#CONEXT

le salon du commerce intelligent

Règlement européen relatif aux données personnelles : décryptage et conseils pour se préparer

sncd de la data à la logistique

syndicat national de la communication directe

Partagez en direct vos réactions sur TWITTER avec #conext @Sncdmulticanal

Présentation Sncd

Le SNCD s'appuie sur ses **200 sociétés membres** et les accompagne dans l'**innovation industrielle et technologique** qui découle de la **forte croissance des données** disponibles et des **droits et usages associés**

Présentation Sncd

- **Des prestataires engagés**
  - Veille, déontologie et échange de bonnes pratiques
  - Promotion des techniques et métiers
  - Représentation institutionnelle et défense des métiers
- **Assistance et formation** : Informatique et libertés, Convention collective, RSE…
- **Un réseau** et du **networking**
- **Études** et interventions d'**experts**

brm AVOCATS en bref :

Situé à Lille (Parc Euratechnologies)

et Paris

Propriété intellectuelle (Droit d'auteur, Marques, Brevets, Bases de données)

Nouvelles technologies (Protection des données personnelles, Contrats Informatiques, Consommation)

AVOCATS

brm en bref :

SPÉCIALISTE

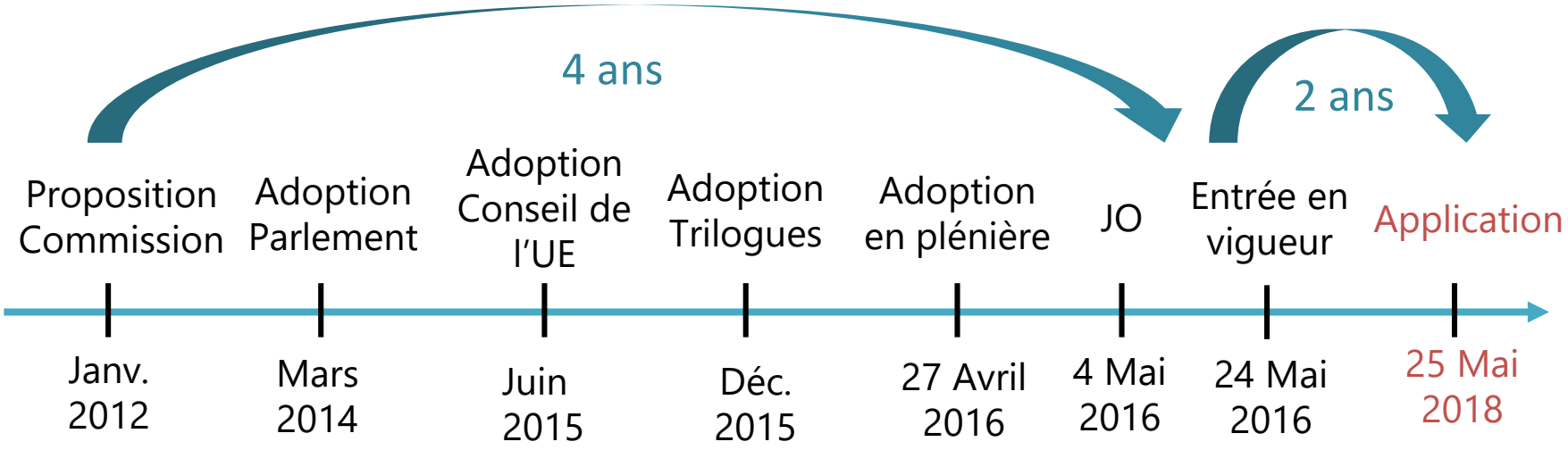
Les mutations en cours

	Données personnelles	Numérique
Aujourd'hui	**Directive 95/46/CE** (protection des données personnelles) — Loi I&L	**Directive e-Privacy** 2002/58/CE (prospection électronique) — CPCE Révisée en 2009 avec le **Paquet Telecom** 2009/136/CE (cookies) — Art 32-II I&L
Demain	**Règlement européen** 2016/679 sur les données personnelles Adopté le 27 avril 2016	**Règlement européen** venant **réviser la Directive e-Privacy** (prospection électronique, cookies, tél., BtoB…) Prévu pour l'automne 2017
	Applicable 25 mai 2018	Objectif : Applicable 25 mai 2018 → mais réaliste 2019

Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

L'adoption du Règlement européen

Chronologie



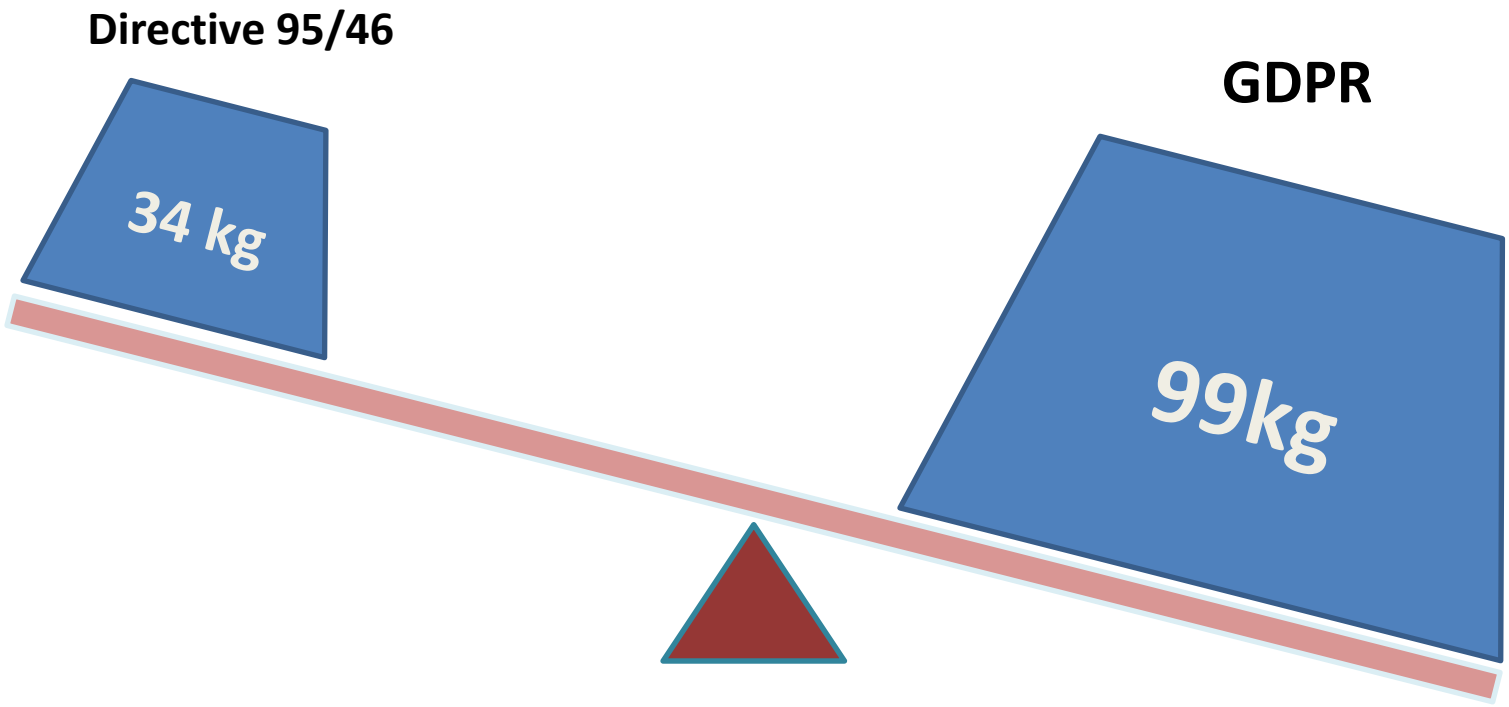
2018

25 mai 2018

Entrée en application

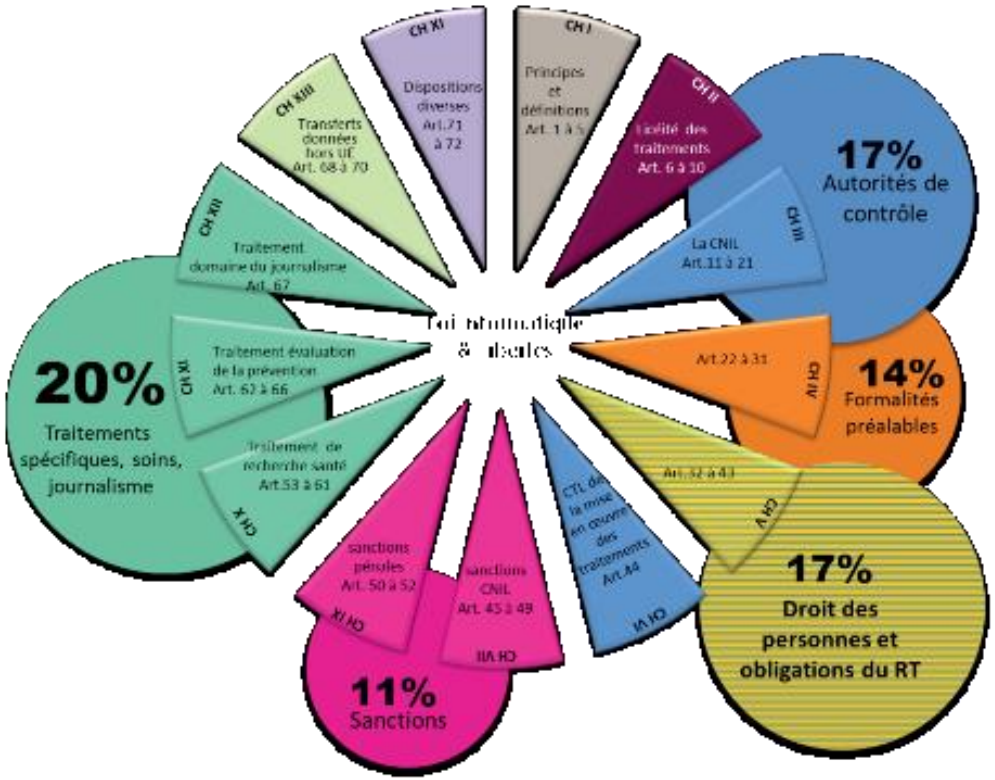
Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

L’adoption du Règlement européen



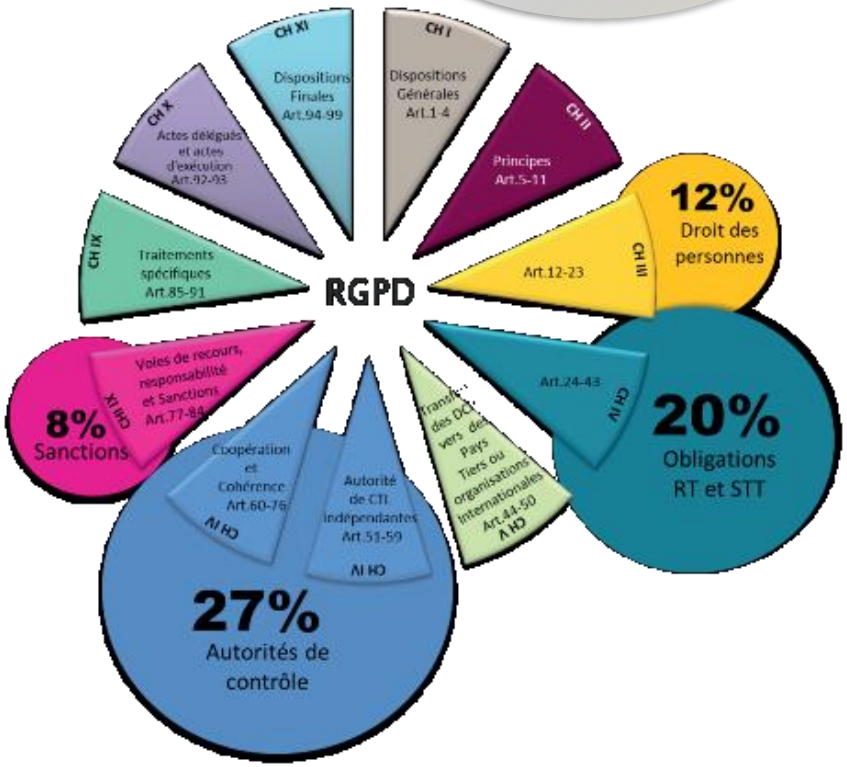
Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

L'adoption du Règlement européen



Rien ne change dans les principes,
tout change, dans la pratique

On retrouve dans le GDPR les mêmes chapitres que dans la loi I&L, hormis les formalités préalables



Copyright La Poste

De nouvelles obligations

De nouvelles obligations pour les Responsables de traitement et les Sous-traitants

Devoir de conseil
Co responsabilité

Accountability

- **Documentation / registres**
- Obligatoire pour sociétés >250 employés, traitements à risque, données sensibles, **traitements non occasionnels**
- **Preuve du respect du Règlement**

Analyses d'impact

- Évaluation des risques avant mise en œuvre : traitement, finalité, risques, mesures de protection
- Obligatoires pour données sensibles, profilage avec effets juridiques
- Liste des traitements concernés à préciser (Cnil)

Privacy by design & by default

- Protection dès la conception (pseudonymisation, minimisation)
- Protection par défaut : traitement et accès aux seules données nécessaires

DPO

- Nouveau CIL
- Interne ou externe
- Obligatoire pour administrations, données sensibles, activités qui impliquent un suivi régulier systématique et à grande échelle
- Conseillé pour toutes les entreprises
- Rôle : information, conseil, contrôle

Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

Une exigence de sécurité renforcée

- Des mesures pour **assurer la sécurité des données**
  - Des techniques favorisées : pseudonymisation et chiffrement
  - Un objectif réaffirmé : confidentialité, intégrité, disponibilité, résilience
  - Un objectif dans le temps : tests, analyses et évaluations régulières
  - Le plus : adhésion Code de conduite, certification

- **La notification des violations** de sécurité
  - Notification du responsable de traitement par le sous-traitant
  - Information de l'autorité de contrôle sous 72h, sauf en l'absence de risque pour les individus
  - En cas de risque élevé, information des personnes concernées dans les meilleurs délais, sauf mesures adaptées ou efforts disproportionnés

Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

Une exigence de sécurité renforcée

- La sécurité informatique repose sur des solutions techniques et organisationnelles :
  - Techniques
    - Sécurisation du parc machine, des logiciels et des flux
    - Traçage, historiques d'accès
    - Pseudonymisation et chiffrement des données
    - Niveaux d'accès et mots de passe
    - Pas de transfert de fichier en clair, envoi du fichier et du mot de passe par des canaux différents
  - Organisationnelles
    - Sensibilisation du personnel, audit, processus, mise en œuvre, suivi...
    - Mesures pour le respect de la confidentialité par le personnel (clauses dans les contrats de travail, charte d'entreprise...)
    - Choix du prestataire, contrôle de ses process physiques et logiques

Cf. Guide sécurité de la Cnil

Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

Le consentement et les autres fondements

- Définition : « manifestation de volonté libre, spécifique, éclairée [informed] et univoque [unambiguous] », « acte positif clair »
- Le consentement n'est pas requis pour la prospection en général
- La prospection est toujours reconnue comme intérêt légitime, fondement du traitement des données
- C'est la directive e-privacy qui impose un consentement pour l'emailing (hors produits analogues et hors BtoB en France) et un accord pour les cookies
- Pas de consentement requis pour les autres canaux du MD (postal, téléphone) → opt out

Régime de l'emailing
Révision directive e-Privacy

Prospection

Intérêt légitime

Consentement

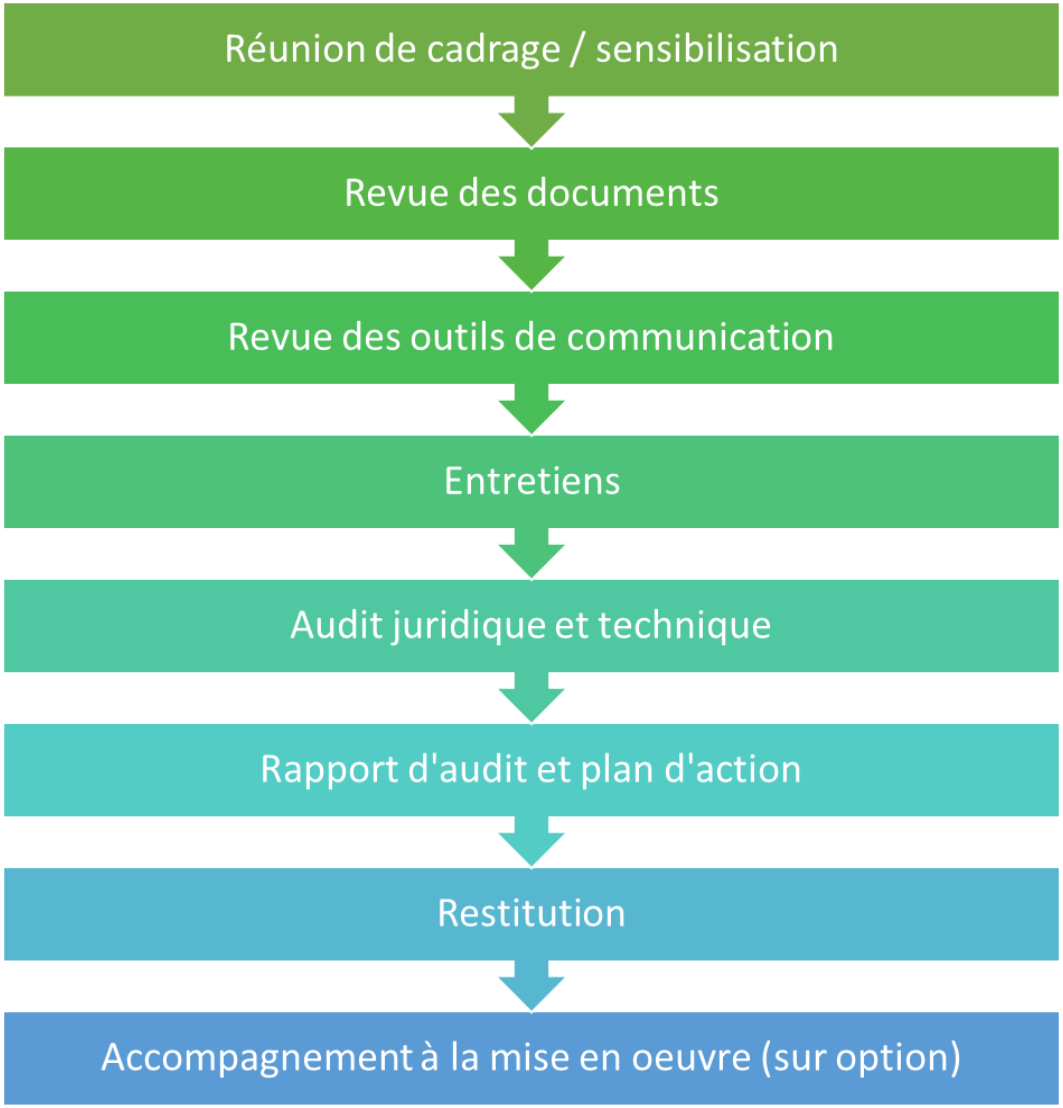
Accord

Bloctel

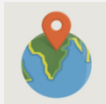
Robinson

Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

DEMARCHE


Réunion de cadrage / sensibilisation
Revue des documents
Revue des outils de communication
Entretiens
Audit juridique et technique
Rapport d'audit et plan d'action
Restitution
Accompagnement à la mise en oeuvre (sur option)

LOYAUTÉ ET TRANSPARENCE : Information des personnes

	Art 32 I LIL COLLECTE DIRECTE : Information au moment de la collecte	Art 13 RGPD COLLECTE DIRECTE: Information au moment de la collecte
	Identité du responsable du traitement et, le cas échéant, de celle de son représentant	L'identité et coordonnées du responsable de traitement **et le cas échéant du Data Protection Officer ou cas de collecte indirecte l'origine des données**
	La finalité poursuivie par le traitement auquel les données sont destinées	La finalité du traitement **(et les éventuelles finalités ultérieures)**
	Les destinataires ou catégories de destinataires des données	Les destinataires des données ou catégories de destinataires des données
	Du caractère obligatoire ou facultatif des réponses et les conséquences éventuelles, à son égard, d'un défaut de réponse	**Le caractère réglementaire ou contractuel du traitement et** les conséquences du refus de renseigner ses données
	Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne	**L'existence ou l'intention de réaliser un transfert hors UE**
	Les droits des personnes : accès, rectification, opposition et de définir des directives post-mortem	Les droits des personnes (accès, rectification, effacement, **limitation**, opposition, **portabilité et introduire une réclamation devant la CNIL**)
	Depuis octobre 2016, **la durée de conservation** ou les critères utilisés pour déterminer la durée	**La durée de conservation ou les critères utilisés pour la déterminer ou les critères utilisés pour déterminer cette durée**
	**Néant**	**La base juridique du traitement (tels que le consentement ou les intérêts légitimes du responsable)** NEW !
	**Néant**	**L'existence d'une prise de décision automatisée (profilage)** NEW !

brm

LOYAUTÉ ET TRANSPARENCE: Information des personnes

	Art 32 III LIL COLLECTE INDIRECTE : Information dès l'enregistrement des données ou lors de la première communication des données	Art 14 RGPD COLLECTE INDIRECTE: dans un délai d'un mois ou au moment de la première communication ou encore lorsqu'elles sont transmises pour la première fois
	Identité du responsable du traitement et, le cas échéant, de celle de son représentant	L'identité et coordonnées du responsable de traitement **et le cas échéant du Data Protection Officer ou cas de collecte indirecte l'origine des données**
	La finalité poursuivie par le traitement auquel les données sont destinées	La finalité du traitement **(et les éventuelles finalités ultérieures)**
	Les destinataires ou catégories de destinataires des données	Les destinataires des données ou catégories de destinataires des données
	Du caractère obligatoire ou facultatif des réponses et les conséquences éventuelles, à son égard, d'un défaut de réponse	**Le caractère réglementaire ou contractuel du traitement et** les conséquences du refus de renseigner ses données
	Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne	**L'existence ou l'intention de réaliser un transfert hors UE**
	Les droits des personnes : accès, rectification, opposition et de définir des directives post-mortem	Les droits des personnes (accès, rectification, effacement, **limitation**, opposition, **portabilité et introduire une réclamation devant la CNIL**)
	Depuis octobre 2016, **la durée de conservation** ou les critères utilisés pour déterminer la durée	**La durée de conservation ou les critères utilisés pour la déterminer ou les critères utilisés pour déterminer cette durée**
	**Néant**	**La base juridique du traitement (tels que le consentement ou les intérêts légitimes du responsable)** NEW !
	**Néant**	**L'existence d'une prise de décision automatisée (profilage)** NEW !
	**Néant**	**La source d'où proviennent les données** NEW !

LA SECURITE DANS LE RGPD : Art 32

Les débiteurs de l'obligation

- Le responsable de traitement
- Le responsable conjoint de traitement
- Le sous-traitant

Les mesures techniques et organisationnelles

- Obligation de protection des données dès la conception
- Obligation de protection des données par défaut

Les mesures destinées à mettre en œuvre les principes relatifs à la protection des données

- La pseudonymisation, le chiffrement, la minimisation
- La confidentialité, l'intégrité, la disponibilité, la résilience
- Les testes et évaluations régulières des mesures techniques et organisationnelles adoptées

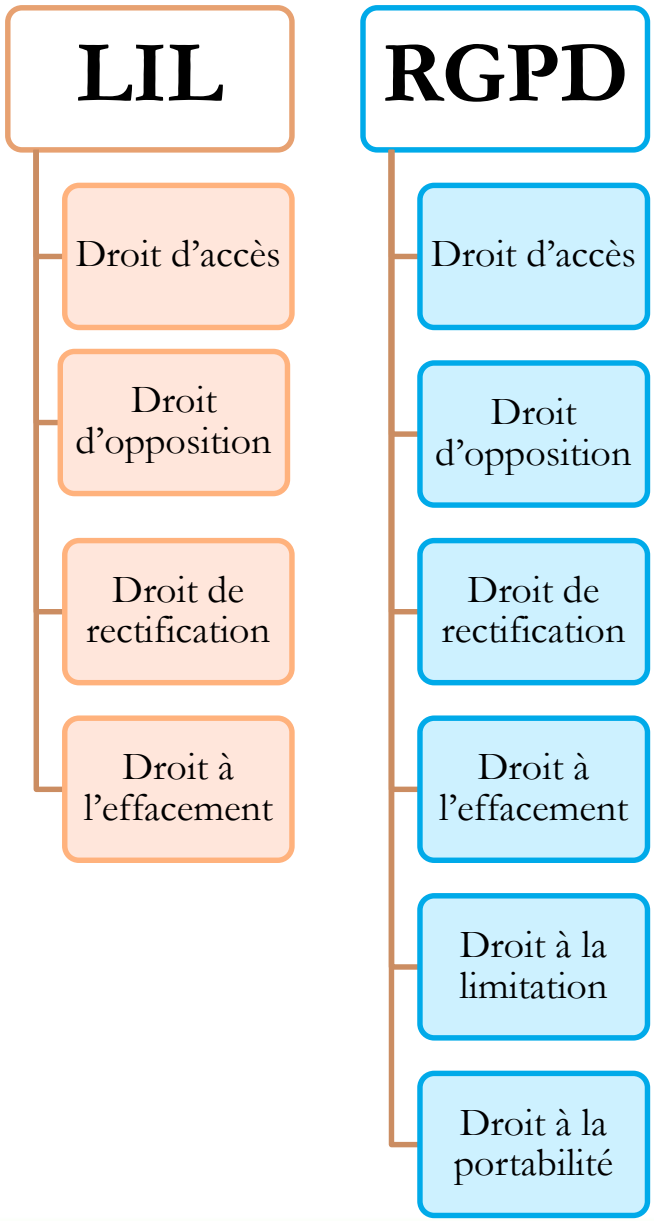
SECURITE ET CONFIDENTIALITE DES DONNEES

« *En cas d'atteinte à la confidentialité de données bancaires, la société ne saurait s'exonérer de sa responsabilité en se retranchant derrière des erreurs humaines* »
Délibération de la formation restreinte n° 2014-299 du 7 août 2014

Le support et les modalités de communication des informations aux tiers indiqués dans la déclaration sont-ils fixés ? (pas de fichier de données personnelles par mail)

Les contrats avec les prestataires obligent-ils ceux-ci aux règles de sécurité imposées par la loi Informatique & Libertés ?

DROIT DES PERSONNES



Accountability

Allègement apparent des formalités

- Formalités limitées auprès de la CNIL
- Mais nécessité de tenir un **registre des activités** de traitement pour les entreprises de plus de 250 salariés

Mais des obligations renforcées

- **Privacy by default & by design** : déployer des process permettant de tenir compte de la protection des données dès la conception et par défaut
- **Obligation de sécurité renforcée** pour les responsables de traitements et les sous-traitants
- **Notification obligatoire** des failles de sécurité (RT et ST)

Accountability : repenser l'organisation de la conformité

Cela suppose d'appliquer la règle des 4 P

Pilote(s) : Equipe conformité et DPO

Politique de protection des données

Process documentés

Preuves et traçabilité

Modification des relations donneur d'ordre/sous-traitant

Face à un sous-traitant

- **Vérifier les garanties concrètes** offertes par le ST en matière de protection des données
- Encadrer les relations avec le ST par le biais d'un **contrat écrit** comportant les exigences écrites
- Vérifier qu'il respecte les nouvelles obligations mises à sa charge

En tant que sous-traitant

- Respecter les nouvelles obligations à la charge du ST: **notification des violations, registre, DPO**
- Recruter uniquement des ST qui offrent **des garanties concrètes** quand à la protection des données
- Devoir d'alerte

A savoir : La violation de ces obligations pourra faire l'objet d'une amende administrative pouvant s'élever jusqu'à 2% du CA

Autorités de contrôle et sanctions

Les Cnil nationales

- Coopération renforcée entre les Cnil, One stop shop
- « European Data Protection Board »
- Transferts internationaux de données

Plaintes et sanctions

- Amende administrative jusqu'à 20 millions d'€ ou 4% du chiffre d'affaires annuel mondial (groupe)
- Droit à réparation de la personne qui a subi un dommage
- Actions de groupe possibles

Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

Anticiper sa mise en conformité

Adapter/initier sa politique de gouvernance des données

Désigner un pilote
CIL, DPO…

Prioriser

Réaliser des études d'impact

Former ses équipes
Penser certification, codes de conduite

Documenter la conformité
Registres, process, décisions…

Sensibiliser les directions (générale, informatique, juridique, marketing) et les équipes

Cartographier les traitements et données (données, finalités, durée conservation, flux, destinataires…)
Registres, approche par les risques

Mettre en place des process
Contrats RT/ST, mentions
Durées de conservation, archivage
Flux transfrontières
Gestion des droits des personnes
Sécurité : mesures techniques et organisationnelles, pseudonymisation, chiffrement
Gestion des violations de sécurité…

Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

Pour plus d'informations

Participez à la formation GDPR du Sncd

- Niveau initiation : vous avez connaissance succincte du GDPR et souhaitez améliorer sa compréhension
- Objectifs de la formation :
  - Comprendre les enjeux du GDPR et ses notions essentielles
  - Anticiper ses impacts sur votre métier et votre organisation
  - Vous adapter à vos nouvelles obligations
  - Mener les premières actions de mise en conformité
  - Comprendre le rôle du DPO
- Public concerné : vous gérez un CRM ou une base de données mutualisée, vous collectez des données sur internet (cookies, email, adresse postale…), vous hébergez des fichiers, vous utilisez des données pour réaliser les opérations de vos clients…
- Intervenante : Nathalie PHAN PLACE, Secrétaire Générale du Sncd et co-présidente de la commission Juridique & Déontologie
- Prochaine date : **1er février 2018 de 9h30 à 12h30 et de 14h à 18h**
- Pour plus d'informations, rendez-vous sur notre site rubrique « Formation GDPR »

Copyright Sncd - Reproduction interdite – Document à titre illustratif sans valeur juridique

Nous contacter

info@sncd.org
01 55 43 06 11

Merci !

Notre mission,
Nos valeurs

ENGAGÉS
RASSEMBLÉS
INNOVANTS

sncd
de la data à la logistique
syndicat national de la communication directe