Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

Newsletter : **La loi belge sur la protection des données entre aujourd'hui en vigueur**

Septembre 2018

Contenu

Cher lecteur,

Le Règlement Général sur la Protection des Données - mieux connu sous les abréviations 'RGPD' ou 'GDPR' - est d'application depuis le 25 mai 2018.

Les entreprises ont entre-temps dû faire le nécessaire pour mettre leurs activités de traitement en conformité avec le RGPD et encadrer celles-ci de la bonne manière.

Les lignes de force du RGPD ont déjà été abordées dans notre Newsletter du 4 mai 2016. Nous avons aussi rassemblé toute une série d'informations sur notre site internet www.gdprbelgium.be.

Bien que le RGPD a pour objet l'harmonisation des règles en matière de protection des données, une possibilité est parallèlement donnée aux Etats membres d'apporter leur propre touche et de prévoir des dispositions spécifiques dans la législation nationale, plus particulièrement sur le plan du droit du travail. Cela doit évidemment être effectué dans les limites du RGPD.

La tant attendue loi belge 'relative à la protection des personnes physiques relativement au traitement de données à caractère personnel' (ci-après: loi sur la Protection des Données) est aujourd'hui publiée au Moniteur Belge. Cette loi remplace la précédente loi sur la protection des données du 8 décembre 1992, et entre aujourd'hui en vigueur.

Vous trouverez ci-après un résumé des règles importantes qui auront un impact sur pratiquement l'ensemble des entreprises.

Nous vous souhaitons une agréable lecture !

1 Champ d'application

La loi belge sur la Protection des Données est en premier lieu applicable aux traitements dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire belge, que le traitement ait lieu ou non sur le territoire belge.

Une exception à ce principe existe pour les sous-traitants belges qui agissent pour un responsable du traitement établi dans un autre Etat membre de l'UE si le traitement a lieu dans cet autre Etat membre de l'UE. Dans ce cas, le droit de cet autre Etat membre de l'UE est applicable.

La loi belge sur la Protection des Données peut cependant également être applicable à des entreprises non-européennes qui n'ont pas d'établissement en Belgique. C'est le cas si une entreprise:

- Offre des biens ou des services à des personnes en Belgique, qu'un paiement soit exigé ou non des personnes concernées;
- Suit le comportement de personnes en Belgique, par exemple via le profilage en ligne (*online profiling)*.

2 Données à caractère personnel sensibles

Sur la base du RGPD, un certain nombre de catégories particulières de données à caractère personnel disposent d'un régime spécifique en raison de leur caractère sensible: les données génétiques, les données biométriques permettant l'identification unique d'une personne, les données concernant la santé, les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Il en va de même pour les données concernent le passé judiciaire d'une personne, consultable en Belgique via l'extrait de casier judiciaire, pour lesquelles un régime spécifique s'applique.

2.1 Interdiction de principe du traitement

Le traitement de ces données sensibles est en principe interdit, à moins que l'entreprise ne puisse invoquer une exception à ce principe.

Une de ces exceptions est la nécessité du traitement de ces données pour des motifs d'intérêt public important. La loi belge sur la Protection des Données stipule que les associations et les fondations pour lesquelles le traitement de données sensibles est nécessaire en vue de la réalisation de leur objet social, peuvent, sous certaines conditions, également invoquer cette exception au principe.

Les autres exceptions du RGPD, par exemple lorsque le traitement est nécessaire pour satisfaire à des obligations en matière de droit du travail, continuent à s'appliquer.

2.2 Données génétiques, biométriques et concernant la santé

Le traitement de telles données est interdit, à moins qu'une entreprise puisse se prévaloir d'une exception. Le traitement est ainsi possible lorsqu'une personne donne son consentement. Dans le cadre d'une relation de travail, le consentement risque toutefois d'être considéré comme non valable parce que le caractère libre de celui-ci pourra être contesté.

En matière de droit du travail, le RGPD prévoit cependant la possibilité pour les Etats membres de déterminer des exceptions complémentaires pour le traitement de ce type de données. Certains pays ont choisi de recourir à cette possibilité pour rendre possible, sous certaines conditions, le contrôle des accès, par exemple, via un scan de l'iris ou une empreinte digitale. Dans la législation belge, une telle exception n'est cependant pas prévue, et la loi sur la Protection des Données

n'autorise pas le recours à cette possibilité. Cela restera par conséquent difficile pour les employeurs de recourir à des systèmes d'authentification biométriques pour le contrôle des accès et l'enregistrement du temps, étant entendu que la situation doit être examinée au cas par cas.

Pour le traitement de données génétiques, biométriques et relatives à la santé, la nouvelle loi sur la Protection des Données confirme les conditions complémentaires qui existaient déjà sur la base de la réglementation antérieure. Il existe donc une obligation d'établir une liste comprenant les catégories de personnes qui auront accès à ces données et une description de leur rôle dans le cadre de ce traitement. Cette liste doit pouvoir être présentée à l'Autorité de protection des données (ci-après: 'APD') sur demande de cette dernière. Les personnes qui ont accès à cette liste doivent par ailleurs être liées par une obligation légale ou contractuelle de confidentialité.

2.3 Données pénales

Le traitement de données relatives au passé pénal d'une personne, tel que par exemple un extrait du casier judicaire, est en principe interdit.

La loi sur la Protection des Données détermine à ce propos différentes exceptions. Un traitement de données pénales est entre autres possible:

- Si le traitement est nécessaire pour la gestion de ses propres litiges;
- Par des avocats ou d'autres conseils juridiques pour autant que la défense des intérêts de leurs clients l'exige;
- Pour des motifs d'intérêt public important pour l'accomplissement de tâches d'intérêt général confiées par ou en vertu d'une loi, d'un décret, d'une ordonnance ou du droit de l'UE;
- Si la personne concernée a rendu ces données publiques de sa propre initiative pour une ou plusieurs finalités bien déterminées;
- Si la personne concernée a donné son consentement pour ce faire. Cette exception ne pourra toutefois pas être utilisée par les employeurs. En raison du lien de subordination dans la relation de travail, le consentement ne peut en effet pas être donné librement et devra par conséquent être considéré comme non valable. Cette nouvelle exception offre toutefois des opportunités dans des situations autres que la relation de travail. Vous devrez toutefois veiller à ce que le consentement satisfasse aux conditions strictes du RGPD: le consentement doit être libre, spécifique, sans équivoque et informé et écrit dans un langage clair et compréhensible.

Au vu de l'interdiction et des strictes exceptions, les employeurs du secteur privé ne pourront en principe pas conserver d'extrait de casier judiciaire de travailleurs ou de candidats, à moins qu'une des exceptions susmentionnées ne puisse s'appliquer.

Nous rappelons à ce propos que l'ADP a par le passé indiqué que, dans les autres cas, il pouvait être demandé à un (candidat) travailleur de présenter un extrait de leur casier judiciaire, mais qu'une copie de celui-ci ne pouvait pas être effectuée ou conservée et qu'aucunes notes ne pouvaient être prises.

3 Offre de services des sociétés de l'information à des enfants

Selon le RGPD, en ce qui concerne l'offre directe de 'services de la société de l'information' aux enfants, tels que des médias sociaux, des sites internet, des apps, ..., le traitement de données relatives aux enfants n'est licite que si le consentement a été donné par les parents. La responsabilité de s'en assurer repose sur les fournisseurs de ces services. Les Etats membres peuvent cependant abaisser la limite d'âge à 13 ans, et la Belgique a fait usage de cette possibilité.

Sur base de la loi belge sur la Protection des Données, les jeunes à partir de 13 ans pourront par conséquent donner eux-mêmes leur consentement pour le traitement de leurs données à caractère personnel lorsqu'ils utilisent les médias sociaux, sites internet, apps, ...

L'ADP avait rendu un avis positif sur l'abaissement de l'âge à 13 ans étant donné que cet âge correspond mieux à la réalité quotidienne de très nombreux jeunes qui surfent déjà sur Internet à un jeune âge.

4 Régime d'exception pour le traitement à des fins historiques, statistiques ou scientifiques

Pour faciliter les recherches scientifiques et historiques et la production de statistiques, les Etats membres peuvent, dans leur législation nationale, prévoir des dérogations aux droits suivants: accès, rectification, limitation et opposition. Le régime dérogatoire peut seulement être appliqué pour autant que les droits susmentionnés rendent impossible la mise en œuvre des finalités spécifiques ou les entravent gravement, et qu'une telle dérogation soit nécessaire en vue d'atteindre ces finalités.

Les traitements pour les finalités susmentionnées doivent être compris largement. Cela ne porte pas uniquement sur des activités de recherche dans un cadre académique, mais cela peut aussi comprendre des activités de recherche et développement en entreprise, peu importe leur taille. Un exemple cité par l'APD dans son avis sur l'avant-projet de loi sur la Protection des Données est une entreprise qui invite un groupe de consommateurs pour tester si un nouvel emballage est plus pratique que l'actuel. Selon l'Autorité de protection des données, l'impact n'est donc pas limité aux universités ou aux entreprises orientées sur l'innovation, mais comprend également les activités de recherche à petite échelle. Cependant, les travaux préparatoires de la loi montrent que tous les membres du gouvernement ne sont pas d'accord avec ce point de vue et que, selon eux, seule la recherche scientifique au sens strict tomberait sous ce régime d'exception. Selon ce point de vue, le régime des exceptions ne s'appliquerait que si la recherche scientifique sert un intérêt sociétal - et pas seulement un intérêt privé. La portée précise de ce régime d'exception devra donc être clarifiée.

Pour pouvoir appliquer le régime dérogatoire au RGPD, la loi sur la Protection des Données détermine les garanties suivantes, qui ajoutent des obligations complémentaires pour toutes les entreprises qui effectuent des traitements aux fins susmentionnées.

4.1 Anonymisation ou cryptage

Selon le RGPD, le cryptage peut être une mesure appropriée pour protéger des données à caractère personnel, et l'anonymisation doit être appliquée là où c'est faisable.

Dans la lignée de la réglementation antérieure, la loi sur la Protection des Données va un pas plus loin et introduit une sorte de système en cascade:

- Les données doivent en principe être anonymisées de sorte que les personnes concernées ne puissent plus être identifiées;
- Lorsque ce n'est pas possible, les données doivent être cryptées ou codées ('pseudonymisation'). De cette manière, les données ne peuvent plus être couplées à une personne déterminée sans que des données additionnelles ne soient utilisées. Ces données supplémentaires doivent être conservées séparément et être suffisamment protégées;
- Seulement lorsque le cryptage n'est pas possible, les données non-cryptées peuvent être utilisées. Les données non-cryptées ne peuvent en principe pas être diffusées ou communiquées à des tiers.

4.2 Registre élargi des activités de traitement

Les entreprises qui traitent des données à caractère personnel aux fins susmentionnées, doivent ajouter les éléments suivants au registre des activités de traitement:

- La justification de l'utilisation des données pseudonymisées ou non;
- Les motifs selon lesquels l'exercice des droits d'accès, de rectification, de limitation et/ou d'opposition de la personne concernée risque de rendre impossible ou d'entraver sérieusement la réalisation de la finalité;
- En cas de traitement de 'données sensibles', l'analyse d'impact de protection des données (si applicable).

4.3 Obligation étendue d'information

Dans le cadre du RGPD, le responsable du traitement doit fournir une série d'informations aux personnes dont les données sont traitées. Les entreprises qui traitent des données pour les finalités susmentionnées devront fournir deux informations additionnelles si elles obtiennent directement les données auprès des personnes concernées:

- Le fait que les données sont anonymisées ou pas ;
- Les motifs selon lesquels l'exercice des droits d'accès, de rectification, de limitation et/ou d'opposition de la personne concernée risque de rendre impossible ou d'entraver sérieusement la réalisation de la finalité.

Si les données ne sont pas directement obtenues auprès de la personne concernée, une convention devra être conclue avec le responsable de traitement initial (la personne de laquelle on reçoit les données) ou, en cas d'exemption de la conclusion d'une convention, une notification à ce dernier doit intervenir. Ces documents doivent également être joints au registre des activités de traitement.

5 Délégué à la protection des données : obligations complémentaires

Sur base du RGPD, certaines entreprises, telles que les autorités publiques ou des entreprises dont l'activité de base consiste en un traitement à grande échelle de données sensibles (comme par exemple les hôpitaux) ou en cas de suivi régulier et systématique des personnes concernées (par exemple les entreprises d'assurance) ont l'obligation de désigner un 'délégué à la protection des données' (DPO ou *data protection officer*).

La loi sur la Protection des Données ajoute deux hypothèses possibles d'instauration d'un DPO:

- Une entreprise qui effectue des traitements pour des recherches historiques ou scientifiques ou à des fins statistiques ;
- Un organisme privé qui traite des données à caractère personnel pour le compte d'une autorité publique fédérale ou à qui une autorité publique fédérale a transféré des données à caractère personnel.

Dans la lignée de l'approche basée sur les risques du RGPD, un DPO devra être mis en place dans les deux hypothèses susmentionnées uniquement si le traitement de ces données peut comporter un 'risque élevé'.

Pour la signification de 'risque élevé', il est renvoyé à l'obligation d'effectuer une 'Analyse d'impact de la protection des données' (AIPD, aussi appelée DPIA en anglais: *data protection impact assessment*) pour les activités de traitement à risque.

Le RGPD n'a pas donné de définition du concept de 'risque élevé'. Le European Data Protection Board ou EDPB (auparavant: Groupe des 29), l'organe européen rassemblant les autorités de contrôle, ainsi que l'APD belge ont clarifié ce concept dans leurs

avis et ont listé une série de situations dans lesquelles une AIPD est exigée, comme le cas de traitement à grande échelle de données biométriques, par exemple dans le cadre de la recherche génétique.

Pour de plus amples informations sur l'obligation d'effectuer une AIPD: voir notre Newsflash du 28 mars 2018.

6 Voies de recours

6.1 Aperçu

Les personnes qui estiment être victimes d'une violation de la législation en matière de protection des données ou qui se sentent entravées dans l'exercice de leurs droits, disposent des moyens d'action suivants:

- Une plainte auprès de l'autorité de contrôle compétente (pas nécessairement l'autorité belge);
- Une action en cessation auprès du tribunal pour faire cesser la violation;
- Réclamer des dommages et intérêts devant le tribunal.

La loi belge sur la Protection des Données prévoit la possibilité de se faire représenter par une organisation ou association qui est active en matière de protection des données. Cette organisation ou association peut alors déposer une plainte ou aller devant un tribunal au nom de la personne physique concernée. Cette organisation ou association doit cependant en recevoir la demande et ne peut pas saisir l'APD ou un tribunal d'une demande de sa propre initiative.

6.2 Action en cessation

Lorsqu'une personne ou l'APD veut faire cesser une violation de la législation en matière de protection des données ou veut faire respecter l'exercice de ses droits, une action en cessation peut être introduite auprès du président du tribunal de première instance, siégeant comme en référé. Il est par conséquent question d'une procédure avec des délais réduits en vue de rendre possible une action rapide.

Le président du tribunal de première instance peut prévoir les mesures suivantes dans son 'ordonnance de cessation':

- Laisser un délai pour mettre fin à la violation ou pour accueillir une demande d'exercice d'un droit;
- Publication: affichage de la décision (ou d'un résumé de celle-ci) dans ou hors de l'entreprise, et/ou de sa publication dans les journaux;
- Si des données personnelles incorrectes, incomplètes ou non pertinentes, ou des données personnelles dont la conservation est interdite ont été communiquées à des tiers, le traitant ou le responsable du traitement peuvent se voir obligés de faire connaitre à ce tiers la limitation, la rectification ou l'effacement de ces données personnelles.

S'il existe des motifs sérieux de craindre que des éléments de preuve soutenant la demande en cessation disparaissent ou soient rendus inaccessibles, le demandeur peut demander au président du tribunal de première instance par voie de requête unilatérale d'adopter des mesures prévenant la dissimulation, disparition ou inaccessibilité.

7 Sanctions

Le RGPD exige un régime de sanctions qui est efficace, proportionné et dissuasif.

7.1 Sanctions administratives

Les entreprises qui ne respectent pas les règles peuvent se voir infliger par l'APD de lourdes amendes administratives qui peuvent atteindre jusque 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial d'une entreprise.

L'APD peut cependant adopter d'autres mesures correctrices:

- avertissement;
- blâme;
- obligation d'accueillir des demandes d'exercice de droits ;
- obligation de mettre les traitements en conformité avec le RGPD;
- obligation de communiquer à la personne concernée une violation en lien avec ses données à caractère personnel;
- limitation temporaire ou définitive du traitement, ce qui inclut une interdiction de traitement;
- obligation de rectification ou d'effacement des données à caractère personnel ;
- obligation de suspendre la transmission de données vers un pays tiers.

La Belgique, via la loi sur la Protection des Données, a fait usage de la possibilité offerte par le RGPD, d'exclure les autorités publiques du régime d'amendes administratives, à l'exception des personnes morales de droit public qui offrent des biens et des services sur le marché.

7.2 Sanctions pénales

Sur base de la loi sur la Protection des Données, différentes violations peuvent également être sanctionnées pénalement. Par ailleurs, le responsable du traitement et le sous-traitant ne sont pas les seules personnes à encourir des sanctions, c'est également le cas d'un préposé ou un mandataire. Le responsable du traitement ou le sous-traitant sont, il est vrai, civilement responsables du paiement des amendes auxquelles le préposé ou le mandataire serait condamné.

Pour les violations suivantes, une amende de 2.000 EUR à 120.000 EUR peut être imposée:

- traitement sans base juridique;
- violation des principes de base en matière de protection des données, par négligence grave ou avec intention malveillante;
- maintien d'un traitement ayant fait l'objet d'une objection, sans raisons juridiques impérieuses;
- transfert de données à caractère personnel en dehors de l'Espace Economique Européen sans décision d'adéquation ou garanties adéquates, par négligence grave ou avec intention malveillante;
- violation d'une limitation temporaire ou définitive de traitement imposée par l'APD;
- absence de respect d'une mesure correctrice adoptée par l'APD;
- entrave au contrôle ou rébellion à l'égard de l'APD;
- usage de certifications obtenues sur base de faux ou de certifications dont la durée de validité a expiré.

Une entreprise qui contraint une personne à donner son consentement pour le traitement de ses données à caractère personnel en faisant usage de voies de fait, de violence ou menaces, de dons ou de promesses est punissable d'une amende de 800 à 160.000 EUR.

Le tribunal correctionnel peut par ailleurs décider que la décision (ou un extrait de celle-ci) soit publiée dans un ou plusieurs journaux.

La réglementation antérieure prévoyait déjà des amendes pénales, mais celles-ci étaient peu appliquées en pratique. L'importance de ces amendes et le risque que celles-ci soient imposées sont désormais plus élevés.

Il faut toutefois remarquer que le montant maximum des amendes pénales est considérablement inférieur à celui des amendes administratives. Dans d'autres domaines, tel que le droit pénal social, le niveau des amendes administratives est généralement inférieur à celui des amendes pénales, qui constituent l'ultime remède. L'APD avait, dans son avis sur l'avant-projet de loi sur la Protection des Données, rappelé que le niveau de sanction prévu devait permettre une réaction efficace, proportionnée

et dissuasive. La pratique va devoir déterminer si ces niveaux de sanction auront l'effet escompté. En tout cas, cela aura aussi un impact sur les interactions entre d'une part l'APD qui peut infliger des amendes administratives et d'autre part le ministère public qui peut décider de poursuivre devant le tribunal correctionnel.

7.3 Concours entre procédure administrative et procédure pénale

Pour les violations pour lesquelles il existe tant une sanction administrative qu'une sanction pénale, la loi sur la Protection des Données a déterminé un certain nombre de règles de procédure pour éviter qu'une entreprise ne se voie infliger deux sanctions pour la même violation.

Le ministère public est le premier à agir et peut lancer une information, une instruction et/ou une procédure pénale devant les juridictions répressives. Le ministère public dispose d'un délai de 2 mois à partir du jour de la réception du procès-verbal pour informer l'APD de l'entame d'une action judiciaire. Pendant ce délai de 2 mois et lorsque le ministère public prend réellement le dossier, l'APD n'a pas (plus) la compétence d'exercer ses compétences correctrices et ne pourra donc pas imposer d'amende administrative (élevée). Si le ministère public laisse s'écouler ce délai de 2 mois, une sanction administrative sera par contre encore possible.

Les règles susmentionnées seront cependant uniquement applicables pour autant qu'aucun autre accord de travail n'ait été convenu dans un protocole entre le ministère public et l'APD.

Bruxelles
280, Bd. du Souverain
1160 Bruxelles
Tel.: 02 761 46 00
Fax: 02 761 47 00

Liège
Bd. Frère Orban 25
4000 Liège
Tel.: 04 229 80 11
Fax: 04 229 80 22

Anvers
City Link
Posthofbrug 12
2600 Anvers
Tel.: 03 285 97 80
Fax: 03 285 97 90

Gand
F. Lousbergkaai 103
bus 4-5
9000 Gand
Tel.: 09 261 50 00
Fax: 09 261 55 00

Courtrai
Ring Bedrijvenpark
Brugsesteenweg 255
8500 Courtrai
Tel.: 056 26 08 60
Fax: 056 26 08 70

Hasselt
Kuringersteenweg 172
3500 Hasselt
Tel.: 011 24 79 10
Fax: 011 24 79 11

Partners with you.