Expertise Areas :

> New Technologies, Privacy & ICT
> E-payment, E-finance & Internet Banking
> Intellectual Property
> E-health & Telemedicine
> Cinema, Media, Entertainment, Sport & Gaming
> Commercial & Company law, Competition law

www.ulys.net

Avertissement : L'objectif du présent texte de présentation du nouveau Règlement relatif à la protection des données à caractère personnel est d'initier le lecteur à ses principales innovations en vue de lui permettre d'exploiter au mieux la banque de données/outil mise en ligne par le cabinet Ulys, contenant un premier commentaire article par article du GDPR.

Au fil de la présentation des innovations du Règlement, il est loisible au lecteur en cliquant sur l'article de son choix d'accéder pour chaque disposition, à une analyse de l'état du droit antérieur (en droit belge et en droit français) et de la nouvelle réglementation, aux considérants pertinents, ainsi qu'à un tableau de comparaison de l'évolution du texte légal.

La version du Règlement qui a servi à l'élaboration de la banque de données « GDPR Experts » d'Ulys est le texte publié le 6 avril 2016 et adopté en séance plénière ce 14 avril dernier.

Thierry LEONARD
Avocat associé (SPRL)
Avocat au Barreau de Bruxelles
thierry.leonard@ulys.net

Didier CHAUMONT
Avocat
didier.chaumont@ulys.net

Commentaire général du GDPR

N. Ref. : 15/00120
V. Ref. :

Date
20/04/2016

1. Introduction. Le Règlement général sur la protection des données marque sans aucun doute une avancée spectaculaire de la protection des personnes physiques dans l'environnement numérisé qui est aujourd'hui le leur.

Texte de compromis, il a tout à la fois tenté d'améliorer la protection des personnes concernées en tenant compte de l'évolution technologique depuis la Directive de 1995 tout en répondant à des demandes de modification du régime provenant à la fois des autorités de contrôle que des responsables, tenant compte de l'expérience acquise durant ces 20 dernières années.

Un commentaire article par article -tel qu'accessible sur le présent site- ne peut jouer son rôle d'indicateur des changements intervenus sans une vision horizontale du texte global.

C'est pourquoi vous trouverez ci-après un texte concis -mais néanmoins complet- permettant non seulement une vision abrégée du texte en projet, mais aussi une mise en exergue de ses orientations de base.

BRUXELLES

224, av. de la Couronne
1050 Bruxelles
Tél. + 32 (0)2 340 88 10
Fax + 32 (0)2 345 35 80

Société civile à forme de SCRL
RPM Bruxelles
TVA : BE 0476.702.936

PARIS

33, rue Galilée
75116 Paris
Tél. + 33 (0)1 40 70 90 11
Fax + 33 (0)1 40 70 01 38

Succursale inscrite au barreau de Paris
en application de la directive 95/5/CE

2. Un règlement qui laisse une marge d'appréciation importante aux États membres. Ce qui frappe d'emblée, c'est que le Règlement censé unifié l'ensemble des règles applicables dans les différents États membres leur laisse finalement pas mal de marge de manœuvre dans sa mise en œuvre.

Celle-ci se perçoit surtout au niveau des exceptions ouvertes aux États membres au regard des principes communs.

Les exemples sont légion. Par exemple, l'article 6 § 2 permet aux États membres d'adapter les dispositions du Règlement en vue de garantir la

conformité des traitements légitimés par la nécessité d'une disposition légale ou de l'intérêt public, l'article 8, § 1er permet aux États membres de prévoir un âge inférieur à 16 ans -mais pas en dessous de 13 ans- permettant aux enfants de s'affranchir de l'autorisation parentale pour consentir au traitement, l'article 9 relatif aux données sensibles permet largement aux législateurs nationaux de déterminer les exceptions admises au principe d'interdiction de traitement et les États membres ont la faculté de maintenir ou d'introduire des dispositions plus précises, incluant des limitations, en ce qui concerne les données génétiques, biométriques ou liées à la santé (cfr. art. 9, § 4), des différences entre États membres pourront apparaître concernant le traitement des données relatives aux condamnations, ou aux infractions pénales ou aux mesures de sécurité dès lors que les conditions de traitement se déterminent dans les législations nationales (modalités de contrôles de l'autorité publique ou autorisation législative spécifique (art. 10) etc.

3. Les considérants du Règlement. Le Règlement débute par une très longue liste de **considérants** faisant partie de son préambule.

Comme il est de plus en plus fréquent, le lecteur du Règlement est confronté à une inflation de « considérants » : près de 173 qui s'étendent sur près de 100 pages des 261 pages que compte la dernière version du texte. C'est dire si ceux-ci n'ont pas fini de révéler leurs secrets.

Si on y retrouve les considérants de motivation traditionnels, expliquant les raisons et justifications de l'intervention du législateur européen en la matière, notamment par voie de Règlement (cfr considérants 1er et s. spéc. considérants 9 et 10 qui justifient la marge de manœuvre laissée aux États membres nonobstant le choix du Règlement pour légiférer), on y trouve la plupart du temps une motivation, voire une explication des dispositions normatives contenues dans le Règlement. Par exemple, les considérants 42 et 47 concernant l'article 6 (Licéité du traitement) apportent des précisions concernant respectivement le caractère libre du consentement et la prise en compte de l'intérêt légitime du responsable du traitement dans son opposition aux droits et libertés de la personne concernée.

SI ces considérants n'ont en règle pas de valeur normative en eux-mêmes[1], force est cependant d'y voir parfois des velléités normatives qui se marquent par le fait qu'ils énoncent un contenu additionnel à celui prévu dans

[1] L'accord interinstitutionnel du 22 décembre 1998 sur les lignes directrices communes relatives à la qualité rédactionnelle de la législation communautaire, en son point 10, indique que « Les considérants ont pour but de motiver de façon concise les dispositions essentielles du dispositif, sans en reproduire ou paraphraser le libellé. Ils ne comportent pas de dispositions de caractère normatif ou de voeux politiques. ». Voy. sur la portée des considérants et les interrogations qu'ils suscitent : S. Lemaire, « Interrogations sur la portée juridique du préambule du Règlement Rome I », Rec. Dalloz, 2008, p. 2157 et s.

les dispositions qu'il est censé commenter (cfr par exemple le considérant 91 qui précise que l'analyse d'impact n'est pas obligatoire si le traitement de ces données est protégé par le secret professionnel, à l'instar des traitements des données à caractère personnel de patients ou clients par un médecin individuel, un professionnel de la santé, un hôpital ou un avocat ou le considérant 171 qui prévoit que les traitements en cours au moment de l'entrée en vigueur du Règlement, soit au vingtième jour suivant sa publication au journal officiel de l'Union européenne, devront être mis en conformité dans ce délai de deux ans). Il faut cependant être conscient du fait qu'il s'agira souvent de textes qui n'ont pu trouver de consensus politique suffisant que pour être inséré dans le texte. C'est évidemment criant concernant des règles qui, ayant d'abord été insérées dans le corps du texte, ont alors été ensuite disqualifiées et intégrées dans les considérants, faute d'accord suffisant sur leur contenu (pour un exemple significatif voy. le considérant 154 qui reprend partiellement le contenu de l'ex article 80 aa intitulé traitement de données personnelles et réutilisation des informations du secteur public).

4. Le plan du Règlement. Le Règlement est divisé en Chapitres et sections, comme suit :

-Chapitre Ier : Dispositions générales

-Chapitre II : Principes

-Chapitre III : Droits des personnes concernées :

Section 1 : Transparence et modalités

Section 2 : Information et accès aux données à caractère personnel

Section 3 : Rectification et effacement

Section 4 : Droit d'opposition et prise de décision individuelle automatisée

Section 5 : Limitations

-Chapitre IV : Responsable du traitement et sous-traitant

Section 1 : Obligations générales

Section 2 : Sécurité des données à caractère personnel

Section 3 : Analyse d'impact relative à la protection des données et consultation préalable

Section 4 : Délégué à la protection des données

Section 5 : Codes de conduite et certification

-Chapitre V : Transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales

-Chapitre VI : Autorités de contrôle indépendantes

Section 1 : statut d'indépendance

Section 2 : Compétence, missions et pouvoirs

-Chapitre VII : Coopération et cohérence

Section 1 : Coopération

Section 2 : Cohérence

Section 3 : Comité européen de la protection des données

-Chapitre VIII : Voies de recours, responsabilité et sanctions

-Chapitre IX : Dispositions relatives à des situations particulières de traitement

-Chapitre X : Actes délégués et actes d'exécution

-Chapitre XI : Dispositions finales

On admet ne pas toujours comprendre la logique du plan suivi. Pourquoi avoir par exemple relégué des dispositions de fond touchant à la responsabilité ainsi que les règles particulières à certaines situations (limitation de la liberté d'expression, règles applicables à la relation de travail, etc.) en fin de Règlement, au milieu de règles procédurales et de compétence spécifiques au droit européen ? Le chapitre IV aurait dû indiquer plus clairement qu'il visait en réalité des devoirs auxquels sont soumis les responsables de traitement et sous-traitants.

5. Concernant les dispositions générales (chapitre I). On constate peu de changements concernant les dispositions générales qui regroupent l'objet et les objectifs du Règlement (art. 1er), le champ d'application matériel (article 2)

Par contre, le champ d'application territorial (art. 3) du Règlement (et non plus des lois nationales applicables) a été modifié, tenant compte des difficultés apparues pour appliquer les règles de protection aux responsables du traitement hors UE. Dès lors que les activités de traitement sont liées à l'offre de biens ou de services à des personnes physiques situées sur le territoire de l'Union ou liées à l'observation des comportements humains, pour autant que ces comportements interviennent au sein de l'Union, le responsable et/ou le sous-traitant sera(ont) soumis au respect du Règlement.

Il est à souligner que le critère de la localisation de l'établissement vise désormais tant celui du responsable du traitement que celui du sous-traitant.

Les définitions se sont également sensiblement étoffées, même si celles reprises de la Directive sont restées assez stables (art. 4).

6. Concernant les principes relatifs au traitement de données à caractère personnel (chapitre II). L'article 5 du Règlement reprend et renforce les principes relatifs au traitement des données à caractère personnel, qui sont énoncés à l'article 6 de la directive en incluant les nouveautés suivantes :

-les principes de loyauté et de licéité du traitement sont complétés par l'énoncé d'un principe général de transparence (art. 5, § 1er, a);

-Une nouvelle exception est reconnue à l'interdiction de poursuite de finalités incompatibles avec la finalité initiale (art. 5, § 1er, b) : l'archivage dans l'intérêt public ;

- le principe de minimisation des données est consacré, selon lequel seules les données à caractère personnel qui apparaissent nécessaires à la réalisation de la finalité peuvent être traitées (art. 5, § 1er, .c).

-le devoir de sécurité et la confidentialité du traitement (art. 5, § 1er, f), qui oblige le responsable à garantir une sécurité et une confidentialité appropriées.

L'article 6 reprend les hypothèses devenues classiques de licéité du traitement : consentement de la personne, exécution d'un contrat, conformité à un devoir légal, protection des intérêts vitaux de la personne concernée ou d'une autre personne physique, l'exécution d'une mission d'intérêt public ou relevant de l'exécution d'une mission d'intérêt public et enfin l'équilibre des intérêts légitimes, droits et libertés du responsable ou d'un tiers, d'une part, et des personnes concernées d'autre part. Remarquons que logiquement cette dernière hypothèse est exclue pour les responsables autorités publiques, ce qui souligne en ce qui les concerne l'application stricte de légalité des traitements qu'elles poursuivent.

Les nouvelles finalités incompatibles avec celles initialement poursuivies restent interdites, sauf cas particulier des finalités d'archivage dans l'intérêt public, de recherches historiques et scientifiques et de statistiques (cfr sur ce point, l'art. 5, § 1er, b). Malgré un débat intense sur ce point, la seule ouverture à l'évolution des finalités est son acceptation en cas de seule compatibilité, sauf consentement de la personne concernée ou lorsqu'un texte légal spécifique le permet au regard des conditions de l'article 23, § 1er (art. 6, § 4).

Sur la base de la définition présente à l'article 4, 11), l'article 7 du Règlement détermine diverses règles relatives au consentement : charge de la preuve, degré de précision de celui-ci dans un écrit à portée plus générale, droit de retrait généralisé, appréciation de celui-ci s'il conditionne l'exécution du contrat.

L'article 8, quant à lui, introduit une règle de protection spécifique du consentement des enfants –concept non défini- en cas d'offre d'un service de la société de l'information : c'est en règle à leurs parents qu'il revient de consentir au traitement.

Le traitement des données sensibles est couvert par deux dispositions spécifiques (article 9 et article 10).

Le champ d'application matériel n'est pas fort différent de celui de la Directive (voy. cependant l'inclusion des données génétiques et biométriques). Les exceptions s'élargissent cependant aux traitements nécessaires pour des motifs d'intérêt public dans le domaine de la santé publique (cfr article 9, § 2, i)) ainsi qu'aux traitements nécessaires à des fins d'archivage dans l'intérêt public ou à des fins historiques, statistiques ou scientifiques dans les conditions fixées à l'article 89 et sur une base légale de l'Union ou de l'État membre (article 9, § 2, j).

À noter que les États membres ont la faculté de maintenir ou d'introduire des dispositions plus précises, incluant des limitations, en ce qui concerne les données génétiques, biométriques ou liées à la santé (article 9, § 4).

Le traitement des données relatives aux condamnations, aux infractions pénales ou aux mesures de sûreté n'est autorisé que pour autant qu'il ait lieu sous le contrôle de l'autorité publique ou qu'il soit autorisé par le droit de l'Union ou par la législation nationale (article 10).

Enfin, l'article 11 du Règlement insère une disposition spécifique concernant les traitements qui ne nécessitent pas (plus) d'identification des personnes concernées. Le responsable n'est pas obligé de traiter d'autres informations permettant l'identification et ne devra normalement plus répondre positivement à l'exercice des droits de ces personnes (accès, effacement, limitation du traitement, etc.).

7. Concernant les droits des personnes concernées (chapitre III).

Deux tendances marquantes apparaissent quant à la règlementation des droits des personnes :

(1) l'augmentation du devoir de transparence. L'article 12 oblige le responsable du traitement à prévoir des procédures et des mécanismes permettant à la personne concernée d'exercer ses droits. Un principe général de transparence est proclamé : toute information adressée au public ou à la personne concernée doit être aisément accessible et facile à comprendre dans une forme concise et transparente, et formulée en termes simples et clairs – spécialement à l'égard d'un enfant-.

La disposition prévoit les modalités d'information (par écrit ou d'autres moyens). Des délais de réaction maximum sont prévus selon les droits en cause. Le principe de gratuité d'exercice des droits est généralisé.

Le devoir d'information en cas de collecte auprès de la personne concernée est du reste étendu à des informations supplémentaires (l'intérêt légitime qui justifie le traitement, les transferts de données vers des pays tiers, le droit de réclamation auprès de l'autorité de contrôle, etc.). D'autres informations peuvent devoir être communiquées si elles apparaissent comme nécessaires à un traitement équitable et transparent (la période de conserva-

tion des données ou à tout le moins les éléments permettant de la déterminer, l'existence de l'ensemble des droits reconnus à la personne, l'existence d'une prise de décision automatisée comprenant un profilage ainsi qu'une information significative de la logique sous-jacente et les conséquences du traitement pour la personne, etc.) (art. 13).

Un régime analogue d'information est organisé par l'article 14 en cas de collecte auprès d'un tiers. Des exceptions sont alors prévues (la personne dispose déjà des informations, si elle s'avère impossible ou nécessiterait des efforts disproportionnés, etc.).

Le droit d'accès prévu par l'article 15 n'innove pas réellement. La personne concernée a le droit d'obtenir la confirmation que des données la concernant sont ou ne sont pas traitées et dans l'affirmative, la personne concernée a le droit d'y accéder. Une information spécifique doit être donnée suite au droit d'accès. Si elle le demande, la personne concernée a le droit à une copie des données.

Le droit de rectification de l'article 16 du Règlement est également en droit ligne de la disposition prévue antérieurement dans la Directive.

L'article 19 met en place une obligation de notification à charge du responsable de traitement qui l'oblige à communiquer à chaque destinataire des données toute rectification, effacement ou limitation du traitement sur la base de l'article 16, l'article 17, paragraphe 1, et de l'article 18 du Règlement. Le responsable peut toutefois se soustraire à cette obligation s'il démontre qu'une telle communication se révèle impossible ou suppose un effort disproportionné

(2) *la reconnaissance ou la consécration de nouveaux droits reconnus à la personne concernée* Le nouvel environnement web2.0 et les réseaux sociaux en particulier ont accentué la perte de contrôle des personnes sur les informations qui les concernent. Le nouveau Règlement tente donc de permettre à l'individu de reprendre la maîtrise de données qu'il projette et dissémine dans ses pérégrinations virtuelles, en reconnaissant de «nouveaux » droits aux personnes concernées par les données.

Au titre des nouveaux droits inscrits dans le règlement, on retiendra spécifiquement :

-le droit à l'oubli numérique et à l'effacement -inspiré de la jurisprudence Costeja- (article 17). L'apport majeur du futur Règlement est de fixer les hypothèses permettant d'obtenir l'effacement ainsi que les conditions d'exercice du droit à l'oubli numérique. On note par exemple l'obligation d'informer ensuite les tiers à qui les données effacées ont antérieurement été transmises, afin d'effacer aussi tout lien vers ces données ou les copies ou reproductions qui en ont été faites ainsi que les exceptions prévues (exercice de la liberté d'expression et d'information, respect d'une obligation légale, etc.)

-le droit à la limitation du traitement (article 18) qui permet à la personne concernée de faire suspendre le traitement et donc, le cas échéant, la publication des données dans différentes hypothèses : lorsqu'elle conteste l'exactitude d'une donnée, le temps que le responsable puisse contrôler celle-ci ; si le traitement est illicite et qu'elle s'oppose néanmoins à leur effacement, préférant une telle limitation, lorsque quoique n'étant plus nécessaires à la poursuite des finalités du traitement, la personne concernée en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice, etc.

- Le droit à la portabilité des données est le droit le plus novateur du futur Règlement (art. 20). Ce dernier apparaît comme un droit d'accès amélioré, auquel est associée une exigence d'interopérabilité et de retrait. L'objet du droit est de reprendre possession des données que l'on a communiquées au prestataire et de les (faire) transmettre d'un système de traitement automatisé à un autre. L'exercice de ce droit est conditionné par le fait qu'il doit nécessairement s'agir d'un traitement automatisé légitimé par le consentement de la personne -fusse concernant des données sensibles- ou par la nécessité d'exécution d'un contrat conclu entre la personne concernée et le responsable.

Deux autres droits se voient encore remodelés par le Règlement.

Le droit général d'opposition (article 21), exercé pour des raisons tenant à la situation de la personne concernée, est seulement ouvert en cas de légitimation du traitement basé sur la nécessité de l'exécution d'une mission d'intérêt public (article 6, § 1er, e) ou sur la base de l'intérêt légitime prépondérant du responsable ou d'un tiers, en ce compris le profilage effectué sur ces bases (art. 6, § 1er, f). Le Règlement prévoit également -comme la Directive auparavant- que la personne concernée peut s'opposer à tout moment au traitement de ses données à caractère personnel à des fins de prospection, en ce compris aussi le profilage effectué dans ce but (art. 19, § 2).

Le droit de ne pas être soumise à une décision automatisée est prévu à l'article 22 du futur Règlement. Il s'agit de la décision résultant exclusivement d'un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière sensible. Il y inclut expressément le profilage. Cette disposition étend cependant les exceptions possibles à l'interdiction. L'interdiction est renforcée pour les décisions fondées sur un traitement de données sensibles au sens de l'article 9 §1er du Règlement qui restent interdites sauf si la personne a donné son consentement explicite au sens de l'article 9, § 2, a) ou si le traitement est nécessaire pour des motifs d'intérêt public important au sens de l'article 9, § 2, g) (art. 22, § 4).

Enfin, l'article 23 du Règlement, directement inspiré de l'article 13 de la Directive, précise que les États membres peuvent maintenir ou introduire par voie législative des limitations aux droits de la personne concernée prévus aux articles 12 à 22 et à l'article 34 relatif à la communication à la personne concernée d'une violation de données à caractère personnel et aux

principes énoncés à l'article 5, pour autant que ces limitations respectent l'essence des droits et libertés fondamentaux et qu'elles constituent une mesure nécessaire et proportionnée dans une société démocratique pour garantir certains intérêts énumérés limitativement.

8. Concernant le responsable du traitement et le sous-traitant (Chapitre IV). Le chapitre IV regroupe deux types de dispositions : les 1ères ont trait à la qualification de responsable de traitement et de sous-traitant, à leur statut et organisation interne ainsi qu'à leurs devoirs réciproques(1), les secondes prévoient les devoirs généraux et particuliers quant à la mise en œuvre des mesures de protection prévues par le nouveau Règlement qui sont mis à charge desdits responsables (2),voire des deux (3).

(1) Statut, qualification et devoirs réciproques des responsables et sous-traitants : L'article 26 du Règlement détermine les devoirs spécifiques aux responsables conjoints qui doivent principalement conclure un accord entre eux afin de définir de manière transparente leur responsabilité et rôle dans l'exécution des devoirs qui leur incombent en application du règlement et en informer du contenu les personnes concernées par les données.

L'article 28 du Règlement concerne le régime spécifique de la sous-traitance. Il amplifie les devoirs antérieurs des responsables et sous-traitants tout en organisant un régime de sous-traitance distinct des devoirs de sécurité prévus à l'article 32 et s. Le principe reste encore celui d'une organisation contractuelle spécifique entre le responsable du traitement et le sous-traitant. Le contenu du contrat écrit -en ce compris un format électronique- c'est-à-dire les obligations du sous-traitant est par contre très élargi. Le Règlement organise la question de la sous-traitance confiée à des tiers -sous-traitants secondaires- par le sous-traitant direct du responsable du traitement, cas de figure très fréquent en pratique.

L'article 29 du nouveau Règlement prévoit désormais que toute personne agissant sous l'autorité d'un responsable du traitement ou d'un sous-traitant et qui a accès aux données ne pourra également traiter les données que sur instructions du seul responsable du traitement (voy. néanmoins l'article 32, § 4 qui vise également le sous-traitant), à moins que le droit de l'Union ou d'un État membre ne le prévoie autrement.

(2) Devoirs du Responsable du traitement : Le premier devoir général du responsable du traitement est un « principe général de responsabilité » (article 24). Il affirme la responsabilité particulière du responsable de traitement dans la mise en œuvre des mesures techniques et organisationnelles appropriées en vue d'effectuer le traitement dans le respect du Règlement. Pour déterminer celles-ci, il y a lieu de tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que de la probabilité et de la gravité des risques au regard des droits et libertés des personnes physiques. La charge de la preuve d'une telle mise en oeuvre repose alors sur les épaules du responsable du traitement.

Deux devoirs spécifiques en découlent et tenter de lui donner un contenu plus précis.

Selon le paragraphe 1er de l'article 25, le principe de *data protection by design* (protection dès la conception) oblige le responsable du traitement à prendre des mesures et procédures techniques et organisationnelles appropriées – tant lors de la conception du traitement que dans sa mise en œuvre- afin de le rendre conforme au Règlement, compte tenu des risques présentés par celui-ci. Parmi ces mesures, le paragraphe 1er cite la minimisation (cfr article 5, § 1er, c) et la pseudonymisation (cfr. article 4, 5).

Le second paragraphe de l'article 25 aborde le principe de *data protection par default* (protection par défaut). Il oblige le responsable à adopter des mesures consistant à limiter par défaut le traitement de données à caractère personnel à ce qui est strictement nécessaire, en ce qui concerne la quantité de données traitées, leur accessibilité et à leur période de conservation.

L'article 33 du Règlement généralise le devoir de notification des violations de données (« data breach ») à l'autorité de contrôle tout en le précisant. Toute violation de donnée doit faire l'objet d'une notification par le responsable du traitement, sauf si la violation ne paraît pas faire courir de risque aux droits et libertés individuelles des personnes concernées. Le sous-traitant doit quant à lui informer le responsable de toute violation de données sans retard injustifié après en avoir pris connaissance. Le contenu minimal de la notification et ses délais –dont une partie peut être différée- est également prévu par la disposition.

L'article 34 n'oblige le responsable à notifier à la personne concernée que les violations de données susceptibles d'exposer les personnes physiques à un risque élevé (« high risk ») à leurs droits et libertés selon des modalités analogues à celles destinées à l'autorité de contrôle. L'article 34 §3 prévoit par contre diverses exceptions à la notification aux personnes.

L'article 35 prévoit que lorsqu'un traitement est susceptible d'exposer les personnes à un risque élevé au regard de leurs droits et libertés, notamment ceux qui recourent aux nouvelles technologies, le responsable doit effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la portée, le contexte, la particularité et la gravité de ce risque. La disposition précise les hypothèses donnant lieu ou non à l'analyse ainsi que le contenu de celle-ci.

Le responsable doit consulter l'autorité de contrôle avant la mise en œuvre du traitement uniquement, et selon les modalités précisées, lorsque l'analyse d'impact mené par le responsable du traitement en application de l'article 35, révèle que le traitement présente un risque élevé en cas d'absence de mesures appropriées prises par le responsable afin d'atténuer le risque (article 36).

(3) Devoirs communs aux responsables et sous-traitants : En cas d'application de l'article 3, § 2, l'article 27 du Règlement oblige les responsables du traitement et les sous-traitants qui ne sont pas établis dans l'Union à y désigner un représentant, lorsque le règlement s'applique à leurs activités de traitement.

À l'article 30 du Règlement, le législateur de l'Union a fait choix de remplacer le devoir de notification à l'autorité de contrôle par une obligation à charge des responsables du traitement **et** des sous-traitants, de conserver une trace documentaire des opérations de traitement sous leur responsabilité. Ainsi, tant les responsables que les sous-traitants (et le cas échéant, leurs représentants) devront tenir des registres pour toutes les catégories d'activités de traitement relevant de leur responsabilité c'est-à-dire pour chacun des traitements qu'ils mettent en oeuvre. Ceux-ci seront mis à disposition des autorités de contrôle sur demande de celles-ci.

L'article 31 du Règlement institue un devoir spécifique des responsables de traitement et des sous-traitants -ainsi que de leur représentant, le cas échéant- qui doivent coopérer à la demande des autorités de contrôle, dans l'exécution de leurs missions.

L'article 32 du Règlement reprend en substance, en les étendant, le contenu des dispositions de la Directive relatives aux devoirs de sécurité. L'objet principal de l'obligation reste la mise en œuvre des mesures techniques et organisationnelles appropriées par le responsable du traitement et le sous-traitant pour garantir un niveau de sécurité approprié au risque. Celles-ci sont cependant largement exemplifiées par le texte lui-même.

L'article 37 du Règlement a arrêté trois cas dans lesquels la désignation d'un délégué à la protection des données est obligatoire au sein de l'organisation du responsable du traitement et du sous-traitant :

- lorsque le traitement est effectué par une autorité ou un organisme public, à l'exclusion des juridictions agissant dans le cadre de leur compétence judiciaire (art. 37, paragraphe 1, a) ;

- lorsque les activités de base du responsable ou du sous-traitant consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes concernées (art. 37, paragraphe 1, b) ;

- lorsque les activités de base du responsable ou du sous-traitant consistent en des traitements à grande échelle de données sensibles au sens de l'article 9 du Règlement (art. 37, paragraphe 1, c).

Le responsable, le sous-traitant ou des associations ou autres organismes qui représentent des catégories de responsables ou de sous-traitants peuvent ou, le cas échéant, doivent désigner un délégué à la protection des données si le droit de l'Union ou le droit d'un État membre l'exige (art. 37, § 4).

L'article 38 impose -sous le titre de fonction (« position ») du délégué à la protection des données- au responsable du traitement ou au sous-traitant une série d'obligations en vue de permettre à ce dernier d'assumer les missions prévues quant à elles, à l'article 39 (l'associer en temps utiles à toutes les questions relatives à la protection des données, assurer son indépendance, le lier par une obligation de secret ou de confidentialité…).

Le délégué à la protection des données reçoit plusieurs missions minimales décrites à l'article 39 : une mission d'avis et de conseil (1) ; une mission de contrôle (2) ; une mission de point de contact avec l'autorité de contrôle (3).

L'article 40 organise le régime de codes de conduite élaborés par des organismes représentant des catégories de responsables ou de sous-traitants. Ils auront pour objet de préciser les modalités d'application des dispositions du Règlement. Ces codes seront soumis à l'autorité de contrôle qui est compétente au titre de l'article 55, elle-même devant les soumettre au comité européen de la protection des données s'il concerne des traitements mis en œuvre dans plusieurs États membres (art. 40, § 5 et 7).

L'article 41 autorise, aux conditions qu'il détermine, un organisme indépendant à contrôler le respect d'un code de conduite agréé visé à l'article 40, sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente. Une procédure spécifique d'agrément est prévue.

L'article 42 du Règlement -complété par l'article 43- met en place un mécanisme de certification des responsables et sous-traitants tenus de se conformer à des règles de protection. La certification ne pourra être délivrée que par un organisme spécialement agréé conformément à l'article 43 ou, le cas échéant, par l'autorité de contrôle compétente, voire par le comité de protection des données amené à intervenir, avec dans ce cas reconnaissance d'un potentiel label européen.

9. Concernant le transfert de données à caractère personnel vers des pays tiers ou des organisations internationales (chapitre V). Les règles relatives aux transferts de données vers des pays tiers ont été modifiées même si le principe de base issu de la Directive a été maintenu : l'interdiction de transfert vers des pays, territoires ou organisation internationale qui n'assurent pas un niveau de protection adéquat, même si son énoncé a été modifié. En effet, le chapitre V a pour objet d'énoncer les cas et conditions dans lesquels de tels transferts sont néanmoins permis.

Cette approche « positive » est d'abord énoncée à l'article 44 du Règlement. Cette disposition a pour objet d'énoncer le principe général régissant les transferts vers les pays ou organisations internationales tiers à l'UE. Ces transferts peuvent seulement avoir lieu si les responsables et sous-traitants qui tombent sous le champ du Règlement respectent les règles prévues par le Chapitre V.

La disposition donne cependant à la règle une extension inédite : non seulement les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale opérés dans le cadre d'un traitement en cours ou prévu sont visés , mais aussi les traitements ultérieurs du pays tiers destinataire vers un autre pays ou une autre organisation. Ils doivent donc aussi être conformes au chapitre V. du Règlement.

C'est dorénavant à la seule Commission de constater que le pays tiers, un territoire ou, un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assurent un niveau de protection adéquat, en application et selon les modalités de l'article 45 du Règlement. La Commission peut également abroger, modifier ou suspendre une décision d'adéquation si le pays tiers, le territoire ou l'organisation internationale n'assure plus un niveau de protection adéquat.

En l'absence d'une décision de la Commission constatant un niveau de protection adéquat, l'article 46 du Règlement prévoit que le transfert ne peut être effectué par le responsable ou le sous-traitant que si des garanties suffisantes sont prises par le responsable ou sous-traitant. Le choix des garanties s'étoffe et les autorités de contrôle nationales pourront intervenir dans une procédure encadrée si les garanties classiques ne peuvent être mises en œuvre pour des raisons propres au responsable ou au sous-traitant.

L'article 47 du Règlement constitue la consécration du système des règles contraignantes d'entreprises, qui peuvent être adoptées par les groupes de sociétés confrontés à des transferts intragroupes de données hors l'Union. Ces Règles d'entreprise contraignantes doivent répondre à plusieurs conditions définies par l'article 47, § 1 et 2, être approuvées par l'autorité de contrôle compétente et contenir toute une série d'informations listée dans cette disposition.

Notons aussi que la version finale du Règlement introduit un nouvel article 48 aux termes duquel un jugement judiciaire ou une décision d'une autorité administrative émanant d'un pays non membre de l'Union et imposant un transfert de données à caractère personnel ne peut être reconnu ou exécuté de quelque manière que ce soit, sauf si il se fonde sur une convention internationale, telle qu'un traité d'assistance judiciaire mutuelle, en vigueur entre ledit État tiers et l'Union et/ou l'État membre concerné.

Comme dans le régime de la Directive, le Règlement prévoit en son article 49 des dérogations spécifiques en l'absence de décision d'adéquation de la Commission (consentement explicite, transfert nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable, etc.). L'élément marquant de l'article 49 est l'introduction d'une nouvelle dérogation fondée sur la nécessité du transfert aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement ou du sous-traitant (art. 49, § 1er *in fine*).

Enfin, en relation avec les pays tiers et les organisations internationales, l'article 50 impose à la Commission et aux autorités de contrôles de prendre certaines mesures aux fins, in fine, de faciliter l'application des principes de protection des données.

10. Concernant l'autorité de contrôle (chapitre VI). Le renforcement des pouvoirs et missions des autorités de contrôle est d'évidence un des éléments forts de révision du régime de protection des données mis en œuvre par le nouveau Règlement.

Tout comme le prévoyait la Directive, le Règlement, en son article 51, fait obligation aux États membres de mettre en place une ou plusieurs autorités de contrôle indépendantes, chargée(s) de surveiller l'application du Règlement. Le but de leur intervention est précisé : d'une part, protéger les droits et libertés fondamentaux des personnes lors du traitement de leurs données à caractère personnel et, d'autre part faciliter la libre circulation des données au sein de l'Union. Elles doivent aussi à contribuer à garantir l'application uniforme du Règlement au sein de l'Union. À cette fin, elles doivent coopérer entre elles et avec la commission, conformément aux mécanismes prévus par le chapitre VII.

L'article 52 a pour objet de clarifier les conditions garantissant l'indépendance des autorités de contrôle, en application de la jurisprudence de la Cour de justice de l'Union européenne (CJUE, 9 mars 2010, C-518/07), et en s'inspirant également de l'article 49 du Règlement (CE) n° 45/200135.

L'article 53 énonce les règles générales du statut applicables aux membres de l'autorité de contrôle, en application de la jurisprudence de la CJUE (cfr. CJUE, 9 mars 2010, C-518/07), et en s'inspirant également de l'article 42, paragraphes 2 à 6, du Règlement (CE) n° 45/2001 qui encadre les traitements de données effectuées par les institutions et organes de l'Union européenne.

L'article 54 laisse aux États membres le soin de prévoir par voie législative les conditions de mise en place des autorités de contrôle. Chaque État membre fixe ainsi les conditions de nomination des membres des autorités de contrôle.

Concernant les compétences des autorités de contrôle, l'article 55 rappelle que chaque autorité est compétente, sur le territoire de l'État membre dont elle relève, pour accomplir les missions et exercer les pouvoirs dont elle est investie et exclut la compétence d'une autre autorité dite « chef de file » (cfr article 56) dans certains cas, principalement lorsque le traitement est effectué par des autorités publiques.

En cas de traitement transnational (cfr la définition à l'article 4, 23), l'article 56 du Règlement détermine l'autorité de contrôle « principale » (dite l'autorité de contrôle « chef de file ») pour les activités de traitement du responsable dans l'Union en fonction du lieu de l'établissement principal du responsable ou de son lieu d'établissement unique. L'objectif est qu'une seule autorité de contrôle soit compétente pour surveiller les activités du responsable du traitement ou du sous-traitant poursuivies dans toute l'Union et pour prendre les décisions y afférentes.

L'article 57 définit les missions qui sont confiées aux autorités de contrôle. Elles sont de différents types : des missions de surveillance, d'investigation et de contrôle, missions d'information et de conseil, d'assistance mutuelle, de gestion des plaintes et réclamations, etc.

L'article 58 prévoit de manière assez précise trois types de pouvoirs dont les États membres doivent, par voie législative, doter leur autorité nationale

de contrôle : pouvoirs d'enquête, pouvoir de prendre des mesures correctrices et pouvoirs d'autorisation et de conseil.

Enfin, l'article 59 organise le devoir pour chaque autorité de contrôle d'émettre et de publier un rapport annuel de leurs activités.

11. Concernant la coopération et la cohérence (chapitre VII). L'article 60 du Règlement fait obligation à l'autorité « chef de file » de coopérer avec les autres autorités de contrôle concernées en vue de parvenir à un consensus en cas de débat potentiel sur la désignation de la ou des autorités de contrôle compétentes. Une procédure – assez complexe — est prévue par cette disposition en vue de parvenir à un équilibre (trop ?) subtil entre les compétences conjointes des différentes autorités.

L'article 61, quant à lui, fixe des règles explicites et uniformes en matière d'assistance mutuelle obligatoire entre autorités de contrôles nationales et prévoit les conséquences en cas de refus de se conformer à la demande d'une autre autorité de contrôle.

L'article 62 instaure le principe selon lequel les autorités pourront, en cas de besoin, mener des opérations conjointes de nature diverse, telles que des enquêtes conjointes ou des mesures répressives conjointes, aux conditions qu'il détermine.

Dès lors que les autorités de contrôle voient leurs missions et compétences augmenter, et que la marge de manœuvre laissée aux États membres dans la mise en œuvre du Règlement reste assez importante, le risque d'interprétations divergentes des règles de protection ou de décisions incompatibles augmente nécessairement. C'est pourquoi l'article 64 introduit le principe du contrôle de la cohérence selon lequel les autorités de contrôle doivent coopérer entre elles et, le cas échéant, avec la Commission au travers des mécanismes mis en œuvre par l'article 64 à l'article 67, en vue d'assurer à la cohérence globale de l'application du Règlement au travers de l'Union.

Ces mécanismes consistent à :

- solliciter l'avis du Comité européen de la protection des données sur certains projets de décisions des autorités nationales avant leur adoption (art. 64) ;

- solliciter une décision obligatoire du Comité européen pour la protection des données en cas de différends entre autorités nationales (art. 65) ;

- permettre à une autorité, dans certains cas, d'adopter des mesures provisoires selon une procédure d'urgence (art. 66, § 1er) voir même des mesures définitives après avoir requis l'avis urgent du Comité européen (art. 66, § 2).

L'article 67 du Règlement confère aussi des compétences d'exécution à la Commission afin de définir les modalités de l'échange d'informations par

voie électronique entre les autorités de contrôle nationales et/ou européennes.

Le Comité européen de la protection des données, amené à remplacer feu le Groupe 29, jouera un rôle majeur dans ce système de contrôle de cohérence. C'est pourquoi il ne faut pas s'étonner de voir le Règlement lui consacrer de nombreuses dispositions (articles 68 à 76).

L'article 68 prévoit la constitution et la composition d'un Comité européen de la protection des données, doté de la personnalité juridique et représenté par son président, en lieu et place du Groupe Article 29. L'article 69 consacre son indépendance.

Ses nombreuses missions sont consignées à l'article 70 du Règlement : garantir le mécanisme de surveillance, conseiller la Commission, émettre des lignes directrices et recommandations, etc. L'article 71 l'oblige à présenter un rapport annuel sur ses activités et l'article 72 prévoit les modalités de son processus décisionnel (quorum, etc.). L'article 73 prescrit les règles relatives à la désignation et au statut du Président du Comité. L'article 74 détermine les missions qui lui incombent de manière spécifique.

L'article 75 prévoit que le secrétariat du Comité est assuré par le Contrôleur européen à la protection des données et en définit les missions. De manière générale, le secrétariat doit fournir un soutien analytique, administratif et logistique au Comité. L'article 76 prévoit expressément que les débats du comité européen de la protection des données sont confidentiels, lorsque le Comité l'estime nécessaire, selon son Règlement d'ordre intérieur.

12. Concernant les voies de recours, la responsabilité et les sanctions (chapitre VIII). Il s'agit sans doute d'un des chapitres qui aura le plus d'implications pour l'avenir. Il renforce en effet considérablement les moyens de protection des personnes concernées ainsi que les sanctions applicables aux responsables de traitement et sous-traitants.

L'article 77 du Règlement investit toute personne concernée par un traitement du droit d'introduire une plainte auprès d'une autorité de contrôle, si celle-ci estime que le traitement de données à caractère personnel la concernant n'est pas conforme aux règles européennes.

Le droit à un recours juridictionnel contre une décision d'une autorité de contrôle est consacré à l'article 78 comme un élément essentiel de la protection des personnes à l'égard des traitements de données à caractère personnel.

L'article 79 confère aux personnes concernées par un traitement, un véritable droit à un recours juridictionnel effectif contre le responsable du traitement ou un sous-traitant en cas d'atteinte à leurs droits, résultant du traitement de leurs données en violation du Règlement. Un règlement procédural spécifique (suspension ou jonction) est prévu à l'article 81 en cas de saisine de juridictions dans différents États.

L'article 80 précise et complète la faculté de représentation par une association, déjà prévue par la Directive. Le troisième paragraphe autorise les États membres à investir les associations chargées de la protection des droits et des libertés dans le cadre de traitement de données d'importants pouvoirs d'action.

L'article 82 du Règlement confirme en le précisant le principe de la réparation du préjudice matériel ou immatériel subi par toute personne résultant d'une violation du Règlement (§ 1er). La réparation peut être obtenue « du responsable du traitement » ou du « sous-traitant ». La disposition précise également en son § 2 les faits générateurs et exclusions de responsabilité propres à chacun des deux acteurs. L'article prévoit aussi une responsabilité solidaire entre responsables, mais aussi entre le responsable et le sous-traitant ayant participé au traitement.

En vertu de l'article 83 du nouveau Règlement, les autorités de contrôle reçoivent la compétence de prononcer des amendes administratives pour la plupart des violations du Règlement. Cette disposition prévoit de nombreux critères à prendre en compte dans la fixation du montant de l'amende. Elle prévoit également deux catégories de fourchettes (jusque 10 millions Eur ou 2% du CA annuel total/jusque 20 millions Eur ou 4% du CA annuel total) spécifiques à certaines violations visées par la disposition.

Concernant les autres sanctions, l'article 84 indique que les États membres doivent en déterminer le régime et prendre toutes les mesures nécessaires pour garantir leur mise en œuvre.

13. Concernant les dispositions relatives à des situations particulières de traitement de données (Chapitre IX). Ce chapitre contient certains régimes spécifiques propres à des catégories de traitements particuliers. En réalité, la plupart du temps, le Règlement s'en remet aux États membres quant à la détermination du contenu des règles.

L'article 85 du Règlement prévoit ainsi que les États membres devront réconcilier par la loi les principes de protection des données qu'elle vise avec la liberté d'expression et d'information.

L'article 86 stipule quant à lui que les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public ou un organisme privé pour l'exécution d'une tâche réalisée dans l'intérêt public peuvent être communiquées par ladite autorité ou ledit organisme afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données.

À l'instar de la Directive, l'article 87 autorise les États membres à fixer des conditions spécifiques concernant le traitement d'un numéro d'identifiant national ou de tout autre identifiant d'application générale. Les États membres sont libres de prévoir un régime juridique particulier pour le traitement des numéros d'identification national, à la condition que les droits et les libertés des personnes consacrés par le futur Règlement soient garantis.

L'article 88 du Règlement s'en remet également aux États concernant les ajustements de la protection des données dans la relation de travail. Des règles plus précises pour assurer la protection des droits et des libertés peuvent en effet être prévues par les États membres, soit par voie législative ou au moyen de conventions collectives.

L'article 89 du Règlement prévoit des dérogations expresses à certaines des règles contenues dans le Règlement pour les finalités à des fins scientifiques, statistiques ou historiques. Il étend également le champ d'application en ajoutant la finalité d'archivage dans l'intérêt public.

L'article 90 autorise les États membres à adopter des règles particulières afin de protéger le secret professionnel ou d'autres obligations de secret équivalentes dans le cadre de l'exercice des pouvoirs d'investigation des autorités de contrôle.

L'article 91 autorise les églises et les associations ou communautés religieuses à continuer à appliquer les règles relatives à la protection des données qui sont en vigueur à la date d'entrée en vigueur du Règlement, pour autant que ces règles soient mises en conformité avec les dispositions du Règlement.

14. Concernant les actes délégués et les actes d'exécution (chapitre X). L'article 92 définit les conditions relatives à l'exercice du pouvoir de la Commission d'adopter des actes délégués (pour préciser certains critères ou exigences, par exemple), en exécution de certaines dispositions du Règlement.

D'autres dispositions chargent la Commission des prendre des mesures d'exécution qui doit alors respecter les procédures prévues à l'article 93 du Règlement.

15. Concernant les dispositions finales (chapitre XI). L'article 94 abroge la Directive à partir du moment où le Règlement est d'application, soit 2 ans après le 20e jour suivant sa publication au Journal officiel de l'Union européenne et règle le problème des actes pris sous son couvert une fois le Règlement adopté.

L'article 95 clarifie la relation avec la Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

L'article 96 précise que les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales qui ont été conclus par les États membres avant l'entrée en vigueur du Règlement et qui sont conformes à la Directive 95/46/CE restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation.

L'article 97 du Règlement renouvelle la mission d'évaluation et de révision de la Commission qui doit soumettre des rapports d'évaluation au Parle-

ment et au Conseil à intervalles réguliers (4 ans). La Commission est en outre investie, par l'article 98, du pouvoir de soumettre des amendements législatifs à d'autres instruments juridiques relevant du droit de l'Union en matière de protection des données.

L'article 99 précise que le Règlement n'entre en vigueur que le vingtième jour suivant sa publication au Journal officiel de l'Union européenne. Il ne sera toutefois applicable que dans les deux ans à partir de son entrée en vigueur.

Le Règlement ne prévoit pas de régime transitoire, mais, étrangement, donne certains principes de transition dans le considérant 171.

Bruxelles, avril 2016

Thierry LEONARD et Didier CHAUMONT