GIDE

GIDE LOYRETTE NOUEL

Thème n° 4

Règlement Général sur la Protection des Données

Le principe d’accountability

27 mars 2018

Table des matières

1. Introduction

Les précédents

- Reconnaissance explicite dans les lignes directrices de l'OCDE de 1980
- Les BCR ou « règles d'entreprise contraignantes » : pour les transferts de données hors UE
- Norme ISO 29100 vise explicitement l'accountability
- Avis du G29 n°3/2010 sur le principe de responsabilité

1. Introduction

Avis n°3/2010 (§ 34)

- Article X – Mise en œuvre des principes de protection des données
  « 1. Le RT prend des mesures efficaces et appropriées en vue de garantir le respect des principes et obligations énoncés dans la directive.
  2. A la demande de l'autorité de contrôle, le RT apporte à celle-ci la preuve du respect des dispositions du paragraphe 1. »

RGPD

- Le RGPD ne cite que deux fois le terme « accountability » (Considérant 85 et art. 5-2 RGPD)
- Aucune définition n'est mentionnée

2. Les principes à respecter – art. 5-1 RGPD

- Les données doivent être traitées de manière loyale, licite et transparente (bases légales)
- Les finalités du traitement doivent être déterminées, explicites, légitimes ; et les données ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités
- Les données doivent être adéquates, pertinentes et limitées
- Les données doivent être exactes et si nécessaire tenues à jour
- Les données ne doivent pas être conservées au-delà de la durée nécessaire au regard de la finalité du traitement
- Les données doivent être traitées en mettant en place les mesures de sécurité appropriées

2. Les principes à respecter – art. 5-2 RGPD

Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

3. L'obligation générale du RT – art. 24 RGPD

1. Compte tenu 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, pour les droits et libertés des personnes physiques,

le RT met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement.

Ces mesures sont réexaminées et actualisées si nécessaire.

3. L’obligation générale du RT – art. 24 RGPD

2. Lorsque cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

3. L’obligation générale du RT, et sa traduction – art. 82-2 et 82- 3 RGPD

2. Tout RT ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du RGPD. Un ST n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le RGPD qui incombent spécifiquement aux ST ou qu'il a agi en-dehors des instructions licites du RT ou contrairement à celles-ci.

3. Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

4. Le délégué à la protection des données

Le DPO :

- La pierre angulaire du principe d'accountability (G29 – Guidelines DPO)
- Il contrôle le respect du RGPD et des règles internes du RT/ST y compris sensibilisation et formation du personnel et audits + rôle de conseil (PIA…)
- L'interface de l'autorité de contrôle et celle des personnes concernées pour l'exercice de leurs droits

5. Le registre

Article 30 RGPD

Le registre se présente sous forme écrite (électronique)

Le registre doit pouvoir être mis à disposition de l'autorité de contrôle

Exemption pour les entreprises (de moins de 250 salariés), sauf si le traitement effectué :

- est susceptible de comporter un risque pour les droits/libertés des personnes concernées,
- n'est pas occasionnel, ou
- porte notamment sur des données particulières ou des données relatives à des condamnations pénales et infractions

Registre RT	Registre ST
Nom et coordonnées du RT/ST/DPO/représentant	
Finalités du traitement	
Catégories de personnes concernées et de données traitées	
Catégories de destinataires	
Délais prévus pour l'effacement *	Catégories de traitement effectués pour chaque RT
Transferts de données hors UE, précision du pays visé et garanties appropriées	
Description générale les mesures techniques et organisationnelles*	

* *Dans la mesure du possible*

5. Le registre

L'obligation de tenue du registre est dynamique

- Mise à jour en fonction de l'évolution des traitements existants ou création de nouveaux traitements

Le RT/ST est libre de faire figurer des informations supplémentaires dans le registre:

- Éventuelle réalisation d'une analyse d'impact
- Mention de la base légale du traitement …

6. Politique de sécurité – art 32 RGPD

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, pour les droits et libertés des personnes physiques,

le RT et le ST mettent en œuvre **les mesures techniques et organisationnelles appropriées** afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

6. Politique de sécurité – art 32 RGPD

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

7. Autres procédures applicables à la mise en œuvre d'un traitement

Privacy by design

Privacy by default

Analyse d'impact

8. Autre documentation

Encadrement des relations avec les tiers

Les contrats avec les sous-traitants – art 28-3

- **Intégrant les obligations prévues par le RGPD**

La politique de suivi des relations de sous-traitance

- **Modalités d'audit des ST et résultats**
- **Instructions documentées du RT pendant le traitement**

Le cas échéant, les accords avec d'autres RT en cas de coresponsabilité

8. Autre documentation

Encadrement des transferts hors UE

Inventaire général des transferts

- **Indiquant pour chacun le mécanisme de transfert retenu**

La documentation relative à la mise en œuvre des transferts

- **Les BCR et leurs décisions d'approbation par l'Autorité**
- **Les clauses types signées**
- **Les documents relatifs aux transferts basés sur des exceptions de l'article 49 du RGPD**
- **La justification de l'adhésion de l'entreprise américaine au Privacy Shield (https://www.privacyshield.gov/list)**

8. Autre documentation

Le respect des droits des personnes concernées

Procédure de traitement des demandes des personnes concernée sur l'exercice de leurs droits

Traçabilité des réponses apportées

Politique de conservation des données

8. Autre documentation

Documentation relative aux violations de données personnelles

La procédure de gestion des violations de données personnelles

Le registre des violations de données personnelles

Les éléments de justification de l'exception de notification à l'autorité et/ou de communication aux personnes concernées

8. Autre documentation

Codes de conduite et certification :

Attestation de l'adhésion à un code de conduite et la documentation associée

Les certifications et leur renouvellement

Correspondances avec l'autorité

9. Sanctions

Art. 83 RGPD:

*« Les violations des dispositions […] font l'objet […] d'amendes administratives pouvant s'élever jusqu'à **10 M €** ou, dans le cas d'une entreprise, jusqu'à **2 % du chiffre d'affaires annuel mondial total** de l'exercice précédent, le montant le plus élevé étant retenu.*

*Les violations des dispositions […] font l'objet, […] d'amendes administratives pouvant s'élever jusqu'à **20 M €** ou, dans le cas d'une entreprise, jusqu'à **4 % du chiffre d'affaires annuel mondial total** de l'exercice précédent, le montant le plus élevé étant retenu*

10. Quelques recommandations

- L’accountibility: la checklist pour se préparer à un contrôle CNIL
- Créer un répertoire de la documentation
- Nommer un DPO de manière facultative : l’obligation de respecter toutes les dispositions relatives au DPO
- Débuter le registre avec la base CNIL (déclarations antérieures, etc.)
- Exhaustivité du registre
- Politique de conservation des données

GIDE

GIDE LOYRETTE NOUEL

Merci pour votre attention

Questions / Réponses

Thierry Dor
dor@gide.com

Gide Loyrette Nouel A.A.R.P.I.
22 cours Albert Ier
75008 Paris
tél. +33 (0)1 40 75 60 00
info@gide.com - gide.com

ALGER
BRUXELLES
CASABLANCA
ISTANBUL
LE CAIRE
LONDRES
MOSCOU
NEW YORK
PARIS
PÉKIN
SHANGHAI
TEHERAN
TUNIS
VARSOVIE