés au sous-traitant, sous réserve que le droit de l'Union ou d'un Etat membre n'impose la conservation des données ;
- de mettre à la disposition du responsable toutes les informations nécessaires pour établir le respect des obligations visées à l'article et pour permettre la réalisation d'audits par le responsable

D. Obligations du sous-traitant.

Le sous-traitant ne peut faire appel à son tour un autre sous-traitant sans l'accord écrit et préalable du responsable. Cet accord peut être spécial ou général, précise l'article 26 du règlement. Lorsqu'il s'agit d'un accord général, le sous-traitant demeure tenu dans tous les cas d'informer le responsable s'il a l'intention de faire appel à de propres sous-traitants, de les remplacer ou d'en ajouter de nouveaux, et ce afin de donner au responsable du traitement l'opportunité de s'opposer à de telles modifications.

Le sous-traitant a également l'obligation d'informer le responsable sans délai lorsque les instructions reçues de ce dernier, selon l'opinion du sous-traitant, constituent un manquement au règlement ou aux règles de protection des données personnelles du droit de l'Union ou d'un Etat membre.

Lorsque le sous-traitant fait appel à son tour à un sous-traitant pour exécuter certaines activités spécifiques au nom du responsable, les obligations qui s'imposent dans le contrat ou l'acte législatif entre le responsable et le sous-traitant, devront également être imposées par le sous-traitant à son sous- sous-traitant, en particulier par l'indication de garanties suffisantes pour la mise en œuvre de mesures techniques et organisationnelles appropriées pour assurer le respect du règlement. Le sous-traitant initial demeure pleinement responsable à l'égard du responsable du traitement pour les actes et omissions de ses propres sous-traitants.

4.3.3. Registre interne des traitements

Afin d'être en mesure de démontrer le respect des dispositions du règlement, le responsable du traitement ainsi que le sous-traitant sont tenus, en vertu de l'article 28 du règlement, d'organiser l'enregistrement d'une série d'informations concernant les catégories de données personnelles traitées et le traitement lui-même. Ces informations doivent être enregistrées par écrit, y compris sous une forme électronique pour autant qu'ils puissent être convertis sous forme lisible. Sur requête de l'autorité de contrôle compétente, le responsable et le sous-traitant sont tenus de mettre ces enregistrements à disposition de ladite autorité.

Les entreprises et organisations qui emploient moins de 250 personnes échappent à cette obligation, sauf si le traitement qu'elles effectuent est de nature à entraîner un risque élevé pour les droits et libertés des individus, si le traitement n'est pas occasionnel ou si le traitement porte sur des données sensibles ou se rapporte à des données concernant des condamnations ou des infractions pénales.

Le responsable et, le cas échéant, son représentant, doivent tenir à jour un registre qui contiendra les informations suivantes :

- le nom et les coordonnées du responsable ainsi que de tous responsables conjoints, du représentant du responsable et du détaché à la protection des données le cas échéant ;
- les finalités du traitement, y compris l'intérêt légitime sur lequel le traitement est basé en vertu de l'article 6 (1) (f) ;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel afférentes à celles-ci ;
- Les catégories de destinataires auxquels les données ont été ou seront communiquées, et en particulier les destinataires établis dans des Etats tiers ;
- le cas échéant, les catégories de transfert de données à caractère personnel vers un pays tiers ou vers une organisation internationale ;
- si possible, la durée envisagée pour l'effacement des différentes catégories de données personnelles ;
- si possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 30 (1) du règlement.

Quant au sous-traitant, il doit lui aussi tenir à jour un registre de toutes les opérations de traitement de données à caractère personnel effectuées pour le compte d'un responsable, et ce registre doit contenir les informations suivantes :

- le nom et les coordonnées du sous-traitant ou des sous-traitants et de chaque responsable pour le compte duquel le sous-traitant intervient, ainsi que, le cas échéant, le représentant du responsable ;
- le nom et les coordonnées du détaché à la protection des données, le cas échéant ;
- les catégories de traitements effectués pour le compte de chaque responsable ;

- le cas échéant, les catégories de transfert de données à caractère personnel vers un pays tiers ou une organisation internationale ;
- si possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 30 (1) du règlement.

4.3.4. Sécurité

A. Mesures de sécurité

L'article 30 du règlement fait obligation non seulement au responsable du traitement mais également au sous-traitant de mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité proportionné aux risques inhérents au traitement.

Le responsable et le sous-traitant ont donc tout d'abord l'obligation d'évaluer les risques inhérents au traitement et d'identifier les mesures qui seraient de nature à diminuer ces risques. À cet égard, ils tiendront compte des techniques disponibles et du coût de leur mise en œuvre, ainsi que de la nature, de la portée, du contexte et des finalités du traitement, de même que de la probabilité et de la gravité des risques pour les droits et libertés des individus. On retrouve ici l'approche basée sur le risque en matière de données à caractère personnel. Selon l'article 30 du règlement, les mesures de sécurité comprennent notamment la pseudonymisation ou l'encryptage des données, la capacité d'assurer de manière continue la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement de données personnelles, la capacité de restaurer la disponibilité et l'accès aux données dans un délai approprié en cas d'incident physique ou technique ainsi qu'un processus de vérification régulière et d'évaluation du caractère effectif des mesures techniques et organisationnelles afin d'assurer la sécurité du traitement.

Dans l'évaluation du niveau approprié de sécurité, le responsable et le sous-traitant veilleront, en particulier, à protéger les données contre la destruction accidentelle ou illicite, la perte, l'altération, la communication non autorisée ou l'accès aux données à caractère personnel transmises, stockées ou autrement traitées.

Les codes de conduite conformes à l'article 38 ou les mécanismes de certification accrédités suivant l'article 39 du règlement peuvent constituer un élément de nature à démontrer que le responsable et le sous-traitant se conforment aux exigences de l'article 30, §1 du règlement.

Par ailleurs, le responsable et le sous-traitant ont tous deux l'obligation de prendre des mesures pour s'assurer que toute personne agissant sous leur autorité et ayant accès aux données à caractère personnel, ne traitera celle-ci que sur instruction du responsable, sauf les obligations imposées par le droit de l'Union européenne ou d'un Etat membre.

B. Notification en cas d'incident de sécurité (« *data breaches* »)

On entend par « violation de données personnelles » un incident de sécurité menant à la destruction accidentelle ou illicite, à la perte, l'altération, la communication ou l'accès non autorisés à des données à caractère personnel qui font l'objet d'une transmission, d'un stockage ou d'un autre traitement (article 4(9) du règlement). Le considérant 67 du règlement indique qu'une telle violation de données personnelles peut entraîner un préjudice corporel, matériel ou moral. Dès lors, il importe que les autorités de contrôle et, le cas échéant, les individus concernés, se voient notifier le plus rapidement possible l'existence de telles violations de données personnelles. De cette façon, le responsable du traitement pourra leur faire connaître la nature des

données qui ont été atteintes, et leur faire parvenir des recommandations en vue d'atténuer les effets négatifs potentiels de la violation de données.

L'obligation de notification est imposée par les articles 31 et 32 du règlement en cas de violation de données personnelles, sauf si cet incident n'est pas susceptible d'entraîner un risque élevé pour les droits et libertés des individus.

Le responsable du traitement a l'obligation de notifier cet incident de sécurité à l'autorité de contrôle compétente en vertu de l'article 51, et ce si possible dans les 72 heures au plus tard après qu'il en ait pris connaissance. Quant à la notification aux individus concernés, le règlement prévoit simplement qu'elle doit être effectuée sans retard injustifié (article 32 (1)).

Le sous-traitant est tenu de notifier sans délai au responsable du traitement toute violation de données personnelles dont il est informé.

Le règlement précise la teneur de cette notification d'une violation de données personnelles à l'article 31 (3). Celle-ci doit à tout le moins :

- décrire la nature de l'incident de sécurité et, si possible, les catégories et le nombre approximatif d'individus concernés ainsi que les catégories et le nombre approximatif d'enregistrement de données concernées ;
- rapporter l'identité et les coordonnées de contact du détaché la protection des données ou de tout autre point de contact auprès desquels des informations supplémentaires peuvent être obtenu ;
- décrire les conséquences probables de l'incident identifié par le responsable ;
- décrire les mesures prises ou proposées par le responsable pour réagir à l'incident et le cas échéant pour en atténuer les conséquences dommageables.

Le responsable a par ailleurs l'obligation de tenir une documentation relative à toutes les violations de données personnelles, y compris les circonstances de fait et le contexte, les conséquences et les remèdes ou les actions entreprises à leur suite. Cette documentation doit permettre à l'autorité de contrôle de vérifier que le responsable s'est conformé à l'article 31 du règlement.

En ce qui concerne les notifications aux individus concernés, le règlement n'impose une communication que si les incidents sont de nature à entraîner un risque élevé pour les droits et libertés individuelles. Le responsable doit alors révéler l'identité et les coordonnées de contact du détaché à la protection des données, les conséquences possibles de l'incident et les mesures prises ou envisagées par le responsable pour réagir à l'incident de sécurité et, si cela est approprié, les mesures pour atténuer les éventuels effets négatifs de l'incident de sécurité. Les responsables ne sont donc pas tenus d'informer individuellement les personnes concernées de la nature de l'incident, des catégories et du nombre d'individus concernés ni des catégories et du nombre d'enregistrements de données concernés. Ces éléments d'information peuvent être réservés à l'autorité de contrôle.

L'article 32(3), du règlement prévoit trois exceptions à l'obligation d'informer personnellement les individus concernés.

La première exception concerne le cas dans lequel le responsable a mis en œuvre des mesures techniques et organisationnelles de protection appropriées, et que ces mesures ont été appliquées aux données concernées par l'incident de sécurité. Les mesures visées sont en particulier celles qui rendent les données inintelligibles pour toute personne non autorisées à y accéder, comme par exemple l'encryptage des données.

La deuxième exception prévue par le règlement correspond à des situations où le responsable a pris des mesures assurant que les risques pour les droits et libertés des individus ne soient plus de nature à se réaliser. Le règlement n'est pas plus précis à ce sujet.

La dernière exception est le cas où une notification individuelle requerrait des efforts disproportionnés, étant entendu que dans ce cas une communication publique ou une mesure similaire doit être faite afin que es personnes concernées soient néanmoins informées de façon aussi effective.

Lors d'une notification à l'autorité de contrôle, celle-ci vérifiera si la notification individuelle s'impose ou si l'une de ces exceptions est susceptible de s'appliquer.

4.3.5. Analyse d'impact et consultation préalable au traitement

Les auteurs du règlement ont souhaité remplacer le système de notifications systématiques et préalables imposées par la directive 95/46. Ce système était en effet jugé peu efficace et il entraînait des obligations administratives et financières importantes pour les responsables de traitement, sans contribuer à améliorer le niveau de protection des données à caractère personnel. Le nouveau système tend à mettre l'accent sur l'obligation d'effectuer une analyse préalable approfondie de certains traitements jugés plus sensibles et des mesures qui peuvent être prises pour atténuer ces risques. Dans les cas où cette analyse préalable conduit à identifier des risques particuliers, le responsable sera tenu de consulter l'autorité de contrôle indépendante avant la mise en œuvre du traitement. Le régulateur peut ainsi formuler des recommandations et exercer tous les pouvoirs qui lu sont dévolus par l'article 53 du règlement.

Lorsqu'un type de traitement est de nature à entraîner des risques élevés pour les droits et libertés des individus, le responsable est tenu, avant de mettre en œuvre ce traitement, d'effectuer une étude d'impact des opérations de traitements envisagées, au regard de la protection des données à caractère personnel. Selon l'article 33 (1) du règlement, cela pourrait être en particulier le cas lorsque en ce qui concerne les traitements qui font usage de nouvelles technologies, et plus généralement en tenant compte de la nature, de la portée, du contexte et des finalités de tels traitements.

L'article 33 (2) du règlement énumère trois catégories de situations plus précises dans lesquelles l'analyse d'impact préalable s'imposera : en cas d'évaluation systématique et exhaustive des aspects personnels de l'individu reposant sur du profilage et sur la base de laquelle seront prises des décisions de nature à produire des effets juridiques en ce qui concerne les personnes concernées ou à les impacter de manière importante ; en cas de traitement à grande échelle de catégories spéciales de données en vertu de l'article 9 (1) ou de données portant sur des condamnations ou des infractions pénales ; et enfin, en cas de surveillance d'espaces publiquement accessibles à grande échelle.

Le considérant 71 du règlement précise l'obligation de conduire une étude d'impact préalable ne s'applique pas à des traitements effectués par un médecin ou un professionnel de la santé ou encore un avocat. Dans de tels cas, le traitement ne peut être considéré comme effectué à grande échelle..

Observons que les traitements justifiés par la nécessité de respecter une obligation légale ou la poursuite d'un intérêt prépondérant d'intérêt général (articles 6 (1) (c) et (e) du règlement), ne doivent pas être soumis à une analyse d'impact, sous réserve qu'une telle obligation soit imposée par le droit national d'un Etat membre.

L'autorité de contrôle peut dresser une liste des types de traitement qui doivent faire l'objet d'une analyse d'impact, et communiquer cette liste au conseil européen de la protection des données. Elle peut également établir une liste des catégories de traitements pour lesquels une telle analyse d'impact n'est pas requise.

L'analyse d'impact doit contenir une description systématique des opérations de traitement envisagées, une évaluation de la nécessité et de la proportionnalité du traitement en rapport avec les finalités, une évaluation des risques visés ci-avant, les mesures envisagées pour gérer ces risques, notamment les mesures de sécurité, les précautions et les mécanismes pour assurer la protection des données personnelles et pour établir la conformité avec le règlement, en tenant compte des droits et des intérêts légitimes des individus et des autres personnes concernées.

Le responsable du traitement et les sous-traitants, pour évaluer la légalité et l'impact des opérations de traitement qu'ils envisagent, pourront se conformer à des codes de conduite visée à l'article 38 du règlement. Le responsable veillera à s'informer du point de vue des individus concernés ou de leurs représentants, sans préjudice à la protection des intérêts commerciaux ou des intérêt public ou des intérêts liés à la sécurité des opérations de traitement.

Sans aller jusqu'à imposer l'obligation d'obtenir une autorisation préalable de l'autorité de contrôle, l'article 34 (2) du règlement oblige le responsable du traitement à consulter cette autorité avant de mettre en œuvre un traitement pour lequel une analyse d'impact préalable, telle que visée à l'article 33, a révélé la possibilité d'un risque élevé à défaut de mesures destinées à atténuer ces risques. Si l'autorité de contrôle est d'avis que le traitement envisagé n'est pas conforme au règlement ou que les risques ne sont pas suffisamment identifiés ou atténués, elle peut, dans une période de 8 semaines au plus suivant la demande d'avis, émettre une recommandation à l'attention du responsable du traitement, par écrit, et faire usage des pouvoirs d'investigation et d'injonction qui lui sont dévolus à l'article 53. Rappelons que cette dernière disposition permet à l'autorité de contrôle non seulement d'obtenir toutes les informations nécessaires pour vérifier le respect du règlement, mais également d'émettre des injonctions de se conformer au règlement, de limiter les traitements de façon temporaire ou définitive, d'ordonner la suspension de flux de données vers un pays tiers ou d'imposer des amendes administratives.

Pour permettre à l'autorité de contrôle d'exercer sa mission, le responsable lui fournira au moins les informations suivantes : les responsabilités respectives du responsable, des responsables conjoints et des sous-traitants impliqués dans le traitement, en particulier pour les traitements au sein d'un groupe d'entreprises, les finalités et les moyens du traitement envisagé, les mesures de précaution destinée à protéger les droits et libertés des individus conformément au règlement, le cas échéant, les coordonnées du détaché à la protection des données ainsi que l'analyse d'impact préalable visée à l'article 33 et toute autre information requise par l'autorité de contrôle.

4.3.6. Détaché à la protection des données (*data protection officer*)

D'après l'article 35(1) du règlement, la désignation d'un détaché à la protection des données personnelles s'impose dans trois catégories de situations : (I) lorsque le traitement est effectué par une autorité publique, sauf les cours et tribunaux ; (ii) lorsque les activités principales du responsable ou du sous-traitant consistent en des opérations de traitement qui, en raison de leur nature, de leur portée et ou de leur finalité, nécessitent une surveillance régulière et systématique des individus à grande échelle ; (iii) lorsque les activités principales du responsable ou du sous-traitant consistent en le traitement à grande échelle de catégories sensibles de

données en vertu de l'article 9 et de données relatives à des condamnations ou des infractions pénales au sens de l'article 9a.

Cependant, l'article 35(4) dispose aussi que, dans d'autres situations, le responsable ou le sous-traitant peuvent ou, lorsque cela est imposé par le droit de l'Union ou le droit d'un Etat membre, doivent désigner un détaché à la protection des données.

Le détaché à la protection des données peut être un membre du personnel du responsable ou du sous-traitant, ou remplir sa mission sur la base d'un contrat de services indépendant. Le détaché à la protection des données doit être désigné sur la base de ses qualités professionnelles et, en particulier, de sa connaissance experte du droit de la protection des données et des pratiques en la matière ainsi que de sa capacité à remplir les missions qui lui sont dévolues à l'article 37 du règlement. Il peut se voir confier d'autres tâches et responsabilités, sous réserve que celles-ci n'entraînent pas un conflit d'intérêts.

Il devra rapporter directement au niveau de management le plus élevé du responsable ou du sous-traitant.

Le responsable ou le sous-traitant doivent publier les coordonnées de contact du détaché la protection des données et communiquer celles-ci à l'autorité de contrôle. Les personnes concernées ont le droit de contacter le détaché à la protection des données à propos de toutes les questions relatives au traitement de leurs données et pour l'exercice des droits que leur reconnaît le règlement.

Les missions du détaché à la protection des données sont énumérées à l'article 37 du règlement. Dans l'exercice de ses missions, le détaché doit avoir égard aux risques liés aux opérations de traitement, et prendre en compte la nature, la portée, le contexte et les finalités du traitement. Les missions énumérées à l'article 37 sont les suivantes :

- informer et conseiller le responsable ou le sous-traitant ainsi que les employés qui traitent des données de leurs obligations en vertu du règlement et des autres dispositions du droit de l'Union ou d'un Etat membre en matière de protection des données ;
- vérifier la conformité avec le règlement, le droit de l'Union ou le droit d'un Etat membre en matière de protection des données, et la conformité aux politiques internes du responsable du sous-traitant, en ce compris l'attribution des responsabilités, la sensibilisation et la formation du personnel impliqué dans les opérations de traitement ;
- fournir un avis à la demande en ce qui concerne l'analyse d'impact préalable et l'évaluation de son exécution en vertu de l'article 33 ;
- coopérer avec l'autorité de contrôle ;
- être le point de contact pour l'autorité de contrôle pour toutes les questions liées à la protection des données, en ce compris la consultation préalable visée à l'article 34.

D'une manière générale, le responsable ou le sous-traitant qui désignent un détaché la protection des données sont tenus de veiller à ce que celui-ci puisse exercer effectivement ses fonctions de manière appropriée. Ils doivent assister le détaché dans l'exercice de ses tâches visées à l'article 37 en lui fournissant les ressources nécessaires pour effectuer ces tâches ainsi qu'en lui donnant accès aux données à caractère personnel et aux opérations de traitement. Ils doivent veiller à ce que le détaché puisse agir de façon indépendante dans l'exercice de ses pouvoirs et qu'il ne reçoive pas d'instructions extérieures. Il ne peut se voir pénalisé pour avoir simplement exécuté ses missions.

4.4. Programmes "vie privée" ?

Pour envisager la mise en conformité de leur organisation avec l'ensemble de ces nouvelles obligations, les responsables de traitement devront probablement réfléchir à l'adoption et à la mise en œuvre de programmes complets de protection des données personnelles[19]. De tels programmes reposent sur la combinaison de différents facteurs : les aspects structurels, à travers la définition de rôles et fonctions, les aspects humains, à travers un ensemble de mesures de formation, de sensibilisation et de participation active de ceux qui prennent des décisions concernant l'usage des données au sein de l'organisation, les aspects procéduraux, à travers des lignes directrices et des mesures concrètes sur le plan opérationnel pour se conformer aux obligations issues du règlement et, enfin, les aspects techniques, à travers un ensemble de moyens logiciels et matériels permettant notamment de prévenir des incidents de sécurité, mais également de promouvoir des traitements prenant en compte la protection des données dès la conception.

Les possibilités d'auto-régulation « encadrée » offertes par les articles 38 e 39 inciteront peut-être certains responsables du traitement ou organisations représentatives à mettre en place des programmes certifiés ou au moins des guides et des bonnes pratiques pour la mise en œuvre de tels programmes.

Benjamin Docquir

SIMONT
BRAUN

Advocaten – Avocats – Lawyers

Avenue Louise 149 (box 20)
1050 Brussels – Belgium

www.simontbraun.eu

Tel: +32 (0)2 533 17 52
Fax: + 32 (0)2 543 70 90
E-mail: benjamin.docquir@simontbraun.eu

[19] Voy. pour quelques observations à ce sujet G. Skouma, L. Léonard, « Les grands changements liés à la réglementation sur la protection des données personnelles et ses implications pratiques pour les entreprises et les professionnels », in A. Grosjean (dir.), *op. cit.*, pp. 403-428, spéc. pp. 424-426.