GIDE

GIDE LOYRETTE NOUEL

Thème n°2

Règlement Général sur la Protection des Données

La sous-traitance de traitements de données personnelles

7 février 2018

Table des matières

1. Sources de la notion de sous-traitance
2. Définitions
3. Une obligation initiale : les garanties appropriées
4. Les informations devant figurer dans le contrat
5. Les obligations du sous-traitant devant figurer dans le contrat
6. Autres obligations incombant au sous-traitant
7. Le « guichet unique »
8. Responsabilité et amendes
9. Quelques recommandations

1. Sources de la notion de sous-traitance (1/2)

- Guidelines OCDE de 1980 régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel :

  « En conséquence, il est essentiel qu'aux termes du droit interne la responsabilité, devant la loi, du respect des règles et des décisions concernant la protection de la vie privée incombe au maître du fichier, qui ne devrait pas être relevé de cette obligation pour la simple raison que le traitement des données est effectué pour son compte par un tiers, tel qu'un centre de traitement à façon »

- Naissance de la notion de sous-traitant dans la 1ère proposition de la Commission lors de l'élaboration de la Directive 95/46/CE, afin *« d'éviter qu'un traitement par un tiers pour le compte du responsable du fichier ait pour conséquence d'affaiblir la protection de la personne concernée »*

1. Sources de la notion de sous-traitance (2/2)

- Articles 16 et 17 Directive 95/46/CE → Article 35 Loi de 1978 :

« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, […], que sur instruction du responsable du traitement. […]

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. »

2. Définitions (1/2)

Art. 4.7 RGPD

- Le **responsable du traitement** détermine les finalités et les moyens du traitement

Art. 4.8 RGPD

- Le **sous-traitant** traite des données personnelles pour le compte et sur instruction du responsable du traitement

Art. 26 RGPD

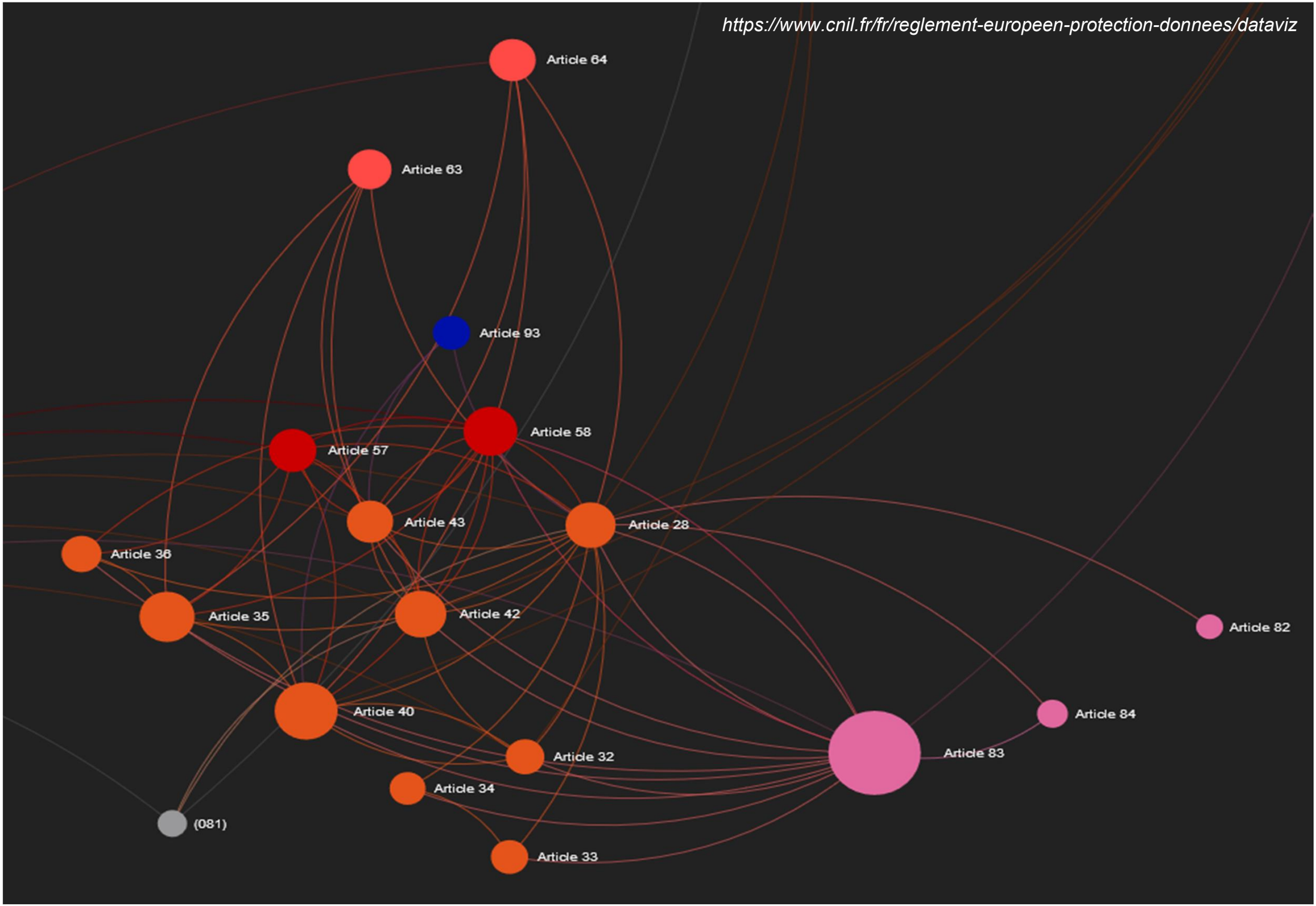
- Lorsque deux responsables du traitement (ou plus) déterminent conjointement les finalités et les moyens d'un traitement, ils sont **responsables conjoints du traitement**

2. Définitions (2/2)

Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» du G29 du 16 février 2010

→ Faisceau d'indices permettant de déterminer la qualité des parties :

- *Niveau d'instruction*
- *Niveau de contrôle*
- *Transparence*
- *Expertise*


https://www.cnil.fr/fr/reglement-europeen-protection-donnees/dataviz
Article 64
Article 63
Article 93
Article 58
Article 57
Article 43
Article 28
Article 36
Article 35
Article 42
Article 82
Article 40
Article 84
Article 83
Article 32
Article 34
(081)
Article 33

3. Une obligation initiale : les garanties appropriées

Le RT doit uniquement faire appel à des ST présentant des garanties appropriées (art 28.1 RGPD), et effectuer des audits réguliers

L'adhésion d'un ST à des codes de conduite (art 40 RGPD) ou à un mécanisme de certification approuvé (art 42 RGPD) peut aider à démontrer l'existence de garanties suffisantes

4. Les informations devant figurer dans le contrat (RGPD 28-3)

- L'objet et la durée du traitement
- La nature et la finalité du traitement
- Le type de données personnelles et les catégories de personnes concernées
- Les obligations et les droits du responsable du traitement

5. Les obligations du sous-traitant devant figurer dans le contrat (1/3) (RGPD 28-3)

a

- Ne traite les données personnelles que sur instruction documentée du RT, y compris en ce qui concerne les transferts de DP vers un pays tiers

b

- Veille à ce que les personnes autorisées à traiter les DP s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité

c

- Prend toutes les mesures requises au titre de l'obligation de sécurité (RGPD 32)

5. Les obligations du sous-traitant devant figurer dans le contrat (2/3) (RGPD 28-3)

d

- Respecte les conditions encadrant le recrutement d'un autre ST

e

- Aide le RT […] à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits

f

- Aide le RT à garantir le respect des obligations de sécurité, de notification à l'AC et de communication à la personne concernée d'une violation de DP, de réalisation d'analyse d'impact et de consultation préalable de l'AC (RGPD 32 à 36)

5. Les obligations du sous-traitant devant figurer dans le contrat (3/3) (RGPD 28-3)

g

- Selon le choix du RT, supprime toutes les DP ou les renvoie au RT au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou d'un État membre n'exige la conservation des DP

h

- Met à la disposition du RT toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits

- Informe immédiatement le RT si, selon lui, une instruction constitue une violation du présent règlement ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la PD

6. Autres obligations incombant au sous-traitant (1/2)

- Tenue d’un registre, sauf si le ST emploie moins de 250 salariés et qu'il ne procède pas à des traitements présentant des risques particuliers (RGPD 30-2), qui comprend :

  - Le nom et les coordonnées de chaque RT, le cas échéant du représentant du RT ou du ST, et celles du DPO
  - Les catégories de traitements effectués pour chaque RT
  - Les éventuels transferts hors UE
  - Dans la mesure du possible, une description des mesures de sécurité techniques et organisationnelles visées à RGPD 32-1

6. Autres obligations incombant au sous-traitant (2/2)

Désignation d'un DPO

- (Art 37 RGPD) Obligatoire si le ST :
  - est un organisme public,
  - effectue un suivi régulier et à grande échelle ou
  - traite de données particulières (art 9 et 10 RGPD) à grande échelle

7. Le « guichet unique » (RGPD 56)

Un ST peut bénéficier du « guichet unique » ou « one-stop-shop »

Ce mécanisme permet aux ST réalisant des traitements transfrontaliers de ne devoir échanger qu'avec une seule autorité « chef de file »

Cette autorité sera celle de l'établissement principal (administration centrale ou établissement où se déroule l'essentiel des activités de traitement)

Elle prendra des décisions applicables à l'ensemble des Etats membres concernés par ces traitements

8. Responsabilité et amendes

Art 28.10

- Si un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce qui concerne ce traitement

Art 82

- Droit à réparation de la personne et responsabilité du responsable de traitement et du sous-traitant

Art 83

- Le sous-traitant est soumis aux mêmes amendes administratives que le responsable du traitement

9. Quelques recommandations (1/2)

- S’interroger sur l’éventuelle existence de règlementations spécifiques en matière d’externalisation
- Si deux DPO sont nommés par un RT et un ST en relation, veiller à la communication et à une cohérence des deux registres
- Pour les ST, utiliser des certifications alternatives (ISO, TRUSTe, SOC 1, SOC 2, SOC 3, etc) en attendant les textes « officiels »
- Le ST qui tient un registre doit aussi tenir un registre RT pour ses propres traitements

9. Quelques recommandations (2/2)

- Même si la tenue d'un registre n'est pas obligatoire, elle est conseillée
- Anticiper les avenants aux contrats de sous-traitance
- Pour le RT, négocier notification / l'information en matière de violation de données + info et exercice des droits
- Pour les RT, réaliser des audits réguliers du/des ST, en fonction des risques qu'impliquent le(s) traitement(s)

GIDE

GIDE LOYRETTE NOUEL

Merci pour votre attention

Questions / Réponses

Thierry Dor dor@gide.com

Aurélie Pacaud aurelie.pacaud@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
LONDRES
MOSCOU
NEW YORK
PARIS
PÉKIN
SHANGHAI
TEHERAN
TUNIS
VARSOVIE