Protection des données: vos nouvelles obligations

Doc'Moment ABD-BVD, 18 septembre 2017

Pierre-Yves Thoumsin, avocat

RGPD à partir du 25 mai 2018

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 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

Personne concernée (droits)

- Information
- Accès
- Rectification
- **Effacement**
- Limitation du traitement
- **Portabilité des données**
- Opposition
- **Droits re. prise de décision individuelle automatisée**

Représentant (dans l'UE)

Responsable du traitement (obligations)

- **Licéité**, loyauté, **transparence**
- Limitation des finalités
- Exactitude
- Limitation de la conservation
- Intégrité et confidentialité
- Responsabilité
  - Registre de traitement
  - Analyse d'impact
  - Sécurité
  - **Notification**
  - **Délégué à la protection des données**

Sous-traitant

(traite pour le compte du responsable)

Autorité de contrôle

- Consultation
- **Amendes administratives**

Plan

A. Concepts de base
B. Obligations du responsable de traitement
C. Droits de la personne concernée
D. Contrôle et sanctions

A. Concepts de base

1. Données à caractère personnel
2. Traitement

A.1. Données à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable

- Nom
- Numéro d'identification
- Données de localisation
- Identifiant en ligne
- Éléments propres à l'identité
  - Physique
  - Physiologique
  - Génétique
  - Psychique
  - Économique
  - Culturelle
  - Sociale

A.1. Catégories particulières de données (art. 9)

Principe : interdiction du traitement

- origine raciale ou ethnique
- opinions politiques
- convictions religieuses ou philosophiques ou appartenance syndicale
- **données génétiques et données biométriques aux fins d'identifier une personne physique de manière unique**
- données concernant la santé
- données concernant la vie sexuelle ou l'orientation sexuelle

Exceptions

- Consentement explicite
- Droit du travail / sécurité sociale
- Sauvegarde des intérêts vitaux de la PC
- Membre d'organismes à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale
- Données manifestement rendues publiques
- Constatation, exercice ou défense d'un droit en justice
- Intérêt public (proportionnalité)
- Soins de santé et santé publique
- Fins archivistiques dans l'intérêt public, recherche scientifique ou historique, statistiques (cf art. 89)

- … autres dérogations prévues par les Etats membres

A.2. Traitement

- (ensemble d') opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données
- RGDP applicable au traitement:
  - Automatisé en tout ou en partie
  - Non automatisé, si contenues ou appelées à figurer dans un fichier
- Exceptions
  - Activités ne relevant pas du champ d'application du droit de l'UE;
  - Activité strictement personnelle ou domestique;
  - Autorité dans le cadre de la prévention et détection des infractions pénales

B. Obligations du responsable de traitement

1. **Licéité**, loyauté et **transparence**
2. Limitation des finalités
3. Minimisation des données
4. Exactitude
5. Limitation de la conservation
6. Intégrité et confidentialité
7. **Responsabilité**

B.1. Licéité, loyauté et transparence

- Licéité (art. 6)
  1) Consentement (art. 7)
     - Si déclaration écrite
       - Clairement distincte des autres questions
       - Forme compréhensible et aisément accessible
       - Termes clairs et simples
     - Acte positif clair ≠ silence, cases cochées par défaut ou inactivité
     - Droit de retrait à tout moment
     - Enfants (art. 8)
     - Réévaluer les consentements existants !
  2) Exécution d'un contrat
  3) Obligation légale
  4) Sauvegarde des intérêts vitaux de la PC
  5) Mission d'intérêt public / exercice de l'autorité publique
  6) Intérêts légitimes du responsable de traitement

B.2. Limitation des finalités

- Finalités déterminées, explicites et légitimes
- Traitement ultérieur = compatible
- Exception: « traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fin statistiques » (cf art. 89, § 1)

B.3. Minimisation des données

- Données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités

B.4. Exactitude

- Données exactes + tenues à jour
- Données inexactes → effacement ou rectification

B.5. Limitation de la conservation

- Données permettant l'identification des personnes concernées
  - période n'excédant pas celle nécessaire au regard de la finalité
- Traitement à des fins exclusivement archivistiques dans l'intérêt du public, recherche scientifique ou historique, ou statistiques (art. 89, § 1)
  - Conservation plus longue
  - Mesures techniques et organisationnelles appropriées pour garantir les droits et libertés

B.6. Intégrité et confidentialité

- Sécurité des données (*cf infra*)

B.7. Responsabilité

- Respect des principes

- Responsabilité accrue
  1) Prévention
     a. Principe de responsabilité (*accountability*)
     b. Registre de traitement
     c. Sécurité du traitement
     d. Analyse d'impact
     e. Délégué à la protection des données

  2) Gestion
     a. Notification des violations
     b. Régime de responsabilité (*liability*)

Prévention
a. Responsabilité (*verantwoordelijkheid - accountability*)

- Principe général de proportionnalité (art. 24)

- Mesures techniques et organisationnelles appropriées, notamment :
  - Code de conduite approuvé (art. 40) → organismes sectoriels
  - Mécanismes de certification approuvés (art. 42)

- Obligations répercutées sur les **sous-traitants** (art. 28)

Prévention
b. Registre de traitement (art. 30)

- Contenu:
  - Nom et coordonnées du responsable / représentant / DPO
  - Finalités du traitement
  - Catégories de personnes concernées et des catégories de données
  - Catégories de destinataires
  - Eventuel transfert vers un pays tiers
  - Délai d'effacement pour les différentes catégories
  - Description générale des mesures de sécurité techniques et organisationnelles

- Exemptions si moins de 250 employés, sauf traitement
  - risqué pour droits et libertés
  - non occasionnel
  - données sensibles ou relatives aux condamnations et infractions

- https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

Prévention
c. Protection et sécurité

- Mesures techniques et organisationnelles appropriées (art. 25)
  - Dès la conception (*by design*)
  - Par défaut (*by default*)

- Mesures à prévoir (art. 32):
  - Pseudonymisation et chiffrement
  - Confidentialité, intégrité, disponibilité et résilience des systèmes de traitement
  - Rétablissement de la disponibilité et de l'accès en cas d'incident physique ou technique
  - Procédures de test, analyse et évaluation régulières des mesures de sécurité

Prévention
d. Analyse d'impact (art. 35)

- Dans quel cas ?
  - Recours à de nouvelles technologies et risque élevé pour les droits et libertés

- Contenu minimal
  - Description des opérations envisagées et finalités;
  - Évaluation de la nécessité et de la proportionnalité;
  - Évaluation des risques pour les droits et libertés;
  - Mesures envisagées pour y faire face.

- Consultation préalable de l'autorité de contrôle si l'analyse d'impact indique un risque élevé

Prévention
e. Délégué à la protection des données

- Désignation (art. 37)
  - Autorités et organismes publics
  - Activités exigeant un suivi régulier et systématique à grande échelle des personnes concernées
  - Traitement de données sensibles / condamnations pénales
  - Autres cas facultatifs

- Fonction (art. 38)
  - Associé à toute question relative à la protection des données
  - Point de contact pour les personnes concernées
  - Secret professionnel
  - Indépendance vis-à-vis du sous-traitant

- Missions (art. 39)
  - Informer et conseiller le responsable de traitement
  - Contrôler le respect du RGDP et autres dispositions en matière de protection des données
  - Conseils concernant l'analyse d'impact
  - Coopérer avec l'autorité de contrôle
  - Point de contact pour l'autorité de contrôle

Gestion
a. Notification des violations

- Notification à l'autorité de contrôle (art. 33)
  - En cas de violation, dans les 72 heures
  - SAUF si la violation n'est pas susceptible d'engendrer une violation des droits et libertés des personnes physiques

- Communication à la personne concernée (art. 34)
  - Si susceptible d'engendrer un risque élevé pour les droits et libertés
  - SAUF si mesures préalables (chiffrement), ultérieures ou disproportionnée

- Notification du sous-traitant au responsable

Gestion
b. *Liability*

- Le responsable ou le sous-traitant peuvent être poursuivis par la personne concernée

- Responsabilité solidaire → réparation effective

C. Droits de la personne concernée

1. Information
2. Accès
3. Rectification
4. **Effacement**
5. Limitation du traitement
6. **Portabilité des données**
7. Opposition
8. **Droits re. prise de décision individuelle automatisée**

D.1. Information (art. 12 – 14)

- Forme concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples
- Contenu:
  - Identité et coordonnées du (représentant du) responsable
  - Coordonnées DPO
  - Finalités
  - Base légale
  - Catégories de données concernées (si pas collectées auprès de la personne concernée)
  - Intérêts légitimes du responsable
  - (Catégories) de destinataires des données
  - Transfert vers des pays tiers et garanties
  - Durée de conservation ou critères pour déterminer la durée
  - Existence des droits d'accès, rectification
  - Existence des droits d'effacement, limitation, opposition et portabilité
  - Existences du droit de retirer son consentement à tout moment
  - Droit de retirer son consentement à tout moment
  - Droit d'introduire une réclamation auprès d'une autorité de contrôle
  - Origine réglementaire ou contractuelle de la fourniture de données
  - Obligation ou non de fournir les données et conséquences d'un refus
  - Existence d'une prise de décision automatisée, y compris profilage
  - Source des données (si pas collectées auprès de la personne concernée)

D.2. Accès (art. 15)

D.3. Rectification (art. 16)

D.4. Effacement (art. 17)

- Droit à l'oubli (cf. CJUE, 13 mai 2014, *Google Spain*, C-131/12)

- Hypothèses visées:
  - Plus nécessaires au regard des finalités
  - Retrait du consentement et plus d'autre fondement juridique
  - Opposition au traitement et pas de motif légitime impérieux
  - Traitement illicite
  - Effacement pour respecter une obligation légale
  - Données collectées quand la personne était un enfant

- Mesures raisonnables pour informer les responsables du traitement en aval

D.5. Limitation du traitement (art. 18)

- « marquage des données à caractère personnel conservées, en vue de limiter leur traitement futur »
- Généralement dans l'attente de l'issue d'une contestation en cours

D.6. Portabilité des données (art. 20)

- Deux facettes:
  - Droit de recevoir les données dans un format structuré, couramment utilisé et lisible par machine
  - Droit de transmettre ces données à un autre responsable du traitement
- Deux conditions
  - Traitement fondé sur le consentement
  - Traitement effectué à l'aide de procédés automatisés

D.7. Opposition (art. 21)

- Pour des raisons tenant à sa situation particulière

- Sans justification, lorsque le traitement est effectué à des fins de prospection

D.8. Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement individuel automatisé (art. 22)

- Profilage: « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements pour cette personne physique »

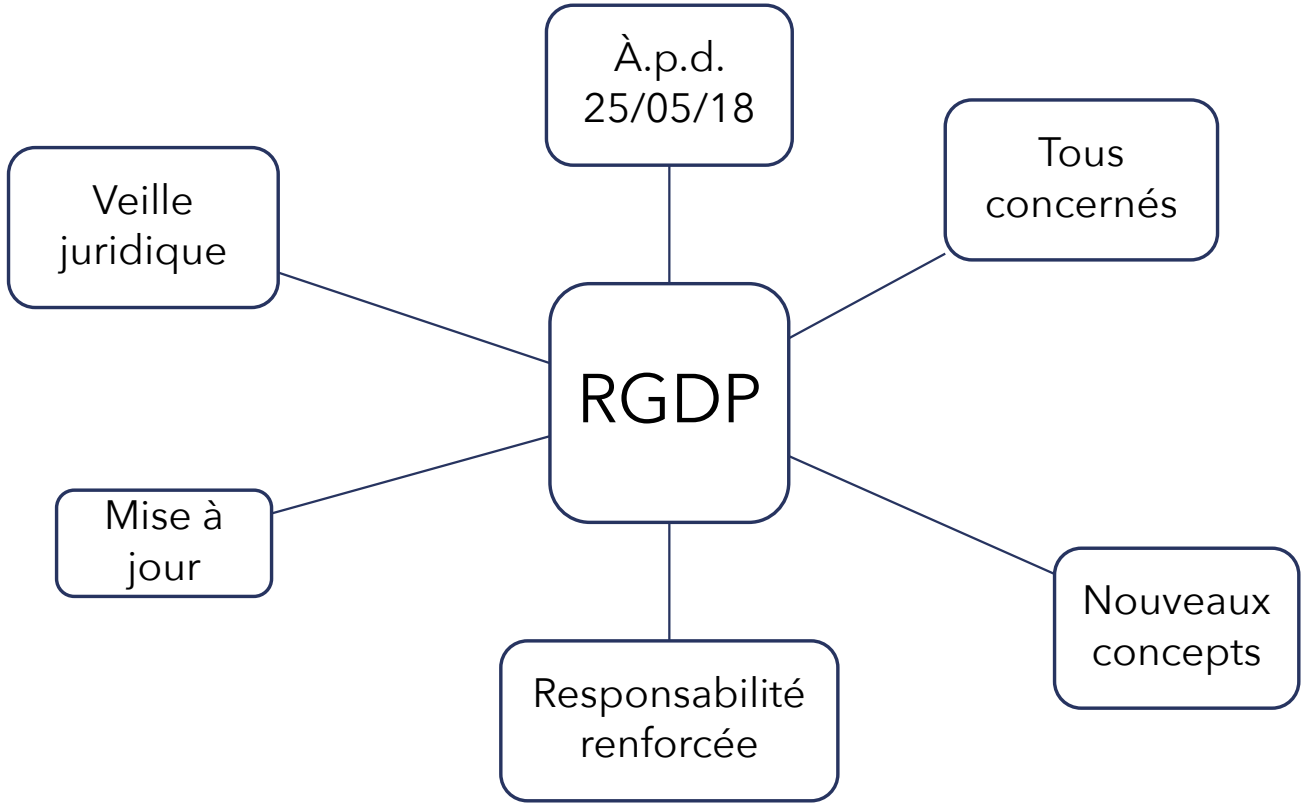
- Exceptions:
  - Nécessité pour la conclusion ou l'exécution d'un contrat;
  - Autorisée par le droit national et des mesures appropriées sauvegardent les droits et libertés;
  - Consentement explicite.

D. Contrôle et sanctions

Recours, responsabilités et sanctions

- Réclamation auprès de l'autorité de contrôle (art. 77)
- Recours juridictionnel contre…
  - Une décision de l'autorité de contrôle (art. 78);
  - Contre le responsable du traitement ou un sous-traitant (art. 79)
- Droit à réparation du dommage matériel et moral (art. 82)
- Amendes administratives effectives, proportionnées et dissuasives (art. 83):
  - Jusqu'à 10.000.000 EUR / 20.000.000 EUR ou, dans le cas d'une entreprise, 2% / 4% du C.A. annuel mondial

Conclusion


À.p.d.
25/05/18
Veille
juridique
Tous
concernés
RGDP
Mise à
jour
Nouveaux
concepts
Responsabilité
renforcée

Pierre-Yves Thoumsin

pierre-yves.thoumsin@jvm.be
02 289 00 20

www.jvm.be
www.belgiantrademark.be

Twitter: @PYThoumsin