

Table des matières

Avant-propos	1
1. Un nouveau règlement pour un nouveau contexte	2
1.1. La vie privée au centre des préoccupations	2
1.2. Une plus grande harmonisation	3
1.3. Un champ d'application large	3
1.4. Une opportunité pour l'entreprise	4
1.5. Comprendre le RGPD et le mettre en pratique	4
1.6. Méthodologie et références utilisées	5
2. Comprendre les règles encadrant le traitement des données à caractère personnel	7
2.1. Les concepts du traitement de données	7
2.1.1. Données à caractère personnel	7
2.1.2. Traitement de données	8
2.1.3. Personne concernée	9
2.1.4. Responsable du traitement	10
2.1.5. Sous-traitant	10
2.1.6. Autorité de contrôle	11
2.2. Les principes relatifs au traitement	11
2.2.1. Licéité	12
2.2.2. Loyauté et transparence	19
2.2.3. Limitation des finalités	19
2.2.4. Minimisation des données	20
2.2.5. Exactitude	21
2.2.6. Limitation du délai de conservation	21
2.2.7. Intégrité et confidentialité des données	22
2.2.8. Le nouveau principe de responsabilité sous le RGPD	23
2.3. Les droits reconnus à la personne concernée	24
2.3.1. Accès	25
2.3.2. Rectification	26
2.3.3. Effacement	26
2.3.4. Limitation du traitement	27
2.3.5. Portabilité des données	28
2.3.6. Opposition	28
2.3.7. Opposition à la prise de décision individuelle automatisée	29

2.4.	La protection des données à caractère personnel dans un contexte international	30
2.4.1.	La libre circulation des données dans l'Union européenne	30
2.4.2.	Le transfert de données vers un pays tiers ou à une organisation internationale	30
2.5.	Le contrôle du respect de la réglementation et les sanctions	32
2.5.1.	Contrôle administratif par l'autorité de contrôle	32
2.5.2.	Contrôle judiciaire	34
3.	Mettre en œuvre le RGPD au sein de son organisation	35
3.1.	Un nouveau préalable : établir un registre des activités de traitement	35
3.1.1.	Champ d'application	36
3.1.2.	Contenu du registre du responsable de traitement	38
3.1.3.	Contenu du registre du sous-traitant	40
3.1.4.	Format du registre	41
3.2.	Informers les personnes concernées	41
3.2.1.	Quelles informations fournir ?	41
3.2.2.	Sous quelle forme fournir ces informations ?	43
3.2.3.	Quand fournir ces informations ?	44
3.3.	Permettre l'exercice des droits des personnes concernées	45
3.3.1.	Quand le responsable du traitement doit-il collaborer avec la personne concernée ?	46
3.3.2.	Quand le responsable du traitement peut-il refuser de collaborer ? ..	46
3.3.3.	Dans quel délai le responsable du traitement doit-il réagir ?	47
3.4.	Garantir l'intégrité et la confidentialité des données	47
3.4.1.	Protection dès la conception	47
3.4.2.	Protection par défaut	48
3.5.	Réaliser une analyse d'impact	49
3.5.1.	Quand réaliser une analyse d'impact ?	49
3.5.2.	Contenu de l'analyse d'impact	51
3.6.	Désigner un délégué à la protection des données	52
3.6.1.	Quand désigner un délégué à la protection des données ?	52
3.6.2.	Qui désigner comme délégué à la protection des données ?	54
3.6.3.	Quelles missions confier au délégué à la protection des données ? ..	55
3.7.	Vérifier les contrats avec ses sous-traitants	55
3.8.	Réagir en cas de violation de données à caractère personnel	57
3.8.1.	Notification à l'Autorité de contrôle	58
3.8.2.	Communication à la personne concernée	58
3.8.3.	Documenter toute violation de données à caractère personnel	60

4. Comment s’y prendre ?	61
4.1. Faire le point sur les traitements de données	61
4.1.1. Identifier les flux de données	61
4.1.2. Identifier les documents existants	62
4.1.3. Identifier les mesures techniques et organisationnelles en place ...	62
4.2. Analyser la conformité de la situation existante	62
4.3. Définir un plan de mise en conformité	62
4.4. Mettre en place une veille juridique et organisationnelle	63
Abréviations utilisées	64

Avant-propos

RGPD. Quatre lettres qui suscitent la curiosité, le débat et souvent de vives inquiétudes, à mesure qu'approche la date du 25 mai 2018. C'est à cette date que deviendra applicable ce Règlement Général sur la Protection de Données, qui pose un nouveau cadre légal harmonisé pour la protection des données personnelles au sein de l'Union européenne.

Curiosité tout d'abord, car le RGPD représente un travail législatif de grande ampleur. Il remplace une directive vieille de 20 ans, dont il triple le volume. Une protection renforcée des données personnelles à l'ère du numérique et du « big data » est à ce prix.

Débat ensuite, car le RGPD ne constitue pas une révolution, mais une évolution. Les entreprises qui connaissent déjà les règles de base en matière de protection des données personnelles ne devraient donc pas être entièrement dépaysées.

Inquiétude, enfin, car le RGPD impose une série d'obligations nouvelles ou renforcées aux entreprises et que leur respect est assorti de sanctions significatives.

Ce dossier a pour objectif de permettre à l'entreprise d'aborder sereinement sa mise en conformité au RGPD, fondée sur une bonne compréhension des règles et de leur impact concret pour l'entreprise.

Emmanuel Plasschaert

Avocat - associé
Crowell & Moring LLP
Bruxelles
www.crowell.com

Pierre-Yves Thoumsin

Avocat
JVM
Bruxelles
www.jvm.be

Abréviations utilisées

- **CPVP**
Commission de protection de la vie privée (<https://www.privacycommission.be>)
- **G29**
Groupe de travail Article 29 sur la protection des données
(<http://ec.europa.eu/newsroom/article29/news-overview.cfm>)
- **Recommandation 04/2017**
Recommandation n° 04/2017 de la CPVP du 24 mai 2017 relative à la désignation d'un délégué à la protection des données conformément au Règlement général sur la protection des données (RGPD), en particulier l'admissibilité du cumul de cette fonction avec d'autres fonctions dont celle de conseiller en sécurité
(https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_04_2017.pdf)
- **Recommandation 06/2017**
Recommandation n° 06/2017 de la CPVP du 14 juin 2017 relative au Registre des activités de traitements (article 30 du RGPD)
(https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_06_2017_0.pdf)
- **Recommandation 01/2018**
Recommandation n° 01/2018 du 28 février concernant l'analyse d'impact relative à la protection des données et la consultation préalable
(<https://www.privacycommission.be/fr/recommandation-dinitiative-concernant-lanalyse-dimpact-relative-a-la-protection-des-donnees>)
- **Vade-mecum**
RGPD Vade-mecum pour les PME. Un guide pour préparer les petites et moyennes entreprises (PME) au Règlement général sur la protection des données
(https://www.privacycommission.be/sites/privacycommission/files/documents/PME_FR.pdf)
- **WP259**
Lignes directrices WP259 du Groupe de travail article 29 sur le consentement adoptées le 28 novembre 2017
(http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239)