Règlement UE 2016/679 du 26 avril 2016

Règlement général sur la protection des données (RGPD)

PANORAMA DES NOUVEAUTES INTRODUITES PAR LE RGPD

dcl avocats / Luxembourg

INTRODUCTION

Cadre Légal

A compter du **25 mai 2018** le **règlement protection des données**, Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, plus connu sous les abréviations « **RGPD** » en français et « **GDPR** » en anglais, **sera d'application directe** dans tous les états européens.

Le RGPD s'inscrit dans le « paquet sur la protection des données » avec la directive (UE) 2016/680 relative au régime de la protection des données à caractère personnel en matière pénale et la directive (UE) 2016/681 relative à l'utilisation des données des passagers (PNR).

INTRODUCTION

Cadre Légal

A partir du 25 mai 2018, la **loi modifiée du 2 août 2002** relative à la protection des personnes à l'égard du traitement des données à caractère personnel **sera abrogée** et les dispositions nationales (loi organique de la Commission Nationale pour la Protection des Données (« **CNPD** ») et dispositions spécifiques pour lesquelles le RGPD prévoit l'obligation d'une législation nationale complémentaire) prévues par le **projet de loi luxembourgeois n° 7184** viendront compléter le cadre européen fixé par le RGPD.

INTRODUCTION

Les objectifs du RGPD

- **Renforcer les droits des personnes physiques:** nouvelle définition du consentement, création d'un droit à la portabilité des données personnelles, droit d'être informé en cas de violation de données etc.
- **Responsabiliser les responsables des traitements et sous-traitants:** passage à un système de contrôle a posteriori.
- **Organiser la régulation au sein de l'UE:** nouveaux rôles pour les autorités de contrôle, coopération entre autorités de contrôle, « one stop shop », etc.

PLAN

1. Quelques définitions
2. Champ d'application matériel et territorial
3. Principes à respecter
4. Licéité du traitement
5. Information de la personne concernée
6. Nouveaux droits de la personne concernée
7. Responsable du traitement et sous-traitant
8. Autres nouveautés
9. Codes de Conduite et Certifications
10. Les sanctions

1. QUELQUES DEFINITIONS

Définitions (art. 4)

Traitement: toute **opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel**, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

Données à caractère personnel: toute **information se rapportant à une personne physique identifiée ou identifiable** (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

1. QUELQUES DEFINITIONS

Responsable de traitement: la personne physique ou morale, l'autorité publique, le service ou un autre organisme **qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement** (…)

Sous-traitant: la personne physique ou morale, l'autorité publique, le service ou un autre organisme **qui traite des données à caractère personnel pour le compte du responsable du traitement**

2. CHAMP D'APPLICATION

Champ d'application matériel (art. 2)

Le RGPD s'applique au traitement des données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier

Champ d'application territorial (art. 3)

Elargissement du champ d'application territorial

- soit le responsable du traitement ou le sous-traitant **est établi** sur le territoire de l'UE
- soit le responsable de traitement ou le sous-traitant **fournit des biens et/ou des services aux résidents européens ou cherchent à cibler les résidents européens**

3. PRINCIPES A RESPECTER

Grands Principes édictés par le RGPD (art.5 § 1)

Ces principes essentiels étaient déjà reconnus ou sous-entendus par la directive 95/46/CE du 24 octobre 1995 transposée en droit luxembourgeois par la loi modifiée du 2 août 2002

« Les données personnelles doivent être:

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (**licéité, loyauté, transparence**);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (**limitation des finalités**);

3. PRINCIPES A RESPECTER

Les données personnelles doivent être: (…)

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (**minimisation des données**);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (**exactitude**);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (**limitation de la conservation**);

3. PRINCIPES A RESPECTER

Les données personnelles doivent être: (…)

f) 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 (**intégrité et confidentialité**); (…) »

4. LICEITE DU TRAITEMENT

Principe de licéité du traitement (Art.6)

Afin de s'assurer de la licéité du traitement, il convient d'abord **d'identifier la base légale** sur laquelle repose le traitement

Le RGPD prévoit que le traitement **n'est licite qui si**, et dans la mesure où, **au moins l'une des conditions suivantes est remplie**:

a) la personne concernée a **consenti** au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques

b) le **traitement est nécessaire à l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci

c) le traitement est **nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis

d) le traitement est **nécessaire à la sauvegarde des intérêts vitaux de la personne concernée** ou d'une autre personne physique

4. LICEITE DU TRAITEMENT

Base légale du traitement (Art.6)

Le RGPD prévoit que le traitement n'est licite qui si, et dans la mesure où, **au moins l'une des conditions suivantes est remplie**: (…)

e) 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 du traitement

f) 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 qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant

4. LICEITE DU TRAITEMENT

Consentement renforcé (Art.7)

Dans le cas où le traitement repose sur le consentement (art.6 b)):

- Il appartient **au responsable du traitement de prouver** que la personne concernée a donné son consentement (avant tout traitement)
- Si le consentement est donné sur un formulaire de demande écrit, la demande de consentement est présentée sous une forme qui la distingue clairement des autres questions, sous une forme **compréhensible** et **aisément accessible**, et **formulée en des termes clairs et simples**
- La personne concernée a le droit de **retirer** son consentement à tout moment
- Le contrat ne doit pas être soumis au fait que la personne concernée consente au traitement de données non nécessaires au contrat

Attention: nouvelle finalité de traitement = nouveau consentement

Le RGPD créé pour la première fois des **conditions particulières pour le traitement des données des enfants** (mineurs de moins de 16 ans)

4. LICEITE DU TRAITEMENT

Traitement portant sur des catégories particulières de données à caractère personnel (Art. 9)

Le RGPD **interdit par principe (Art. 9 § 1):** le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

Cependant, **des exceptions** sont prévues dans certains cas (Art. 9 § 1) notamment lorsque:

- 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 de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée

5. INFORMATION DE LA PERSONNE CONCERNEE

L'article 13 du RGPD prévoit une **liste d'informations à fournir lorsque les données sont collectées auprès de la personne concernée**.

- **Au moment de la collecte** il s'agit notamment d'indiquer :
  - **l'identité et les coordonnées du responsable du traitement** et, le cas échéant, du représentant du responsable du traitement
  - les **coordonnées du délégué à la protection des données** le cas échéant
  - les **finalités du traitement** auquel sont destinées les données à caractère personnel ainsi que **la base juridique du traitement**
- **Au moment où les données sont obtenues** il s'agit notamment d'indiquer :
  - la **durée de conservation** des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée
  - l'existence **du droit de demander au responsable du traitement l'accès** aux données à caractère personnel, la **rectification** ou **l'effacement** de celles-ci, ou une **limitation** du traitement relatif à la personne concernée, ou du droit de **s'opposer** au traitement et du droit à la portabilité des données

5. INFORMATION DE LA PERSONNE CONCERNEE

- Il s'agit notamment d'indiquer **au moment où les données sont obtenues** : (…)
  - lorsque le traitement est fondé sur le consentement, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci
  - le droit d'introduire une réclamation auprès d'une autorité de contrôle

Attention: lorsque le responsable du traitement a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, il doit fournir au préalable à la personne concernée des informations au sujet de cette autre finalité

6. NOUVEAUX DROITS DE LA PERSONNE CONCERNEE

Maintien et développement des droits existants

Le RGPD maintient les droits existants et les étend pour certains tels le **droit d'accès, à la rectification, à l'effacement et à la limitation des données** (art.15, art.16, art.17 et art.18)

Droit à la portabilité

Il introduit notamment un **droit à la portabilité** des données (art. 20). Ce nouveau droit permet à une personne concernée de récupérer les données qu'elle a fournies à un responsable du traitement dans un format « structuré, couramment utilisé et lisible par machine » et le cas échéant décider de les transférer à un autre responsable du traitement

Voie de recours devant l'autorité de contrôle

Si elle considère qu'une violation a été commise, la personne concernée peut introduire une réclamation auprès de l'autorité de contrôle en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise
L'autorité de contrôle l'informera de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel

7. RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

Identifier le responsable du traitement (art.24)

Afin de déterminer si l'acteur est sous-traitant ou responsable de traitement, il convient de se référer à l'avis 2/2010 du groupe 29 et d'analyser au cas par cas:

- Le niveau d'instruction donné par le client au prestataire : quelle est l'autonomie du prestataire dans la réalisation de sa prestation ?
- le degré de contrôle de l'exécution de la prestation : quel est le degré de «surveillance» du client sur la prestation ?
- valeur ajoutée fournie par le prestataire: le prestataire dispose-t-il d'une expertise approfondie dans le domaine ?
- degré de transparence sur le recours à un prestataire : l'identité du prestataire est-elle connue des personnes concernées qui utilisent les services du client ?

Le RGPD **étend une large partie des obligations du responsable du traitement aux sous-traitants** (ex: sécurité, confidentialité, tenue d'un registre, désignation d'un DPD).

7. RESPONSABLE DU TRAITEMENT ET SOUS-TRAITANT

Le sous-traitant (art.28)

Le traitement réalisé par le sous-traitant sera régi par un **contrat** dans lequel devra figurer une liste d'éléments repris à l'article 28 du RGPD.

Le sous-traitant devra notamment (art. 28 h)) s'engager à mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Le sous-traitant doit requérir l'autorisation écrite préalable du responsable du traitement pour **recruter un autre sous-traitant.**

8. AUTRES NOUVEAUTES

Registre des activités de traitement (art. 30)

Obligatoire pour les entreprises comptant plus de 250 personnes

Le délégué à la protection des données (« DPD » ou « DPO ») (art. 37 et suivants)

S'applique au responsable du traitement ainsi qu'au sous-traitant

Désignation **volontaire ou obligatoire** notamment:

- lorsque les activités de base du responsable de traitement ou du sous-traitant consistent en des **opérations qui, du fait de leurs natures, de leurs portées et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle** des personnes concernées (ex: pour une banque les données financières)
- lorsque les activités de base du responsable de traitement ou du sous-traitant consistent en un **traitement à grande échelle de catégories particulières de données** visées à l'article 9 et des données à caractère personnel relatives à des condamnations pénales ou à des infractions à l'article 10.

DPD **interne** (salarié) **ou externe** (contrat de service avec personne physique ou morale)

Possibilité de **DPD mutualisé** (art. 37 § 2)

8. AUTRES NOUVEAUTES

Analyse d'impact (art. 35)

Sauf exception prévue par le règlement, lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques le responsable de traitement effectue une analyse d'impact des opérations de traitement envisagées (peut viser un traitement ou un ensemble de traitements)

Procédure en cas de violation (art. 33 et 34)

En cas de violation des données à caractère personnel (ex: perte de confidentialité, d'intégrité, ou/et de disponibilité) le responsable du traitement doit enregistrer la violation, dans certains cas la notifier à la CNPD dans un délai défini et éventuellement communiquer à la personne concernée

Nouvelles dispositions sur le profilage

Mises à jour des transferts de données hors de l'UE

9. CODES DE CONDUITE ET CERTIFICATIONS

Définitions

Le RGPD ne donne pas de définition du code de conduite et de la certification (Art 40 à 43)

Certification: Assurance écrite (sous la forme d'un certificat) donnée par une tierce partie qu'un produit service ou système est conforme a des exigences spécifiques (ISO)

Code de conduite: Un engagement pris volontairement par une société ou une organisation d'appliquer certains principes et normes de comportement à la conduite de ses activités ou opérations (OCDE)

Pourront être certifiés:

- les opérations de traitements d'un responsable du traitement ou d'un sous-traitant
- un programme de gouvernance de la protection des données d'un responsable du traitement ou d'un sous-traitant
- des produits et des services

La **CNPD** pourra avaliser et approuver des organismes de certifications et codes de conduite dont elle publiera **une liste** sur son site internet après l'entrée en vigueur du RGPD

10. LES SANCTIONS

Les responsables des traitements et les sous-traitants peuvent faire l'objet de **sanctions administratives** importantes en cas de méconnaissance des dispositions du RGPD. La CNPD pourra notamment (Art. 58):

- prononcer un avertissement
- mettre en demeure l'entreprise
- limiter temporairement ou définitivement un traitement
- suspendre les flux de données
- retirer une certification ou ordonner à l'organisme de certification de retirer une certification
- ordonner de satisfaire aux demandes d'exercice des droits des personnes
- ordonner la rectification, la limitation ou l'effacement des données.

Les **amendes** prononcées par la CNPD (Art. 83) pourront s'élever jusqu'à un maximum de 20.000.000 EUR ou dans le cas d'une entreprise, jusqu'à 4% de son chiffre d'affaire annuel total au niveau mondial.

EN CONCLUSION

Les nouvelles règles introduites par le RGPD impliquent de procéder à un audit de l'ensemble des traitements de données des personnes physiques effectuées par une entité soumise à la réglementation afin de déterminer les mesures de mise en conformité.

Il conviendra notamment d'identifier pour chaque traitement si elle agit en qualité de responsable de traitement ou de sous-traitant et en tirer les conséquences (en terme de modification des procédures internes etc.).

Le passage au contrôle a postériori engendrera en outre l'obligation pour toute entité concernée par le RGPD, de documenter l'ensemble des décisions relatives aux traitements.

EN CONCLUSION

Les sites internet des régulateurs européens constituent une source d'informations fiable et facilement accessible. Certains outils sont déjà disponibles afin de simplifier la mise en conformité, tel que:

- l'outil permettant de réaliser les analyses d'impact sur la protection des données mis à disposition sur le site du régulateur français:

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

- Le modèle de registre des activités de traitement élaboré par la commission de la protection de la vie privée belge, Recommandation n° 06/2017 du 14 juin 2017

https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_06_2017_0.pdf

POUR TOUTE QUESTION

Dorothée CIOLINO
Avocat aux Barreaux de Paris et de Luxembourg
ciolino@dclavocats.com

Emilie MACCHI
Avocat à la Cour
macchi@dclavocats.com

DCL Avocats S.à r.l.
9, Avenue Jean-Pierre Pescatore
L-2324 Luxembourg
Tél. + 352 26 00 11 1
Fax +352 27 12 51 81
www.dclavocats.com