Association Française des Fundraisers

Petit-déjeuner à Paris – 24 octobre 2017

Protection des données personnelles

se mettre en conformité avec le règlement européen, c'est maintenant

Adopté définitivement en avril 2016, le règlement européen relatif aux données personnelles sera directement applicable à compter du 25 mai 2018. Cela ne laisse plus que quelques mois aux organisations pour se mettre en conformité avec la nouvelle législation : nomination d'un délégué à la protection des données, reporting des traitements de données, protection des données dès la conception et par défaut, politique de sécurité renforcée… Tour d'horizon des nouveaux enjeux et de l'impact pratique pour la gestion et l'utilisation de votre base de données.

Nathalie Phan Place

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

Carine Vincent

Ediis 100% FUNDRAISING AID

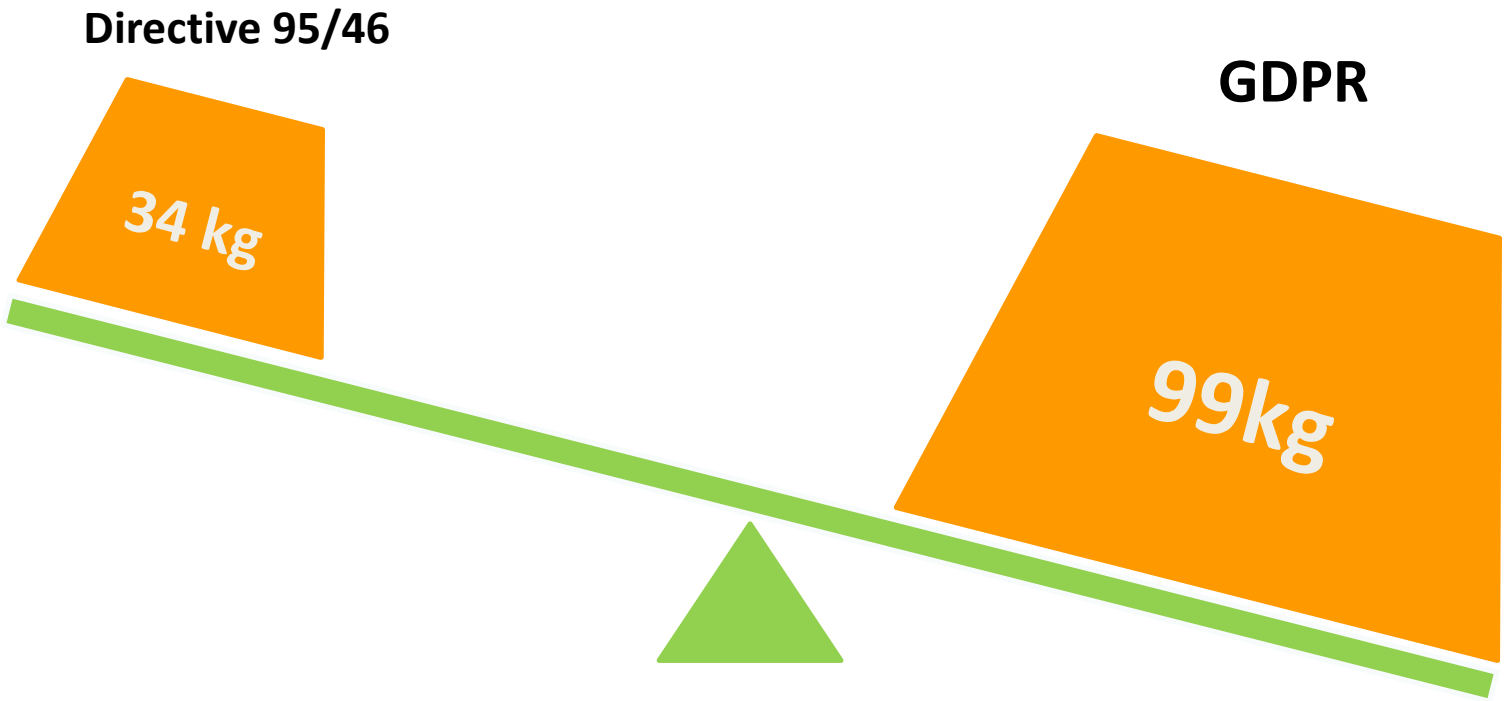
Présentation du Sncd

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**

- 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

GDPR
Les nouvelles règles de traitement des données

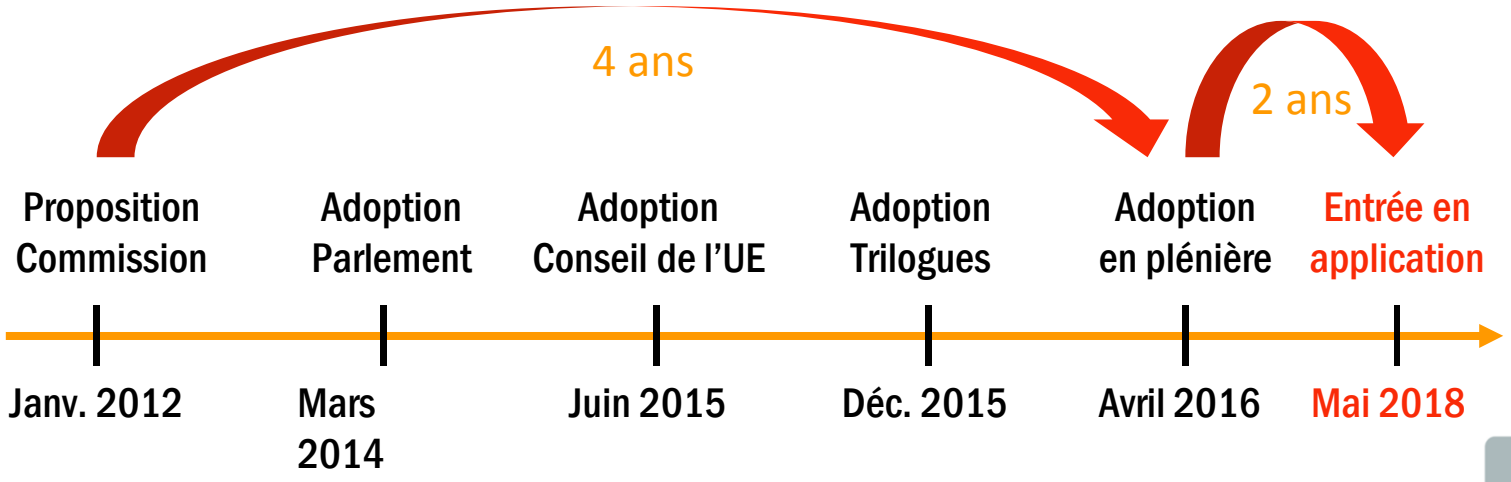
L’adoption du Règlement européen



	Données personnelles	Numérique
Aujourd'hui	**Directive 95/46/CE (protection des données personnelles)** Loi I&L	CPCE **Directive e-Privacy** 2002/58/CE **(prospection électronique)** 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

L'adoption du Règlement européen

Chronologie



2018

TODO :
25 mai 2018
Entrée en application

Les risques

Plaintes et sanctions

- Amende administrative jusqu'à 10 ou 20 millions d'€ ou 2 ou 4% du chiffre d'affaires annuel mondial (groupe)
- Droit à réparation de la personne qui a subi un dommage
- Actions de groupe possibles

Perte de confiance

- Doute, suspicion sur les procédures de confidentialité
- Doute sur les échanges de fichiers
- Réputation via les émissions d'investigation, la presse, le mauvais buzz…
- Comportement de collecte des données sensibles et désidérata des donateurs pris en compte

Pourquoi le GDPR est une opportunité pour vous ?

- Gage de confiance pour les donateurs
- Information de votre mise en conformité
- Harmonisation des pratiques entre les acteurs
- Compréhension de la circulation des flux et des impacts
- Maintien des procédures à jour (association et prestataire)
- Réappropriation du pilotage du traitement
- Rééquilibrage de la relation partenariale association / prestataire
- Responsabilisation …

Qu’est-ce qu’une donnée à caractère personnel ?

Toute information qui permet **d’identifier directement** ou **indirectement** une personne physique

*« toute information se rapportant à une **personne physique** identifiée ou identifiable [...] ; 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) »*

Qu'est-ce qu'une donnée à caractère personnel ?

2 types d'identification

BtoC et BtoB

- **Identification directe** : nom, prénom, photographie, image sur bande vidéo

Syndicat Sncd
Mme N Phan Place
68 BD SAINT MARCEL
75005 PARIS

- **Identification indirecte** : numéro de téléphone, numéro de CB, numéro de compte bancaire, empreinte digitale, cookie, adresse IP, etc.

C17VA38

Données particulières : les données sensibles

Les données à caractères personnel qui révèlent

- L'origine raciale ou ethnique
- Les opinions politiques
- Les convictions philosophiques ou religieuses
- L'appartenance syndicale
- Les données génétiques et les données biométriques d'identification
- Les données de santé
- Les données relatives à la vie ou l'orientation sexuelle

Traitement interdit

Données particulières : les données sensibles

Sauf

- Consentement explicite de la personne pour une finalité spécifique
- Traitement nécessaire aux intérêts vitaux d'une personne
- Traitement mis en œuvre par une fondation, une association ou tout organisme à but non lucratif à finalité politique, philosophique, religieuse ou syndicale, pour ses membres, anciens membres, contacts réguliers en liaison avec ses finalités
  Mais pas de communication vers des tiers sans consentement
- Données rendues publiques par la personne
- Traitement nécessaire à l'exercice d'un droit
- Traitement nécessaire pour des motifs d'intérêt public important ou dans le domaine de la santé publique
- Médecine préventive ou du travail, gestion des services de soin ou de protection sociale…
- Professionnel de santé soumis au secret médical

Et les données anonymes ?

- Une **donnée anonymisée**

  Une donnée transformée de manière irréversible pour tout acteur

  - Ne permet plus l'individualisation
  - Ne permet plus la corrélation (relier entre eux des ensembles de données distincts concernant un même individu)
  - Ne permet plus d'inférence (déduire de l'information sur un individu)

  → n'est pas une donnée personnelle, donc non soumise au GDPR

- Une **donnée pseudonymisée**

  Une donnée hashcodée, un identifiant…

  → est une donnée personnelle, donc soumise au GDPR

  → contribue aux process de sécurisation des données

Les acteurs concernés

- Le Règlement concerne :
  - Toute entreprise procédant au traitement de données à caractère personnel, quelle que soit sa taille et son activité principale
  - Le traitement manuel autant que le traitement informatisé (exemple : écriture manuscrite des mailings grands donateurs, traitement des dossiers de legs…)

- Ce qui vous concerne :
  - Aujourd'hui même sans formalités de déclaration (dispense DI-008 pour certaines données exonérées), toute la loi I&L s'applique aux associations (information, conservation, sécurité…)
  - Demain tout le GDPR s'appliquera également, y compris la tenue des registres

Cnil - Dispense DI-008

Associations : gestion des membres et donateurs

- La dispense de déclaration n° 8 (ancienne norme simplifiée n° 23) c… …s traitements de données personnelles mis en œuvre par tout organisme à but no… …iation loi 1901, fondations, fonds de dotation) **pour la gestion administrativ… …, bénévoles et donateurs.** Elle concerne également les annuaires des m… …ux diffusés sur internet ainsi que toute action de prospection réalisée auprès… …teurs.

- La dispense 8 prévoit que **seules peuvent êt… …données relatives à l'identité, l'identité bancaire, vie associative, et à… …s les données de connexion. Elle exclut les données sensibles** telles… …ales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'a… …e, l'état de santé ou la vie sexuelle des personnes, les infractions, co… …dure de justice, les informations sur les difficultés sociales et le numéro de …

- **Ces données ne… …vées au delà de la démission ou de la radiation du membre** (sauf s'il fait la… …**et pour les donateurs au delà de deux sollicitations restées infructue…** …s sur les prospects ne sont pas conservées après la réalisation de la camp… …**Les personnes concernées doivent être informées lors de la collecte de…** …opération visant à **diffuser** leurs données personnelles, ainsi que sur leur **droit d'op… …ccès et de rectification** et sur les modalités d'exercice de ces droits. Leur **conse…** doit être obtenu si l'association envisage de **céder ou louer leurs coordonnées à des fins de p…ospection commerciale par voie électronique** (e-mailing).

Disparition de cette dispense avec le GDPR

Les acteurs concernés

Exemples d'acteurs concernés :

- Toute **association** qui gère un fichier de donateurs, d'adhérents, de sympathisants, de prospects
- **Le gestionnaire de BDD** qui gère les dons et les données marketing
- Le **routeur** qui stocke une base de données en attendant l'envoi du prochain numéro d'un magazine papier,
- Le routeur qui effectue un traitement informatique de fichiers et/ou d'adresses
- Le **e-routeur**
- Le **personnalisateur** qui lasérise les adresses sur les porte-adresses
- Le **dédupliqueur** qui confronte les fichiers et livre le ou les lots
- Le **centre d'appel**
- **…**

Les acteurs concernés

Principalement 2 types d'acteurs :

- les **responsables de traitement** (les associations, fondations, etc.) :

  « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »

- les **sous-traitants** (ex. SSII, routeur…) :

  « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »
  Il n'agit que sur instruction de son responsable de traitement

Le contrat

Plus de transparence et plus de responsabilité pour les parties

A minima : objet/ durée/ finalité/ type de données traitées/catégorie de personnes concernées

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) [...].
La nature des opérations réalisées sur les données est […].
La ou les finalité(s) du traitement sont [...].
Les données à caractère personnel traitées sont […].
Les catégories de personnes concernées sont […].
Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes […].
Expl issu du site de la CNIL

\+

Instructions documentées du RT /Obligation de confidentialité au personnel du ST/ Politique de sécurité interne conforme au RGPD/ Politique suppression des données / Devoir d'alerte et d'assistance du ST/ Audit juridique et technique/ Responsabilité / Obligation d'assurer la sécurité

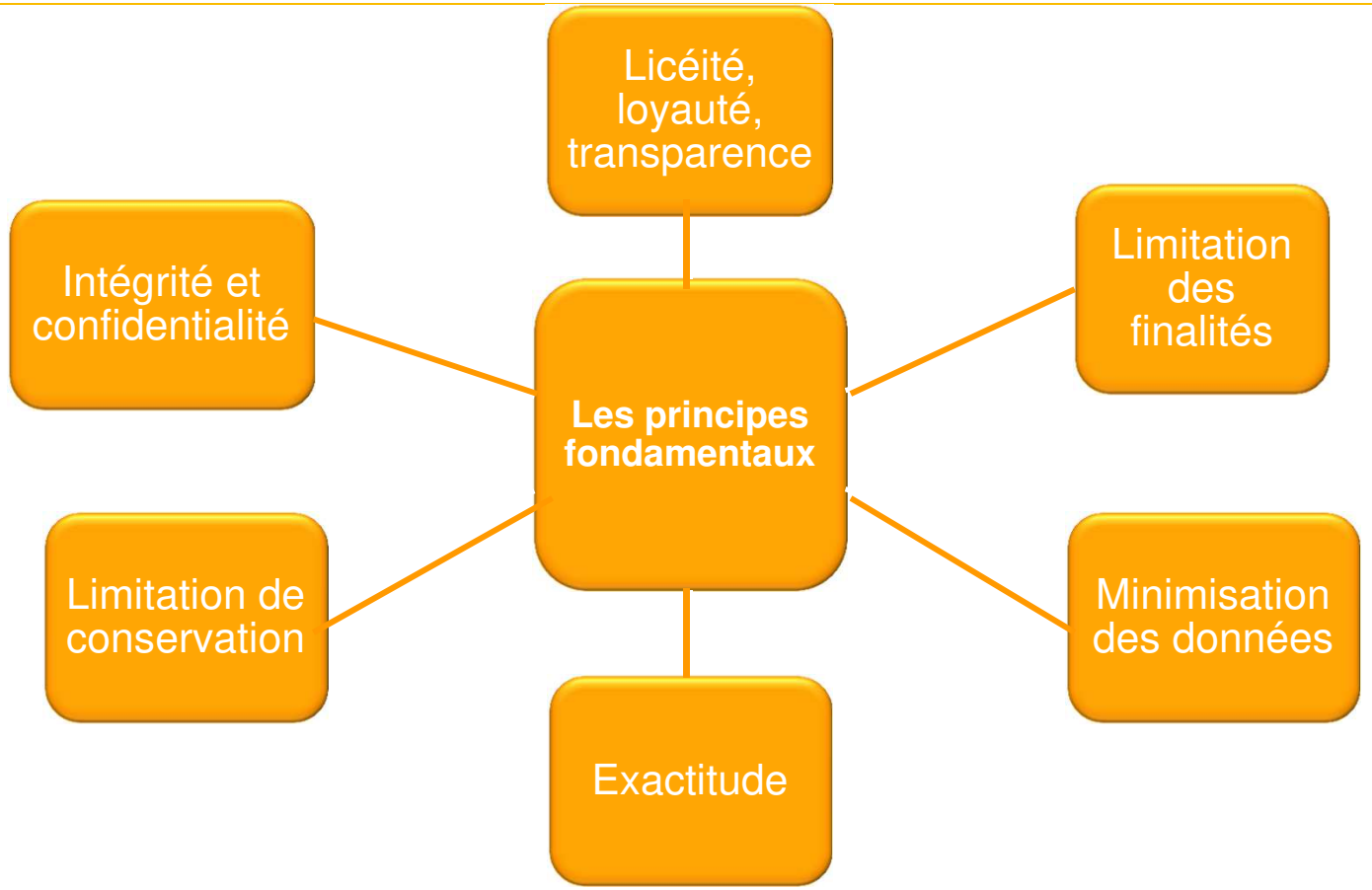
Le contrat

Des impacts concrets pour les deux parties

Le responsable de traitement s'engage à (extrait recommandation CNIL) :
Fournir au sous-traitant les données visées au II des présentes clauses
Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant
Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant

- Négociations plus dures mais éviter les bras de fers
- Co responsabilité 50/50
- Encadrement obligatoire de la sous traitance du sous traitant
- Points de vigilance off shore et hébergement
- Audit des écosystemes
- Impact si nouveau flux, nouvelle prestations,…

Les principes fondamentaux

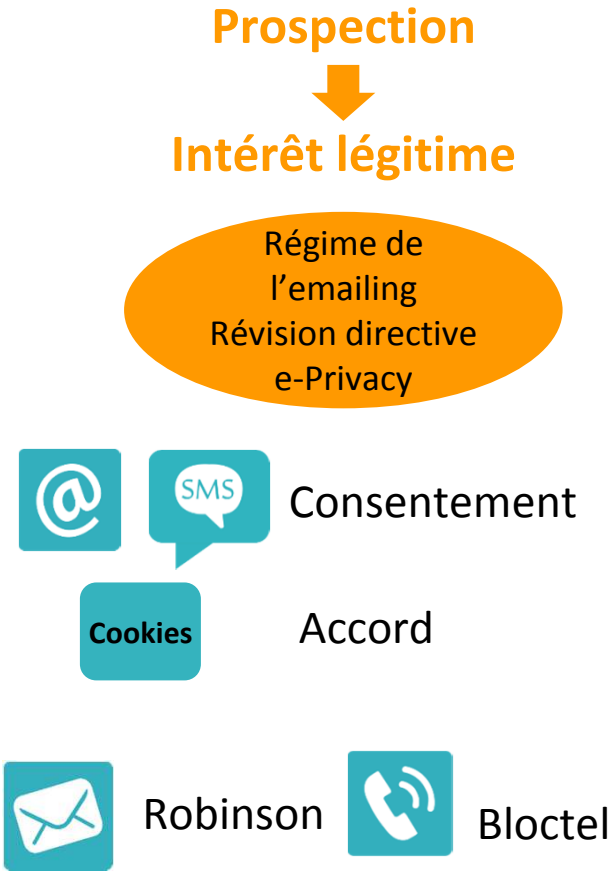


Le consentement et les autres fondements en MD

- Le consentement
  - Définition : « manifestation de volonté libre, spécifique, éclairée [informed] et univoque [unambiguous] », « acte positif clair »
  - Exit les cases pré-cochées et les consentements « forcés »
- La preuve du consentement
  - Le Responsable de traitement devra pouvoir prouver le consentement : date et heure, url…
  - Attente des guidelines européennes
- Le consentement n'est pas cessible
  - Attention à l'opt-in partenaire : pas de transfert en cascade

Le consentement et les autres fondements en MD

- 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



Zoom sur les cookies et autres traceurs

- Les cookies sont des informations stockées à la demande des serveurs web sur l'ordinateur de l'internaute, lors de sa navigation
- Ils sont aujourd'hui régis par l'art 32-II loi I&L, transposant la Directive européenne 2009/136/CE
- Tous les traceurs sont concernés :
  - Cookies utilisés pour la publicité ciblée
  - Boutons de partage de réseaux sociaux
  - Certains cookies de mesure d'audience
  - …
- Principe : information et accord préalable de l'internaute avant tout enregistrement

Zoom sur les cookies et autres traceurs

Information succincte par un bandeau cliquable	• **En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de** *[Cookies ou autres traceurs]* **pour vous proposer** *[Par exemple, des publicités ciblées adaptées à vos centres d'intérêts]* **et** *[Par exemple, réaliser des statistiques de visites]*. • **Pour en savoir plus et paramétrer les traceurs**
Information complète sur le site et offre d'opposition	• Information complète sur les cookies déposés, les finalités • Solutions pour s'opposer à la dépose de cookies
Poursuite de la navigation et absence d'opposition	• Dépose des cookies • Durée de conservation = 13 mois

Évolution attendue avec la révision de la Directive e-Privacy en cours

Droits des personnes

I&L	GDPR
Droit d'accès	Droit d'accès
Droit d'opposition	Droit d'opposition + Opposition au profilage
Droit de rectification	Droit de rectification
Droit à l'effacement	Droit à l'effacement
	Droit à la limitation
	Droit à la portabilité

Uniquement pour les traitements fondés sur le consentement ou sur un contrat
Fourniture des données dans un format standard

Une information renforcée des individus

- Identité du **responsable de traitement** (RT)
- **Finalités** du traitement
- **Destinataires** ou catégories
- Caractère **obligatoire ou facultatif** des réponses
- Existence des **droits d'accès et de rectification + d'opposition en marketing direct**
- Traitement **hors UE**

+

- Coordonnées du RT et du **DPO**
- **Base juridique** du traitement
- **Intérêts légitimes** poursuivis
- **Durée de conservation** (ou critères en cas d'impossibilité)
- Droit à **l'effacement**, à la **limitation de traitement**, à la **portabilité** des données
- Droit d'introduire une **réclamation** auprès d'une autorité de contrôle
- **Profilage** : l'existence d'une prise de décision auto, info sur la logique sous-jacente, conséquence pour la personne
- **Nouvelle finalité** du traitement ultérieur

- **Durée de conservation** (ou critères en cas d'impossibilité)

+

En cas de collecte indirecte (échange…) :

- **Source** des données (peut être général)

L'information doit être concise, transparente, compréhensible, aisément accessible, en termes clairs et simples…

De nouvelles obligations pour

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

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 données
  - 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
  - Notification du responsable de traitement par le sous-traitant

Cf. Guide sécurité de la Cnil

Une exigence de sécurité renforcée

La sécurité informatique repose sur des solutions techniques et organisationnelles

Techniques

- Sécurisation du parc machine, des logiciels, des flux et des sites de back up
- Traçage, historiques d'accès
- Pseudonymisation et chiffrement des données
- Niveaux d'accès (datas et batiment) 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 prestataires, contrôle de ses process physiques et logiques

Association Française des Fundraisers

Justifier/finalité des traitements

Premiers impacts sur vos datas

Collecte des données	Base de données	Exploitation des données
• Consentement • Garantie de collecte loyale des données • Vigilance / échanges • Transparence • …	• Où je stocke • Circulation des flux entrants/sortants • Minimisation des données sensibles • Gestion du droit à l'oubli = définir la durée de conservation + purge automatique	• Circulation des flux • Fidélisation et réactivation • Fichier de récup/dédup • Automatiser au maximum • …

simplifier, rationaliser la gestion de la donnée, éviter les redondances inutiles et supprimer/purger une partie des données.

Étendue géographique

Le Règlement concerne

- l'ensemble des entreprises implantées dans l'Espace Économique européen, quel que soit le lieu de traitement des données

- les entreprises qui ne sont pas implantées dans l'Union, dès lors qu'elles procèdent à un traitement de données lié à l'offre de biens ou de services (gratuits ou payants) à des personnes situées au sein de l'Union ou au suivi de leur comportement

Exemples

- Perso des mailings dans l'UE (pays de l'Est) ou hors UE (Asie)
- Appel tél dans l'UE (pays de l'Est) et hors UE (Afrique)

La responsabilité du choix du prestataire repose sur l'annonceur, qui doit prendre toutes les garanties nécessaires

Les transferts de données hors UE

Les transferts vers des pays tiers ne peuvent avoir lieu que si :

- La Commission a décidé que le pays assure un **niveau de protection adéquat** (règles en matière de protection des données, autorité de contrôle indépendante)

- Ou le responsable de traitement ou le sous-traitant a prévu des **garanties appropriées**
  - Règles d'entreprises contraignantes
  - Clauses types de protection approuvées par la Cnil ou la Commission
  - Code de conduite approuvé
  - Mécanisme de certification approuvé

Dans tous les cas, **les individus doivent disposer de droits opposables et de recours effectifs et doivent être informés de ce transfert**

- Ou par certaines dérogations particulières
  - Consentement de la personne, après information des risques liés
  - Exécution d'un contrat entre le RT et la personne ou dans son intérêt
  - Motifs importants d'intérêt public
  - Défense de droits en justice
  - Sauvegarde d'intérêts vitaux (et impossibilité de consentement)

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…

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
- Intervenante : Nathalie PHAN PLACE, Secrétaire Générale du Sncd et co-présidente de la commission Juridique & Déontologie, titulaire d'un Master 2 en droit des nouvelles technologies des Université Paris Sud et Panthéon-Sorbonne
- Prochaines dates : Jeudi 11 janvier 2018 et jeudi 1er février de 9h30 à 18h
- Pour plus d'informations, rendez-vous sur notre site rubrique « Formation GDPR »