Union des Villes et Communes de Wallonie asbl

RGPD – NOUVEAU RÈGLEMENT EUROPEEN EN MATIERE DE PROTECTION DE LA VIE PRIVEE

Marie-Laure Van Rillaer, Conseiller

A été signé le 27 avril 2016 le nouveau règlement européen relatif à la protection des données à caractère personnel[1] destiné à remplacer la directive 95/46/CE[2]. La matière de la protection des données à caractère personnel, qui constitue un pan de la protection de la vie privée, est aussi dense que complexe. Elle n'est pas facilement appréhendable par les administrations publiques locales, d'autant qu'elle s'immisce dans de nombreuses matières où les pouvoirs locaux œuvrent. Les domaines touchés par les données à caractère personnel sont vastes : données à caractère fiscal, données issues du registre national ou de la banque-carrefour de la sécurité sociale, données issues du développement économique local ou encore les données relatives au personnel employé par le pouvoir local quel qu'il soit. Le présent article entend faire un tour d'horizon global dans le nouveau règlement, sans prétendre à l'exhaustivité[3].

Ce règlement amène de nombreuses nouveautés visant à protéger davantage les données à caractère personnel dans un monde ultra-numérisé et ultra-connecté.
L'accent est donc résolument mis sur la sécurité et l'intégrité des données et les obligations des responsables de traitement de ces données sont renforcées

A l'heure d'écrire ces lignes, n'est pas encore connue la manière dont la ou les autorité(s) compétente(s) implémentera(ont) ce nouveau règlement dans le droit belge. L'on rappellera utilement la distinction entre le règlement européen et la directive européenne. Le premier type d'instrument juridique, le règlement, reçoit une « *applicabilité directe complète (en ce qu'il est apte à conférer des droits et des obligations aux particuliers non seulement dans leurs relations avec les Etats membres (…) mais également dans leurs relations interindividuelles* »[4]. La directive, par contre, nécessite des mesures de mise en œuvre par l'Etat membre. Même si ce nouveau règlement ne nécessite en théorie pas de transposition, il est clair que la loi[5] qui régit la matière devra être revue. L'on se souviendra en outre que cette loi

[1] Ci-après, le règlement ; Règlement 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27.4.2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, 4.5.2016.
[2] Ci-après la directive ; Directive 95/46/CE du Parlement européen et du Conseil, du 24.10.1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.U.E.*, 23.11.1995.
[3] Pour un commentaire doctrinal plus approfondi, le lecteur se référera utilement à : C. de TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016/62, p. 5 et s. ; ainsi qu'à : https://www.gdpr-expert.eu/#textesofficiels; ne sont notamment pas évoqués le champ d'application territorial, les transferts de données transfrontières ou la coopération entre autorités de contrôle.
[4] S. VAN RAEPENBUSCH, *Droit institutionnel de l'Union européenne*, Bruxelles, Larcier, 2001, p. 493.
[5] Loi du 8.12.1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18.3.1993.

générale est complétée par des réglementations plus précises qui touchent l'un ou l'autre domaine plus spécifique. L'on songe notamment aux données contenues dans la banque-carrefour de la sécurité sociale[6] ou dans le registre national[7]. A notre sens, ces lois devront être revues également.
Au titre de prémisse, il convient de rappeler les éléments suivants qui constituent les notions triangulaires de la réglementation :

- La notion de *donnée à caractère personnel* : toute information se rapportant à une personne physique[8] identifiée ou identifiable ; est réputée être une personne physique identifiable, une personne physique qui peut être identifiée, directement ou indirectement, notamment via un nom, un numéro d'identification, des données de localisation, un identifiant ou un élément spécifique se rapportant à l'identité physique, physiologique, génétique, psychique, économique, culturel ou social[9].
- La notion de *traitement de données* à caractère personnel : toute opération ou ensemble d'opérations appliquées à des données, telles que la collecte, l'enregistrement, la conservation, la consultation, la communication par transmission, la diffusion ou la mise à disposition[10].
- La notion de *responsable de traitement* : il s'agit de la personne, physique ou morale, l'autorité publique qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement[11].

1. Traitement des données à caractère personnel

1.1. Principes de traitement des données à caractère personnel

Les données à caractère personnel ne peuvent être utilisées, c'est-à-dire traitées, de manière libre puisqu'elles constituent un aspect de la vie privée des personnes physiques que cette réglementation tend à protéger.
C'est pourquoi les données doivent être :

- traitées de manière licite, loyale et transparente (principes de licéité, loyauté et transparence);
- collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités (principe de limitation des finalités) ;
- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités (principe de minimisation des données) ;
- exactes et, si nécessaire, tenues à jour (principe d'exactitude) ;
- conservées pour une durée n'excédant pas celle nécessaire au regard des finalités (principe de limitation de la conservation) ;
- traitées de façon à garantir une sécurité appropriée d'elles-mêmes (principes d'intégrité et de confidentialité qui constituent une nouveauté) [12].

[6] Loi du 15.1.1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, *M.B.*, 22.2.1990
[7] Loi du 8.8.1983 organisant un registre national des personnes physiques, *M.B.*, 21.4.1984.
[8] Ni les personnes morales ni les personnes décédées ne sont protégées par cette réglementation.
[9] Art. 4, 1) du règlement.
[10] Art. 4, 2) du règlement.
[11] Art. 4.7) du règlement.
[12] Art. 5 du règlement.

Au rang de la première condition, celle relative notamment à la licéité du traitement, le règlement reprend presqu'à l'identique ce qui était autrefois contenu dans la directive[13] : le traitement n'est possible que si, et dans la mesure où – cette précision est neuve – il se situe dans l'une des hypothèses suivantes:

- la personne concernée a consenti au traitement pour la ou les finalité(s) spécifique(s) ; dans cette hypothèse, le responsable de traitement doit être en mesure de démontrer le consentement de la personne concernée, sollicité dans une forme claire et accessible et retirable à tout moment par elle[14] ; « *il sera considéré comme ayant été librement donné uniquement si la personne concernée dispose d'une véritable liberté de choix ou est en mesure de refuser ou de retirer son consentement sans subir de préjudice* »[15] ; les considérants du règlement précisent que le consentement n'est pas valable s'il est obtenu par le silence, par des cases cochées par défaut ou en raison d'une inactivité[16] ; l'on notera l'attention portée par l'Union européenne au consentement des enfants par la consécration d'une disposition particulière[17] ; en quelques mots, le responsable de traitement doit se soucier de ce que l'enfant a au moins 16 ans pour que le traitement soit licite[18] ; à défaut, le consentement ne pourra être donné que par le titulaire de la responsabilité parentale[19] ;

- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ; il s'agit par exemple du cas entre une intercommunale, l'employeur, et son travailleur ;

- le traitement est nécessaire au respect d'une obligation légale (ou décrétale ou découlant d'une ordonnance) à laquelle le responsable de traitement est soumis ; cette hypothèse de traitement autorise le traitement de données à caractère personnel lorsqu'une loi ou un décret le prévoit (sans préjudice des autres conditions de traitement), l'on peut songer au traitement des données effectué en vue de la tenue par l'autorité de contrôle du cadastre des mandats et des rémunérations[20] ;

- le traitement est nécessaire à la sauvegarde des intérêts vitaux d'une personne ;

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement[21] ; sous l'ère de la directive, l'on ne disposait que de peu d'informations sur cette hypothèse de traitement licite des données à

[13] Art. 7 de la directive.
[14] Art. 7 du règlement.
[15] C. de TERWANGNE, K. ROSIER et B. LOSDYCK, *op. cit.*, p. 41.
[16] Considérant 32 du règlement.
[17] Art. 8 du règlement.
[18] Notons à cet égard que le règlement permet aux Etats membres de rabaisser cet âge jusqu'à 13 ans : art. 8.1, al. 2 du règlement.
[19] Art. 8.1, al. 1er du règlement.
[20] Art. L5111-1 et s. du CDLD
[21] Et non plus le tiers auquel les données sont communiquées, comme le prévoyait l'article 7, e) de la directive.

caractère personnel alors que cette hypothèse paraît être une voie royale pour le traitement des données par les autorités publiques locales ; le nouveau règlement apporte des précisions bienvenues[22] : « *Les finalités du traitement sont définies dans cette base juridique ou (…) sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, (…). Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi* ». Le considérant 41 du règlement précise encore : « *cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme* » ;

- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée (hypothèse non applicable en cas de traitement par les autorités publiques)[23].

1.2. Condition de collecte des données « classiques »

Le règlement impose aux responsables de traitement de fournir, au moment de la collecte des données à caractère personnel, à la personne concernée plusieurs informations :

- l'identité et les coordonnées du responsable de traitement ;
- les coordonnées du délégué à la protection des données (*cf. infra*) ;
- les finalités du traitement ainsi que la base juridique du traitement ;
- les destinataires des données ;
- la durée de conservation ou ce qui permet de la déterminer ;
- l'existence de multiples droits de la personne concernée (*cf. infra*) ;
- l'existence d'un éventuel profilage[24].

Le règlement impose également aux responsables de traitement la communication de pareils éléments lorsque les données n'ont pas été collectées directement auprès de la personne concernée[25]. L'on y rajoutera tout de même l'obligation de mentionner la source d'où proviennent les données et le cas échéant la mention qu'elles sont issues ou non de sources accessibles au public[26]. Mais le règlement

[22] Art.6, § 3, al. 2 du règlement.
[23] Art. 6.1, al. 2, du règlement.
[24] Art. 13 du règlement.
[25] Art. 14 du règlement.
[26] Art. 14.2.f) du règlement.

précise que cette communication ne s'impose notamment pas si la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés [27]!

1.3. Données sensibles

Le règlement distingue, comme la directive, différentes catégories de données à caractère personnel dont certaines sont plus sensibles, telles que les données qui révèlent l'origine raciale, les opinions politiques, les convictions religieuses ou philosophiques, les données de santé ou l'orientation sexuelle. Une nouvelle catégorie de données sensibles s'est explicitement ajoutée aux précédentes : les données génétiques et biométriques[28].

Le traitement de ces données sensibles est en principe interdit sauf exception et est soumis à des règles particulières[29]. Parmi ces exceptions, l'on relèvera les plus intéressantes pour les pouvoirs locaux :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit européen ou national prévoit que l'interdiction ne peut pas être levée par la personne concernée;

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit européen ou national ou par une convention collective conclue en vertu du droit national qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée; (…)

e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée; (…)

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit européen, belge ou en vertu d'un contrat conclu avec un professionnel de la santé.

Une disposition spécifique est consacrée aux données à caractère personnel relatives aux condamnations pénales et aux infractions[30]. On se souviendra qu'il existe une directive spécifique relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données[31].

2. Accroissement des droits de la personne concernée

2.1. Consentement éclairé de la personne concernée

[27] Art. 14.5.b) du règlement.
[28] Art. 9 du règlement.
[29] Art. 9 du règlement.
[30] Art. 10 du règlement.
[31] Directive 2016/680 du 27.4.2016, *J.O.U.E.*, 4.5.2016.

Le règlement renforce la protection de la personne concernée en agissant sur le consentement requis, c'est-à-dire en amont du traitement. Le consentement de la personne concernée constitue l'une des hypothèses admissibles de traitement et nous avons vu juste ci-avant les nouveaux contours de ce consentement[32] : la nouvelle réglementation définit ce consentement comme la manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement[33]. L'on remarque que les consentements obtenus avant la mise en application de ce règlement ne seront plus nécessairement valables puisqu'il faudra vérifier si le consentement a été donné conformément aux (nouvelles) conditions énoncées dans le règlement[34]. De plus, la personne concernée dispose du droit de retirer le consentement donné, ce qui aura un effet sur la cause du traitement ultérieur à la rétractation de consentement[35].

2.2. Droits de la personne concernée

Le nouveau règlement augmente les droits de la personne dont on traite les données à caractère personnel. L'on dénombre les six droits suivants : droit d'accès, droit à la rectification, droit à l'effacement, droit à la limitation, droit à la portabilité des données et droit de ne pas faire l'objet d'un profilage.

2.2.1. Droit d'accès

Le règlement reprend le *droit* pour la personne concernée *d'accéder* à toute une série d'informations sur le traitement de ses données (semblables à celles qui doivent être communiquées au moment de la collecte[36]), outre le droit d'accès aux données elles-mêmes[37].
Il confirme également le *droit à la rectification de ses données*[38], déjà présent dans la directive[39].

2.2.2. « Droit à l'oubli »

Le règlement innove en définissant les modalités de ce que l'on a appelé « *le droit à l'oubli numérique* »[40] suite au fameux arrêt « Google Spain » qui avait, à l'époque, défrayé la chronique[41]. Ce droit à l'effacement s'applique notamment lorsque :

- Les données ne sont plus nécessaires au regard des finalités ;
- La personne concernée retire son consentement et qu'il n'existe pas d'autre fondement juridique au traitement ;
- Les données ont fait l'objet d'un traitement illicite.

Le responsable de traitement, tenu d'effacer les données qui ont été rendues publiques, doit prendre les mesures raisonnables, compte tenu des technologiques existantes, pour informer les autres responsables de traitement traitant ces mêmes

[32] Cf. point 1.1.
[33] Art. 4.11) du règlement.
[34] Considérant 171 du règlement.
[35] Art. 7.3 du règlement.
[36] Art. 13 du règlement ; *cf. supra*.
[37] Art. 15 du règlement.
[38] Art. 16 du règlement.
[39] Art. 12 de la directive.
[40] Art. 17 du règlement.
[41] C.J.U.E., *Google Spain SL c. Costeja,* 13.5.2014, C-121/12.

données dont la personne concernée a demandé l'effacement[42]. Ce « droit à l'oubli » n'est toutefois pas absolu, car le règlement prévoit des exceptions telles que la liberté d'expression ou l'exercice de droits en justice. Il faudra donc s'attendre à des cas jurisprudentiels.

2.2.3. Droit à la limitation du traitement

Par ailleurs, le règlement rappelle le *droit à la limitation* du traitement[43], qui était consacré sous les termes de droit au verrouillage dans la directive[44]. Cette limitation consiste à marquer les données en vue d'empêcher provisoirement leur traitement[45] lorsque par exemple, l'exactitude des données est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données[46].

Il est à noter que le règlement prévoit l'obligation pour le responsable de traitement de notifier toute rectification, tout effacement et toute limitation de données à toute personne qui reçoit communication de ces données, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés[47]. La personne concernée peut obtenir du responsable de traitement des informations sur ces destinataires[48].

2.2.4. Droit d'opposition au traitement

Le règlement confirme le droit pour la personne concernée de *s'opposer au traitement de ses données,* en cas de traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, en cas de traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, et en cas de traitement des données à des fins de prospection, y compris le profilage[49]. Ce droit d'opposition se concrétise par l'arrêt du traitement et n'est possible que pour des raisons se rapportant à la situation particulière de la personne concernée.

2.2.5. Droit à la portabilité des données

Ensuite, et c'est une nouveauté introduite par le règlement, celui-ci octroie désormais le *droit à la portabilité des données*[50], soit le droit de la personne concernée de recevoir les données à caractère personnel qui la concernent et qu'elle a fournies à un responsable de traitement[51], dans un format structuré, couramment utilisé et lisible par machine, le droit pour cette personne de transmettre ces données à un

---

[42] Art. 17.2 du règlement.
[43] Art. 18 du règlement.
[44] Art. 12.b) de la directive.
[45] Art. 4.3) du règlement.
[46] Art. 18.1.a) du règlement.
[47] Art. 19 du règlement.
[48] Art. 19 du règlement.
[49] Art. 21 du règlement.
[50] Art. 20 du règlement.
[51] Et donc pas fournies à un tiers ; mais bien des données générées par la personne concernée elle-même lors de l'utilisation du service proposé par le responsable de traitement : G29, « Guidelines on the right of data portability », 13.12.2016 : http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf; https://www.droit-technologie.org/actualites/gdpr-droit-a-portabilite-donnees-analyse-lignes-directrices-g29/

autre responsable de traitement et même le droit de voir transférer ces données d'un responsable à un autre responsable de traitement.

Il s'agit donc pour la personne concernée de retrouver la maîtrise de ses données. Nombre de personnes répugnent en effet à l'idée de changer de prestataire en raison de la difficulté sinon de l'impossibilité de faire transférer ses données d'un prestataire à un autre.

Ce droit est toutefois limité aux hypothèses de traitement admis en cas de consentement de la personne concernée ou d'exécution d'un contrat auquel la personne concernée est partie et n'est pas applicable lorsque la licéité du traitement est justifiée par la nécessité du traitement à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement[52]. Il faut également que le traitement ait été réalisé au moyen de processus automatisés[53]. Ce nouveau droit à la portabilité des données n'est pas sans susciter de nombreuses questions juridiques et économiques qui devront recevoir réponse en jurisprudence[54] notamment parce que ce droit à la portabilité peut porter atteinte aux droits et liberté de tiers[55].

2.2.6. Droit de ne pas faire l'objet d'un profilage

Enfin, le règlement consacre le droit pour la personne concernée de *ne pas faire l'objet d'une décision individuelle fondée exclusivement sur le traitement automatisé* (dont le *profilage*) produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire[56], sauf exception[57].

2.3. Recours pour la personne concernée

D'après le règlement, la personne concernée doit disposer *grosso modo* de trois types de recours :

- d'une part, la possibilité d'introduire une réclamation auprès de l'autorité de contrôle[58] de l'Etat membre dans lequel se situe la résidence principale de la personne concernée, son lieu de travail ou le lieu de la commission de la violation[59] ;
- d'autre part, la possibilité d'introduire un recours contre une décision de l'autorité de contrôle ou contre l'absence de réaction de sa part[60] ;
- enfin, le droit d'introduire un recours devant les juridictions compétentes afin d'obtenir réparation du préjudice subi du fait d'une violation du règlement[61].

---

[52] Art. 20.3 du règlement.
[53] Sont donc exclus les dossiers papiers ; art. 20.1.b) du règlement.
[54] https://www.droit-technologie.org/actualites/gdpr-droit-a-portabilite-donnees-analyse-lignes-directrices-g29/
[55] Art. 20.4 du règlement.
[56] Art. 22 du règlement ; le considérant 71 du règlement cite de manière exemplative le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans intervention humaine.
[57] Art. 22.2 du règlement : consentement de la personne concernée, nécessité pour la conclusion ou l'exécution du contrat et autorisation légale.
[58] En Belgique, la Commission de Protection de la Vie privée : https://www.privacycommission.be/fr.
[59] Art. 77 du règlement.
[60] Art. 78 du règlement.

Un organisme, une organisation ou une asbl, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées, pourra introduire une réclamation en raison du non-respect de la réglementation, mandatée par un ou plusieurs personnes concernées[62], ou non[63].

3. Responsabilisation accrue des acteurs

Le règlement impose une véritable responsabilisation du responsable de traitement et de son sous-traitant. C'est sans doute l'aspect de la réglementation le plus touché par le nouveau règlement puisque de nombreuses nouvelles obligations apparaissent à charge du responsable de traitement et même des sous-traitants.

3.1. En amont – prévention des risques

3.1.1. Le principe de responsabilité (ou « *accountability* ») du responsable de traitement

Le responsable de traitement se voit désormais contraint non seulement de respecter la réglementation, mais aussi de démontrer ce respect[64] et qu'il a mis en place une politique proactive de protection des données compte tenu des risques.

3.1.2. Sous-traitant

Le sous-traitant doit, comme antérieurement, présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement et garantisse la protection des droits de la personne concernée[65]. Mais le règlement va plus loin en imposant au sous-traitant d'obtenir une autorisation générale ou spécifique en cas de recours à une sous-traitance au second degré[66], ce qui paraît très délicat dans l'environnement numérique du *cloud*.

3.1.3. Registre des traitements

Le règlement impose désormais l'obligation pour le responsable du traitement de tenir un registre des activités de traitements[67]. Cette obligation remplace l'obligation de notification préalable des traitements prévue par la loi du 8 décembre 1992[68]. Outre les coordonnées du responsable de traitement, ce registre reprend entre autres les finalités du traitement, une description des catégories de personnes concernées et dans la mesure du possible une description générale des mesures de sécurité (*cf. infra*). Semblable obligation existe aussi désormais pour le sous-traitant[69]. Ces registres doivent être tenus à la disposition de l'autorité de contrôle sur

---

[61] Art. 82 du règlement.
[62] Art. 80.1 du règlement.
[63] Art. 80.2 du règlement.
[64] Art. 5.2 du règlement.
[65] Art. 28.1 du règlement ; art. 17 de la directive.
[66] Art. 28.2 du règlement.
[67] Art. 30.1 du règlement.
[68] Art. 17 et s. de la loi du 8.12.1992.
[69] Art. 30.2 du règlement.

demande[70]. Une exemption de cette obligation est prévue pour des entreprises ou organisations de moins de deux-cent-cinquante employés sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données dites sensibles[71]. Autant dire que cette exemption a une portée très limitée[72].

3.1.4. Réalisation d'une étude d'impact

Nouveauté de taille introduite par le règlement, il est désormais prévu que « *lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires* »[73].

Quand faut-il faire une étude d'impact pour la protection des données ?
Tout d'abord, dit le règlement, lorsqu'il y a un risque élevé pour les droits et libertés pour les personnes physiques. De façon étonnante, le règlement ne définit ni la notion de risque élevé[74] ni le type de risque concerné.

Le règlement précise de toute façon trois hypothèses dans lesquelles il y a nécessité d'effectuer cette analyse d'impact : lorsqu'il y a :

- évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;
- traitement à grande échelle de catégories particulières de données sensibles ;
- surveillance systématique à grande échelle d'une zone accessible au public.

Cette obligation de mise en place d'une analyse d'impact se double d'une obligation de consulter l'autorité de contrôle lorsque cette analyse révèle que le traitement présente un risque élevé malgré la prise de mesures adaptées[75].

En quoi consiste cette analyse ?
La Commission de protection de la vie privée a émis un projet de recommandation relativement à cette analyse et l'a soumis à consultation préalable[76]. Ce projet de

[70] Art. 30.4 du règlement.
[71] Art. 30.5 du règlement.
[72] C. de TERWANGNE, K. ROSIER et B. LOSDYCK, *op. cit.*, p. 29.
[73] Art. 35.1 du règlement.
[74] Mais le G29, qui réunit les autorités de contrôle au niveau européen devrait s'atteler à la définir : http://derriennic.com/feuille-de-route-pour-une-mise-en-conformite-avec-le-reglement-general-donnees-personnelles-a-horizon-mai-2018/
[75] Art. 36.1 du règlement.
[76] Voyez le projet de recommandation de la Commission de protection de la vie privée : https://www.privacycommission.be/fr/consultation-publique-sur-la-recommandation-concernant-lanalyse-dimpact-relative-a-la-protection

recommandation découpait les étapes essentielles de cette analyse d'impact comme suit:

- inventaire des opérations de traitement et des finalités de traitement en se basant sur les informations qui devront être contenues dans le registre des activités de traitement (*cf. supra*) ;
- contrôle de l'application du principe de proportionnalité ;
- analyse des risques au regard des risques pour les droits et libertés des personnes physiques et donc pas seulement des risques sur la vie privée, mais aussi sur les autres libertés comme la liberté de religion ou d'expression ;
- énumération des mesures retenues afin de faire face aux risques identifiés.

3.1.5. Désignation d'un délégué à la protection des données (« *data protection officer* » ou DPO)

Les responsables de traitement ou leur(s) sous-traitant(s) peuvent ou doivent désigner un DPO en fonction de certaines conditions[77]. En tout état de cause, lorsque le traitement est effectué par une autorité publique ou un organisme public, il s'agit d'une obligation[78]. Il appartiendra au législateur national de déterminer ce qu'est une autorité publique ou un organisme public[79].
Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul DPO peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille[80].

Cette mission de DPO pourra être confiée à un agent de l'administration en interne ou pourra être externalisée à une entreprise spécialisée[81]. Le DPO est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions[82].

Le rôle de ce DPO est assez large : informer et conseiller le responsable de traitement (ou son ou ses sous-traitant(s)), contrôler le respect de la réglementation, conseiller l'administration quant à la réalisation d'une analyse d'impact, coopérer avec l'autorité de contrôle,[83] mais aussi être le point de contact des citoyens en ce qui concerne le traitement de leurs données.

Ce DPO ne pourra toutefois pas recevoir d'instructions en ce qui concerne l'exercice de ses missions et ne pourra pas être relevé de ses fonctions ou pénalisé par le responsable de traitement ou le sous-traitant pour l'exercice de ses missions[84]. Ce

[77] Art. 37.1 et 37.4 du règlement.
[78] Art. 37.1.a) du règlement.
[79] Article 29 Data Protection Working Party (G29), « Guidelines on Data Protection Officers, 13.12.2016,http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.
[80] Art. 37.3 du règlement.
[81] Art. 37.6 du règlement.
[82] Art. 37.5 du règlement.
[83] Art. 38 et 39 du règlement.
[84] Art. 38.3 du règlement.

délégué pourra exercer d'autres missions pour autant que cela n'entraîne pas de conflits d'intérêts[85]. Par exemple, le DPO ne pourra à la fois être le DPO et être en position de déterminer les objectifs et les moyens de traitement de données à caractère personnel[86].

Des lignes directrices sur la fonction et le rôle du DPO ont été établies par le G29[87]. Ce guide aborde notamment la manière de concilier l'indépendance du DPO et le contrôle de ce DPO par le responsable du traitement ou le sous-traitant, mais aussi les conditions dans lesquelles ce DPO doit pouvoir travailler.
Enfin, notons que les coordonnées du DPO devront faire l'objet d'une publication et d'une communication à la Commission de protection de la vie privée[88] de manière à ce que celle-ci puisse contacter directement et facilement le DPO.

3.1.6. Protection des données dès la conception et par défaut (« privacy by design and by default »)

Le règlement prévoit que compte tenu de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte, des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à appliquer les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du règlement et de protéger les droits de la personne concernée[89]. Le responsable du traitement déploie les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité[90].

3.2. En aval du traitement – gestion des risques

3.2.1. Notification des violations des données à caractère personnel

Les conditions de traitement des données à caractère personnel imposent que les données soient traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. Il s'agit là de la consécration des principes d'intégrité et de confidentialité des données[91]. Malgré toutes les

[85] Art. 38.6 du règlement.
[86] Article 29 Data Protection Working Party (G29), « Guidelines on Data Protection Officers, 13.12.2016, p. 15, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.
[87] Article 29 Data Protection Working Party (G29), « Guidelines on Data Protection Officers, 13.12.2016,http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
[88] Art. 37.7 du règlement.
[89] Art. 25.1 du règlement.
[90] Art. 25.2 du règlement.
[91] Art. 5.1.f) du règlement.

mesures qui peuvent être prises par le responsable de traitement[92], nul n'est à l'abri d'une faille de sécurité comme la perte, l'altération ou la divulgation de données. Sous l'ère de la directive, seule une recommandation émise par la Commission de protection de la vie privée enjoignait les responsables de traitement, sur la base volontaire, à lui notifier tout incident et à informer le public[93]. Désormais, avec le règlement, en cas de violation de données à caractère personnel[94], le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard[95].
Par ailleurs, le règlement prévoit aussi la notification à la personne concernée de la violation de ses données à caractère personnel lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique[96]. La réglementation contient toutefois des exceptions à cette obligation, lorsque par exemple, cette notification exigerait des efforts disproportionnés (auquel cas, une communication publique est exigée) ou lorsque le responsable de traitement a pris des mesures de protection techniques et organisationnelles appropriées aux données concernées par la violation[97].
En outre, le sous-traitant est contraint de notifier la violation de données à caractère personnel non pas à l'autorité de contrôle, mais bien au responsable de traitement[98]. Contractuellement, il conviendra de prévoir l'étendue des informations que devra communiquer le sous-traitant au responsable de traitement pour que ce dernier soit en mesure de se conformer à ses propres obligations[99].
Enfin, en cas de violation, le responsable de traitement devra documenter celle-ci : faits, effets, mesures prises, etc.[100]

3.2.2. Régime de responsabilité du responsable de traitement et du sous-traitant

La directive[101]prévoyait la responsabilité du responsable du traitement pour tout dommage découlant d'un traitement illicite ou de toute action incompatible avec les dispositions nationales ainsi que la possibilité d'une exonération de responsabilité si

[92] Art. 5.2 du règlement.
[93] En dehors des obligations découlant, dans le secteur des télécoms, de la loi du 13.6.2005 relative aux communications électroniques, *M.B.*, 20.5.2005 ; Commission de la protection de la vie privée, Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données, n°01/2013, 21.1.2013, p. 6, disponible sur : https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf
[94] Définie à l'article 4.12) du règlement de manière très large : « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* ».
[95] Art. 33.1 du règlement.
[96] Art. 34.1 du règlement.
[97] Art. 34.3 du règlement.
[98] Art. 33.2 du règlement.
[99] C. de TERWANGNE, K. ROSIER et B. LOSDYCK, *op. cit.*, p. 35.
[100] Art. 33.5 du règlement.
[101] Art. 23 de la directive.

le responsable de traitement prouvait que le fait qui a provoqué le dommage ne lui était pas imputable. Le règlement amplifie les responsabilités du responsable de traitement et du sous-traitant par rapport à la directive. D'une part, parce que désormais le sous-traitant peut être lui aussi tenu responsable, mais uniquement s'il n'a pas respecté les obligations prévues par le règlement qui incombent spécifiquement aux sous-traitants ou s'il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci[102]. D'autre part, parce que le règlement prévoit désormais une solidarité entre le(s) responsable(s) de traitement et/ou le(s) sous-traitant(s) lorsque deux d'entre eux au moins sont considérés comme responsables d'un dommage causé par le traitement. En ce cas, la victime pourra utilement se retourner contre l'un ou l'autre, à charge pour celui qui indemnise la victime de se retourner à son tour contre l'autre ou les autres (co-)responsable(s)[103].

4. Transfert de données à caractère personnel vers des pays tiers

Le règlement pose le principe de l'interdiction de transferts de données à caractère personnel en dehors de l'Union européenne et de l'Espace économique européen « *à moins que le pays de destination des données n'ait été reconnu comme assurant une protection adéquate aux données, ou que l'émetteur des données n'offre lui-même une protection adéquate par le biais de garanties appropriées telles des clauses contractuelles (…), ou enfin qu'une dérogation trouve à s'appliquer* »[104]. Cette interdiction pose de nombreuses questions de légalité et de praticabilité pour une société qui stocke ses données dans le *cloud*.

5. Réorganisation de la Commission de la protection de la vie privée et nouveaux pouvoirs

Le règlement est l'occasion de revoir les missions et les pouvoirs de sanctions des autorités de contrôle des Etats membres. L'effectivité des nouvelles règles, fort contraignantes et protectrices, n'est possible que grâce à l'accroissement des pouvoirs de contrôle et de sanction de l'autorité de contrôle, en la personne de la Commission de protection de la vie privée.

Aussi, le règlement attribue aux autorités de contrôle notamment les missions suivantes :

- sensibilisation du public et sa compréhension des risques et des droits ;
- sensibilisation des responsables de traitement et des sous-traitants ;
- Conseil du Parlement national, du gouvernement et autres institutions ;
- traitement des réclamations ;
- coopération avec les autres autorités de contrôle[105].

Le règlement octroie aux autorités de contrôle des pouvoirs d'enquête ainsi que le pouvoir de prendre des mesures correctrices[106] telle que la possibilité d'imposer une amende administrative – ce qui constitue une nouveauté – pouvant aller jusqu'à 20.000.000 € ou 4% du chiffre d'affaires annuel mondial de l'exercice précédent[107].

6. Comment l'application de ce nouveau règlement se prépare-t-elle ?

[102] Art. 82.2 du règlement.
[103] Art. 82.5 du règlement.
[104] C. de TERWANGNE, K. ROSIER et B. LOSDYCK, *op. cit.*, p. 53 ; art. 44 du règlement.
[105] Art. 57 du règlement.
[106] Art. 58 du règlement.
[107] Art. 83.5 du règlement.

Ce nouveau règlement qui a mis plus de 4 ans à naître, a été publié au Journal officiel de l'Union européenne le 4 mai 2016, est entré en vigueur le 24 mai 2016 et devra être appliqué dans les Etats membres dès le 25 mai 2018. Il reste donc une année pour que la Belgique et les pouvoirs locaux wallons s'adaptent aux changements.
Le G29 a adopté un plan d'action en février 2016 pour permettre l'application effective de ce nouveau règlement dès mai 2018. Les quatre objectifs principaux de ce groupe de travail européen sont les suivants :

- Préparer la mise en place du Comité européen de la protection des données destiné à remplacer le G29 en 2018.
- Préparer la mise en place du guichet unique et la coopération entre les différentes autorités des Etats membres européens.
- Proposer des lignes directrices sur quatre sujets identifiés prioritaires : le droit à la portabilité[108], la certification, le DPO[109] et les traitements à risque.
- Promouvoir et diffuser le règlement[110].

Le règlement permet à l'autorité de contrôle d'approuver des codes de conduite élaborés par des associations ou autres organismes représentant des catégories de responsables de traitement[111]. Ces codes de conduite seront des outils utiles pour les responsables de traitement.
De même, le règlement[112] prévoit la mise en place d'un système de certification des responsables, mais aussi et surtout des sous-traitants, ce qui pourra s'avérer très utile lors du choix des cocontractants opéré par le pouvoir public (logiciel de gestion des salaires, cloud, etc.).
Notons que la Commission de protection de la vie privée a mis sur son site internet la possibilité pour les autorités publiques, les entreprises et les citoyens de poser leurs questions en ligne, de manière à publier une Foire Aux Questions[113].
La Commission de protection de la vie privée a également édité une brochure « R.G.P.D. : préparez-vous en 13 étapes »[114] que nous résumons comme suit :

- conscientisation ; il s'agit de conscientiser les personnes clés et les décideurs aux changements importants en matière de données à caractère personnel qui se dessinent pour mai 2018 ;
- établissement d'un registre de données : il est recommandé de faire un inventaire minutieux des données traitées, de noter leur provenance, les personnes avec lesquelles elles sont partagées ainsi que leur fondement légal ; la Commission de protection de la vie privée conseille d'effectuer un audit d'information ;

---

[108] Voyez : Article 29 Data Protection Working Party (G29), «Guidelines on the right to data portability », 13.12.2016, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
[109] Article 29 Data Protection Working Party (G29), « Guidelines on Data Protection Officers, 13.12.2016,http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
[110]https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels.
[111] Art. 40 et 41 du règlement.
[112] Art. 42 et 43 du règlement.
[113] https://www.privacycommission.be/fr/forms/formulaire-questions-sur-le-rgpd
[114] Disponible sur le lien suivant : https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf

- communication : le responsable de traitement doit communiquer à chacune des personnes concernées ses droits ; cela se fait par une déclaration de confidentialité[115] qui devra être mise à jour au regard des nouvelles obligations du règlement ;
- gestion des droits de la personne concernée : il s'agit d'examiner si la façon de traiter les données respecte les (nouveaux) droits de la personne concernée et notamment le nouveau droit à la portabilité des données à caractère personnel ;
- gestion des demandes d'accès : la Commission conseille de réfléchir sur la manière de gérer les demandes d'accès aux données par les personnes concernées ;
- déterminer le fondement légal du traitement de données à caractère personnel ;
- évaluer la qualité du consentement lorsqu'il s'agit du fondement légal du traitement utilisé et adapter les procédures aux nouvelles obligations du règlement ;
- évaluer et adapter les procédures en offrant aux enfants une protection spécifique ;
- détection et gestion des fuites de données : il s'agit de déterminer les risques de fuites de données, leur gestion et la mise en place d'une procédure en cas de notification à l'autorité de contrôle ;
- protection des données dès la conception et analyse d'impact : veiller, dès le début, à prévoir une conception des traitements des données qui permette le respect du nouveau règlement et envisager la réalisation d'une analyse d'impact ;
- désignation d'un délégué à la protection des données : elle est obligatoire pour les autorités publiques et les organismes publics ; le DPO peut être désigné en interne ou en externe ;
- au niveau national, déterminer l'autorité de contrôle compétente et si les opérations de traitement ont un caractère national ;
- en ce qui concerne les contrats existants et futurs, évaluer et mettre en conformité les relations contractuelles avec vos sous-traitants (soit généralement, les adjudicataires de marchés publics locaux).

En conclusion, l'on peut dire que ce nouveau règlement amène de nombreuses nouveautés, qui s'intègrent logiquement dans la continuité de la réglementation protégeant les données à caractère personnel tout en évoluant sur des points précis. Notre association ne manquera pas d'informer ses membres sur les mesures de mise en œuvre de ce règlement et de proposer des outils utiles en vue de l'implémentation de cette réglementation dans la vie quotidienne de nos membres.

[115] Voyez notamment cet exemple: http://www.belgium.be/fr/declaration_de_confidentialite