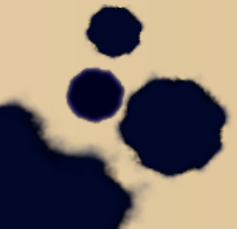
#GDPRBookClub

Présentation du RGPD à travers l'expérience d'un club de lecture atypique

Suzanne Vergnolle & Benoît Piedallu

Pourquoi faire un club de lecture ?

- Historique
- Volonté
- Logistique



GDPR ou RGPD, mais qu'est-ce donc ?

- Historique
- Quelle différence entre une directive et un règlement ?
- Les renvois aux droits nationaux
  - Action de groupe,
  - Mineurs,
  - Algorithmes.

Contenu du RGPD

Lire le règlement : distinction entre les considérants et les articles

→ Mais quand ce texte s'applique-t-il ?

Contenu du RGPD

En cas de traitement automatisé,

ou non,

de données à caractère personnel

Définition de donnée personnelle art. 4(1)

1) «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;

Définition de donnée à caractère personnel art. 4 (1) RGPD

« Toute information se rapportant à une **personne physique identifiée ou identifiable** »

Définition de donnée à caractère personnel : Art. 4 (1) RGPD

Pour le club de lecture :

- personne physique,
- mort,
- pseudonymisation / anonymisation
- données sensibles

Définition de donnée à caractère personnel : Art. 4 (1) RGPD

5) «pseudonymisation», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

(26) Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche.

Qu'est-ce qu'un traitement de données personnelles ? Art. 4 (2)

2) «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;

Qu'est-ce qu'un traitement de données personnelles ? Art. 4 (2)

« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données »

Qu'est-ce qu'un responsable du traitement ? art. 4 (7)

7) «responsable du 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; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

Qu'est-ce qu'un responsable du traitement ? art. 4 (7)

« 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** »

Qu'est-ce qu'un sous-traitant ? art. 4 (8)

8) «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;

Qu'est-ce qu'un sous-traitant ?
art. 4 (8)

« 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** »

Dans quels cas est-il possible de traiter des données personnelles ? art. 6

Article 6

Licéité du traitement

1. Le traitement n'est licite que si, et dans la mesure où, au moins 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;

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.

Dans quels cas est-il possible de traiter des données personnelles ? art. 6

Consentement

Contrat

Obligation légale

Intérêts vitaux

Mission d'intérêt public

Intérêts légitimes

Quelles dispositions clées ?

Le principe de responsabilité

Sécurité et **violations de données**

Les **droits des personnes**

Les **sanctions**

Passage d'un système déclaratif à un principe de responsabilité

Capacité de démontrer le respect des obligations à tout moment

- Privacy by design / default (art. 25)
- Registre (art. 30)
- Sécurité (art. 32)

Privacy by design / by default art. 25

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement 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 mettre en œuvre 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 présent règlement et de protéger les droits de la personne concernée.

S. Vergnolle B.Piedallu

Le registre des activités de traitement

Fiche de registre	ref-000
Description du traitement	
Nom / sigle	
N° / REF	ref-000
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	
Sous-finalité 3	
Sous-finalité 4	
Sous-finalité 5	

Mesures de sécurité	
Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images...		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale,		
Données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM, etc.)		

Les obligations
L'obligation de sécurité

Article 32 RGPD

Vise le responsable du traitement **et** le sous traitant

Mise en œuvre de :

- Mesures **techniques et organisationnelles**
- Pour garantir **niveau de sécurité** approprié au **risque**

La sécurité

- Le point actu du book club
- Walmart
- Equifax
- Ashley Madison, Grindr, Cambridge Analytica...

Violation de données personnelles art. 4 (12)

12) «violation de données à caractère personnel», 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;

Notification de la violation art. 33

Article 33

Notification à l'autorité de contrôle d'une violation de données à caractère personnel

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, 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.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Notification de la violation à l'autorité art. 33

- Un traitement de données personnelles,
- A subi une atteinte,
- Notification à l'autorité compétente dans les 72 heures de la découverte de l'atteinte.

Sauf si la faille n'est pas susceptible de porter atteinte aux droits et libertés

Quelques uns des droits des personnes

- Transparence sur les traitements (art. 12, 13 et 14),
- Droit d'accès, éventuellement avec copie des données (art. 15),
  - ➢ Droit à la portabilité (art. 20)
- Droit de ne pas faire l'objet d'une décision individuelle automatisée (art. 22)
- Notification en cas de modification de données au destinataire (art. 25)

Sanctions : amendes administratives art. 83

Manquement aux obligations :

jusqu'à 2 % à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent ou **jusqu'à 10 à 20 millions d'euros**.

Le montant le plus élevé est retenu

Merci de votre attention !

Plus d'informations : #GDPRBookClub

Suzanne Vergnolle (@SuVergnolle)
&
Benoît Piedallu (@klorydryk)