LA CONSCIENCE NUMERIQUE

au service

de la

CONFIANCE NUMERIQUE

SOMMAIRE

I. RGPD : Notions clés

II. Les 8 règles d’or

III. Responsabilités des acteurs

IV. DPO et outils de conformité

Mais pour débuter…

QUIZZ de « mise en forme »

Selon vous,

1. Le RGPD, le DPO … c'est quoi ?

2. En France, la 1ère loi sur la protection des données date de … ?

3. Quelles nouveautés apporte le RGPD ?

4. Quelles sont les sanctions encourues ?

Préambule

L'évolution de la protection des données personnelles

L'évolution de la protection des données personnelles

Mai 2024 eIDAS 2.0

UNE IDENTITÉ NUMÉRIQUE

Juillet 2024 (RIA)

Demain

ePrivacy

SOUVERAINETÉ NUMÉRIQUE

E. SNOWDEN

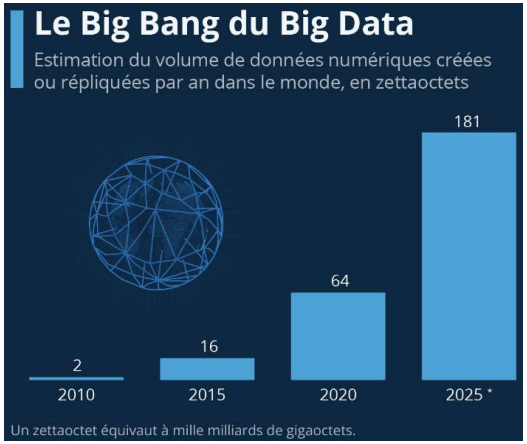
Le Monde 21 mars 1974

Safari ou la chasse aux Français *

1970 — 1974 — 1978 — **2013** — 2016 Adoption — 25/05/2018 Application

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

RGPD RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES



Loi 3V

- **Volume**
- **Variété**
- **Vitesse**

Chaque individu est devenu un générateur de données,

parfois même sans le savoir clairement

* Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus Le monde (cnil.fr)

I. RGPD: NOTIONS CLES

1. Traitement de données personnelles, quésaco ?

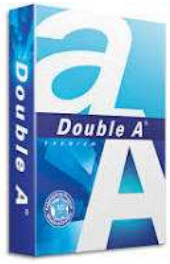
Toute opération effectuée à l'aide de procédés automatisés **ou non**, appliquée à des **données personnelles**

- Collecte
- Enregistrement
- Organisation
- Conservation
- Modification
- Extraction
- Consultation
- Transmission
- Diffusion
- Effacement
- Destruction…

2. Données personnelles, quésaco ?

I.2 Qu'est ce qu'une donnée personnelle ?
Définition

Où la trouve t-on ?



I.2 Qu'est ce qu'une donnée personnelle ?

Des exemples

C'est à vous !

Quelques exemples de données personnelles ?

Nom - Prénom	Numéro de SS (NIR)	Adresse IP
N° de téléphone	Identifiant de connexion	Situation professionnelle
Date de naissance	Adresse postale	Identité bancaire
Matricule d'un salarié	Photographie	Etat de santé

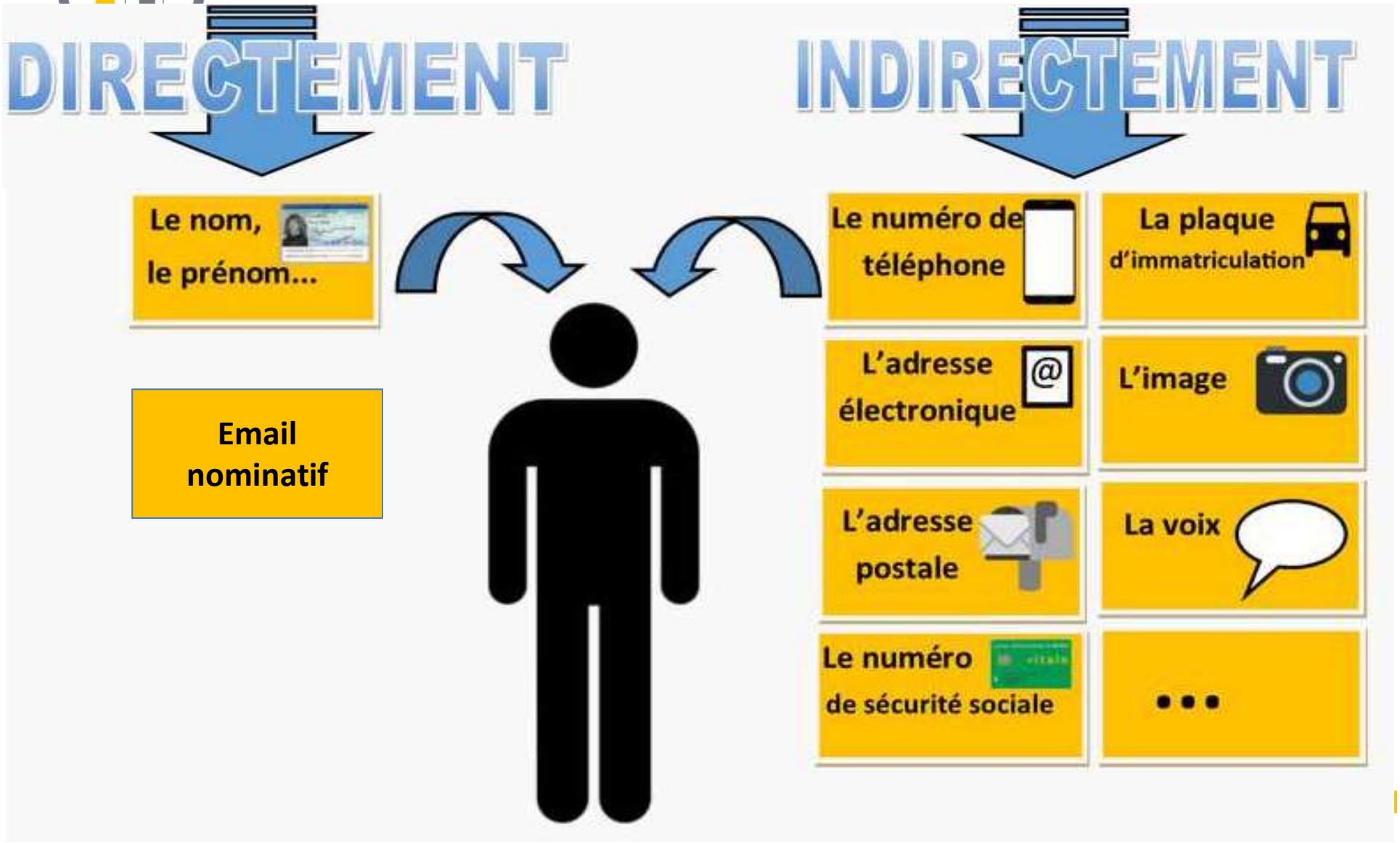
I.2 Qu'est ce qu'une donnée personnelle ?

Concernant une personne physique

candidat au recrutement

I.2 Qu'est ce qu'une donnée personnelle ?

Identifiée ou identifiable, directement ou non



3. A QUI S'APPLIQUE LE RGPD ?

I.3 A qui s'applique le RGPD ?

LES PERSONNES PHYSIQUES

(Sauf dans un cadre strictement personnel)

Toute personne physique et **tout** organisme **est concerné** par le RGPD dés lors :

qu'il est établi sur le territoire de l'UE*

ou

qu'il traite des données personnelles d'individus se trouvant sur le territoire de l'UE*

*UE = union européenne

4. Les acteurs : Responsable de traitement et sous-traitant

Les acteurs

Responsable de traitement

+

Co-responsable de traitement

Détermine (seul ou conjointement avec d'autres) les **finalités et les moyens** du traitement (le pourquoi et le comment du traitement).

C'est sur lui que pèse **la responsabilité** du respect des obligations

Ex : directeur général, gérant, président d'association, maire …

Sous-traitant

Traite des données personnelles **pour le compte et sur instruction documentée** du responsable de traitement

Ses obligations sont déterminées dans un contrat de sous-traitance, **obligatoirement** conclu

Ex : un prestataire réalisant une enquête (satisfaction, OPS, SLS …), un éditeur de logiciel Full Web …

Fin partie I

II. LES 8 REGLES D'OR

II. Les 8 règles d'or

- ✓ **Finalité** du traitement
- ✓ **Licéité*** du traitement
- ✓ **Minimisation** des données
- ✓ Protection des **données sensibles**
- ✓ **Conservation limitée** des données
- ✓ Obligation de **sécurité**
- ✓ **Transparence**
- ✓ **Droits** des personnes

* La base légale

1. LA FINALITE DU TRAITEMENT

C'est l'objectif poursuivi (pour quoi)

- Déterminée **avant** la mise en œuvre du traitement
- **Précise, compréhensible**, **claire**
- et **Légitime**

INTERDICTION de collecter et traiter des données à toutes fins utiles ou dans l'éventualité ou elles pourraient, un jour, peut-être, servir à quelque chose

PRINCIPE CLE

- DUREE DE CONSERVATION
- PERTINENCE DES DONNEES COLLECTEES
- LES PERSONNES HABILITEES A Y ACCEDER

2. LA LICEITE DU TRAITEMENT

6 BASES LEGALES

Interdiction

de traiter des données personnelles

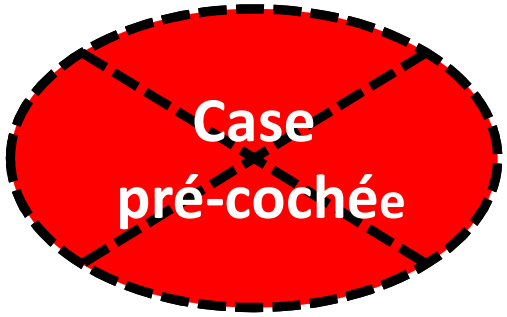
sans base légale

II.2 La licéité du traitement

LIBRE
et
SPECIFIQUE
et
ECLAIRE
et
UNIVOQUE
(acte positif clair)

- 15 ans

Preuve du consentement = notre responsabilité



Le traitement est nécessaire aux fins des intérêts légitimes poursuivis

La personne doit raisonnablement s'attendre à ce que ses données soient traitées

Le traitement est nécessaire à l'exécution d'un contrat signé par la personne concernée ou aux mesures précontractuelles prises à sa demande

Le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle nous sommes soumis

---

Le traitement est nécessaire à l'exécution d'une mission d'intérêt public.

Ex : le logement social est une mission d'intérêt public

Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne.

Ex : en cas de menace pour la vie de la personne en incapacité physique d'exprimer son consentement.

SELON LA BASE LEGALE,
LES DROITS DES PERSONNES* SONT DIFFERENTS

A DEFAUT DE BASE LEGALE,
AUCUN TRAITEMENT NE PEUT ETRE MIS EN OEUVRE

* Voir II.8 Les droits des personnes

3. LA MINIMISATION DES DONNEES

II.3 La minimisation des données

Que les données **strictement nécessaires** à l'objectif (collecte – conservation - transmission)

Les données doivent être :

- **Exactes et à jour**
- adéquates
- pertinentes
- proportionnées
- et limitées

Ex : la situation familiale d'un candidat à un emploi :
- ✓ n'est pas pertinente pour vérifier ses compétences (c'est un objectif)
- ✓ mais peut être justifiée pour l'attribution d'avantages sociaux (c'est un autre objectif)

LES QUESTIONS A SE POSER :

Quel est mon objectif ?

Quelles données sont indispensables pour l'atteindre ?

Ai-je le droit de collecter ces données ?

Ai-je bien distingué les données obligatoires des données facultatives ?

Besoin d'aide ?
Appelez le DPO

Zone bloc note et commentaire

Si la personne concernée regardait par-dessus mon épaule, Serais-je gêné ?

«échanges difficile», «ne pas se rendre seul à son domicile», **au lieu de** «locataire complètement dingue, alcoolique, drogué, violent»

«utiliser un vocabulaire simple», «parler fort et distinctement», «communiquer par écrit»… **à la place de** «débile léger», «sourd», «muet »

4. LES DONNEES SENSIBLES

PRINCIPE : tout traitement de **donnée sensible** est **INTERDIT** sauf consentement écrit

- Origine raciale ou ethnique
- Opinion politique
- Conviction philosophique ou religieuse
- Appartenance syndicale
- Santé physique/mentale
- Donnée biométrique
- Orientation ou vie sexuelle
- Donnée génétique

Mais aussi

- N.I.R. *
- Infraction pénale

* NIR : Numéro d'Inscription au Répertoire (= n° sécurité sociale)

Également à considérer comme hautement personnelles,
les données concernant :

Les revenus

Les difficultés sociales

Les personnes vulnérables (âgées, dépendantes, mineurs, salariés)

Pompiers, gendarmes, policiers et militaires

La géolocalisation

La vie familiale et privée

Les impayés, incidents et fraudes

Notation, scoring

Les moyens de paiement

5. LA CONSERVATION LIMITEE DES DONNEES

DROIT À L'OUBLI

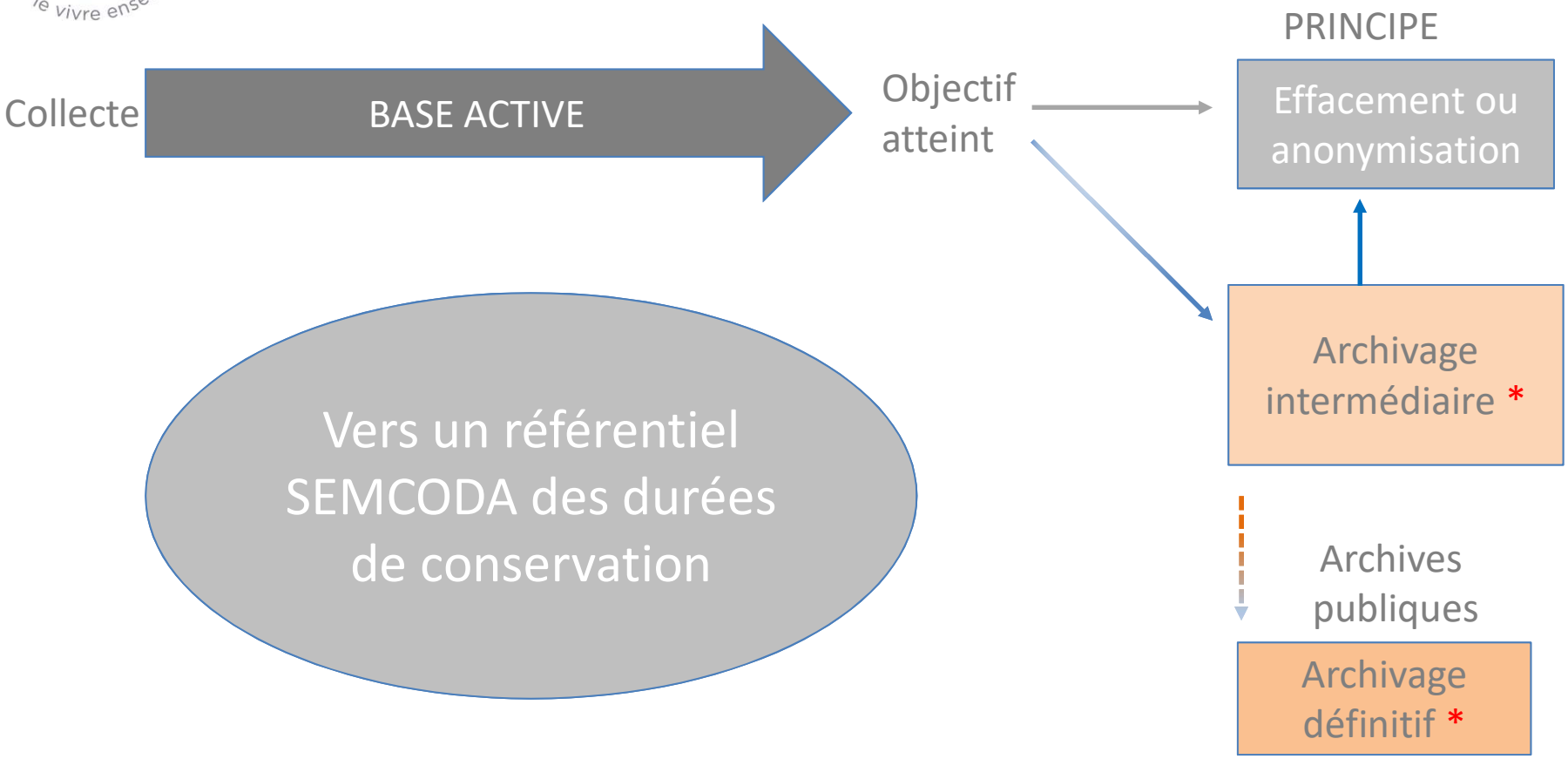
Une durée de conservation **limitée** et **cohérente** avec l'objectif poursuivi

Une **durée fixe** de conservation

Ou

un **critère objectif** utilisé pour la déterminer
(ex : le temps de la relation contractuelle)

CYCLE DE VIE DE LA DONNEE



* Phases non systématiques

II.5 La conservation limitée des données

La durée de conservation peut être fixée par :

Ex : Double bulletin salaire : 5 ans après remise au salarié
Données de facturation : 10 ans même si la personne n'est plus cliente

Ex : Images de vidéosurveillance : 1 mois
Données relatives aux prospects : 3 ans
CV : 2 ans par le service RH (sauf opposition)

LES QUESTIONS A SE POSER :

Jusqu'à quand ai-je besoin des données pour atteindre l'objectif ?

Suis-je soumis à une obligation légale de conservation des données ?

Si oui, pour combien de temps ?

Ai-je besoin des données pour me défendre en cas de contentieux ?

Dans quels délais des recours en justice peuvent-ils intervenir ?

Besoin d'aide ?
Appelez le DPO

6. L'OBLIGATION DE SECURITE

II.6 L'obligation de sécurité

Objectifs:

Protéger les personnes

Protéger le patrimoine informationnel, l'image et la réputation de la Semcoda

L'obligation s'applique au

UNE SECURITE ADAPTEE

A chaque traitement

En fonction du risque

ET DYNAMIQUE

Enjeu de sécuriser :

LA CONFIDENTIALITE
Les données ne sont accessibles qu'aux personnes autorisées

LA DISPONIBILITE
Les données sont en permanence accessibles aux personnes autorisées

L'INTEGRITE
Les données ne sont pas altérées ou modifiées

Une attention accrue en cas de **transfert de données hors de l'UE**

Source des

délibérée

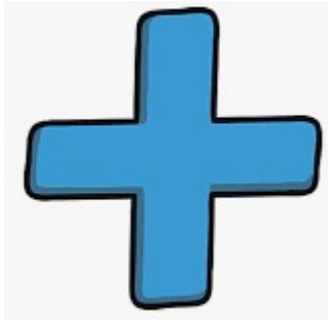
Accidentelle

externe

interne

Des mesures techniques :

MDP rigoureux, verrouillage des PC, contrôle de l'usage des ports USB, outil de transmission de données, traçabilité des accès, pare-feu et antivirus …



Des mesures organisationnelles :

Processus de transmission de données, contrôle d'accès aux données, chartes, sensibilisation du personnel, gestion des incidents, audits réguliers…

ET NOUS

7. TRANSPARENCE A L'EGARD DES PERSONNES

LOYALE & TRANSPARENTE

Une information **compréhensible**

accessible

dans un format **lisible**,

donne une **vision globale** du traitement

Lors de la collecte

Dés que possible et au plus tard à la 1ère communication

II.7 Transparence à l'égard des personnes concernées

CONTENU DE L'INFORMATION A DONNER

En plus :
- les catégories de données
- d'où elles proviennent

- Identité + coordonnées du RT*
- Finalité + base juridique
- Caractère obligatoire ou non
- Les destinataires des données
- La durée de conservation
- Ses droits sur les données traitées
- Son droit de saisir la CNIL
- Les coordonnées du DPO
- Le droit de retirer son consentement
- L'existence d'une prise de décision automatisée
- L'existence d'un transfert hors UE

Selon vous, chez Semcoda,
où retrouve t-on ces mentions d'informations ?

Dans les contrats de location,

Dans les avants contrats,

Dans les contrats de syndic,

En ligne sur internet …

Un modèle disponible auprès du DPO

* RT = responsable de traitement

8. LES DROITS DES PERSONNES CONCERNEES

II.8 Les droits des personnes concernées sur leurs données

DE **NOUVEAUX** DROITS

PORTABILITE

LIMITATION

MORT NUMERIQUE

30 jours pour répondre

DES DROITS EXISTANTS **RENFORCES**

ACCES

RECTIFICATION

EFFACEMENT

OPPOSITION ou RETRAIT DU CONSENTEMENT

2 Les 8 règles d'or

- **Les personnes sont au centre du dispositif : leurs données leur appartiennent**
  - Je délivre une information transparente aux personnes concernées
- **Chaque traitement à une finalité et une base juridique**
  - A défaut d'une autre base juridique, je demande un consentement
- **Je minimise les données collectées, conservées, transmises en fonction de mon objectif**
  - Je porte une attention particulière aux données sensibles ou hautement personnelles
- **Je favorise l'exercice des droits des personnes en associant le DPO**

CAS PRATIQUE

Monsieur R. Gépédé dépose à l'accueil de la Semcoda son formulaire papier de demande de logement social. Vous le parcourez pour vérifier que toutes les zones sont correctement renseignées.

A ce stade, avez-vous traité des données à caractère personnel (DCP) ? **OUI** ~~NON~~

Monsieur R. Gépédé vous remet également la copie de son titre de séjour, de sa carte vitale et ses 6 derniers bulletins de salaire.

Quelle(s) catégorie(s) de DCP ces documents contiennent-ils ? Courantes (nom…)

hautement personnelles (revenus…)

Sensibles (NIR, origine)

Pouvez-vous prendre ces documents ?

Titre de séjour ~~Carte vitale~~ ~~Bulletin de salaire~~

CAS PRATIQUE (suite)

Que faites vous si … ?

1. La police vous demande de lui transmettre les noms, adresse email, n° de téléphone de tous les occupants d'un immeuble

2. Un locataire vous demande d'accéder à ses informations et à celles de sa concubine

3. Une personne vous appelle afin de connaître le montant de son impayé et l'état de la procédure contentieuse

4. La mairie de Bourg en Bresse vous demande de lui transmettre tous les mois la liste des locataires entrants sur le territoire de l'agglomération.

5. Une assistante sociale vous demande la quittance de loyer de M. R. Gépédé qu'elle accompagne.

6. Un de vos interlocuteurs habituels vous signale qu'il a reçu un email suspect de votre part

III. RESPONSABILITES DES ACTEURS

1. LE PRINCIPE DE RESPONSABILITE

Avant mai 2018 : Adhésion à une norme

Depuis mai 2018

chaque acteur est RESPONSABLE de

- Protection **dés la conception**
- Détermination des données nécessaires
- Définition des durées de conservation
- Droits des personnes
- Contrats avec les sous-traitants
- Devoir d'information
- Preuve des consentements

Et doit en RENDRE COMPTE

- Registre des traitements
- Registre des violations
- AIPD *
- Politique et charte de protection des données
- Procédure d'exercice des droits

Une documentation régulièrement réexaminée et actualisée

* AIPD = Analyse d'Impact sur la Protection des Données

2. QUI PORTE LA RESPONSABILITE?

III. 2 Qui porte la responsabilité ?

Responsable de traitement

Co-responsable de traitement

Responsabilité conjointe

Sous-traitant

Responsabilité spécifique

Offre des garanties suffisantes en terme de sécurité technique et organisationnelle

Et à la SEMCODA ?

Son Directeur Général

et

Directeurs généraux délégués

(CNIL –TRIBUNAUX – PERSONNES CONCERNEES)

et ses salariés

vis-à-vis de la Direction, en cas de négligence ou malveillance

3. LES SANCTIONS

Ces sanctions peuvent être cumulées

Amendes administratives * :

10 à 20 Millions d'euros

ou 2 à 4% du CA

+

Jusqu'à 30 M€ ou 6% CA

Sanctions pénales ** :

300 000 € d'amendes

+ 5 ans de prison

1 500 000 €

(X 5 si personne morale)

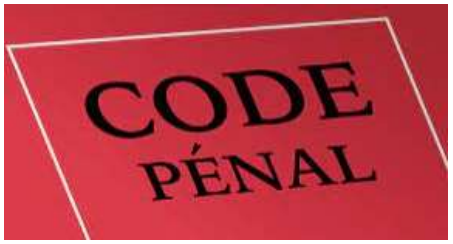
+

Publicité

de la décision de sanction

* Rgpd, art.83

** Art. 226-16 et suivants du code pénal



Quelques articles

Art.226-21
Non-respect de la délimitation des usages (détournement de finalité)

Art. 226-20
Non respect de la durée de conservation

Art. 226-22
Fait de porter, sans autorisation de l'intéressé, des données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir

Art. 226-17-1
Fait de ne pas procéder à la notification d'une violation

Art. 226-18-1
Poursuite d'un traitement malgré l'opposition de la personne concernée

** art. 83-5 Rgpd

4. LES CONTRÔLES DE LA CNIL

LES TYPES DE CONTROLE

la **CNIL** peut auditionner **tout collaborateur** de son choix

+ accès à tous locaux

Entrave action CNIL : 1 an de prison et **15 000 €** d'amende

X 5 si personne morale

Depuis 2022
Procédure simplifiée

→ Accélérer les procédures de sanctions

ACTIVITE CNIL 2023

- **16 433** plaintes reçues
- **20 800** demandes d'exercice de droits
- **4700** notifications de violations de données

Le 25 mai 2024

Le RGPD a 6 ans

Depuis 2018

+ 70% de plaintes reçues par la CNIL

350 contrôles/an opérés par la CNIL

214 106 000 €
En 2021

2018 -> 2023 :

600 millions d'euros d'amendes infligées par la CNIL

Quelques exemples de sanctions prononcées par la CNIL

CNIL 24 juillet 2018 : **sanction de 30.000 € et décision rendue publique** suite à l'envoi par un **bailleur social** d'un courrier à ses locataires critiquant la décision du gouvernement de diminuer le montant des aides personnalisées au logement (APL)- **Utilisation abusive du fichier des locataires à des fins politiques**

Evitons ensemble que la **SEMCODA** apparaisse dans cette liste

Cnil décembre 2020 : **Sanction de 7300 €** à l'encontre d'une **TPE de 2 salariés** pour
- défaut de consentement pour l'envoi d'emails de prospection commerciale
- Manquement à la minimisation des données, à la durée de conservation ….

CNIL novembre 2020 : **sanction de 2 250 000 € et décision rendue publique** à l'encontre d'une **société de grande distribution** pour
- Manquement à son obligation d'information
- Non respect des durées de conservation des données
- Manquement au respect des droits des personnes

IV.
LES OUTILS DE LA CONFORMITE

1. LE REGISTRE DES TRAITEMENTS

IV. 1 Le registre des traitements

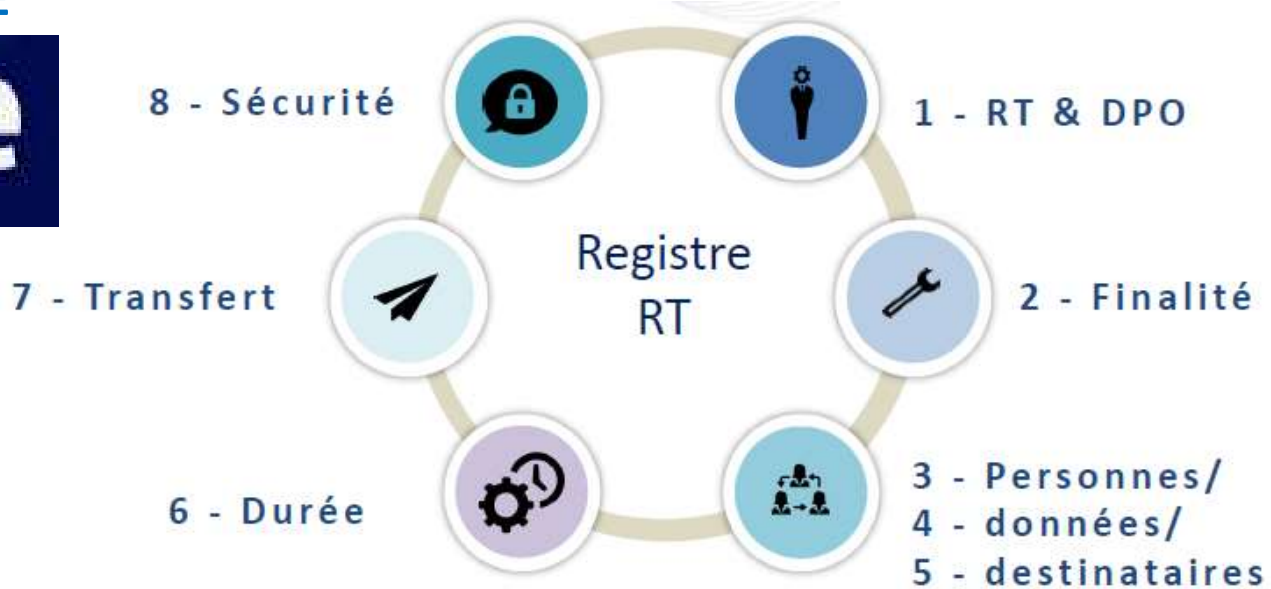
Si contrôle

CNIL.

UN OUTIL DYNAMIQUE

update

Il contient



2. L'AIPD (ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES)

IV.2 : L'AIPD

*Obligatoire si **risque élevé** pour les droits et libertés des personnes*

Effectuée **avant** la mise en œuvre du traitement

AIPD non requise : une liste de 12 traitements

Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse n'est pas requise | CNIL

AIPD OBLIGATOIRE : Une liste de 14 traitements

Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse est requise | CNIL

Traitements RH établissant des profils de personnes physiques

Gestion des alertes et des signalements en matière professionnelle

Instruction des demandes et gestion des logements sociaux

Accompagnement social ou médico-social des personnes

Traitements RH dans une entreprise de - 250 personnes

Traitements de gestion de la relation fournisseurs

Traitements aux seules fins des contrôles d'accès physiques et des horaires pour le calcul du temps de travail (sauf dispositif biométrique)

9 critères du CEPD (comité européen de la protection des données)

1. *Évaluation/scoring (y compris le profilage)*
2. *Décision automatique avec effet légal ou similaire*
3. *Surveillance systématique*
4. *Données sensibles ou hautement personnellles (santé, géolocalisation, etc.)*
5. *Collecte à large échelle*
6. *Croisement de données*
7. *Personnes vulnérables (patients, personnes âgées, enfants, etc.)*
8. *Usage innovant (utilisation d'une nouvelle technologie)*
9. *Exclusion du bénéfice d'un droit/contrat*

3. NOTIFICATION DES VIOLATIONS DE DONNEES

Notification des violations de données

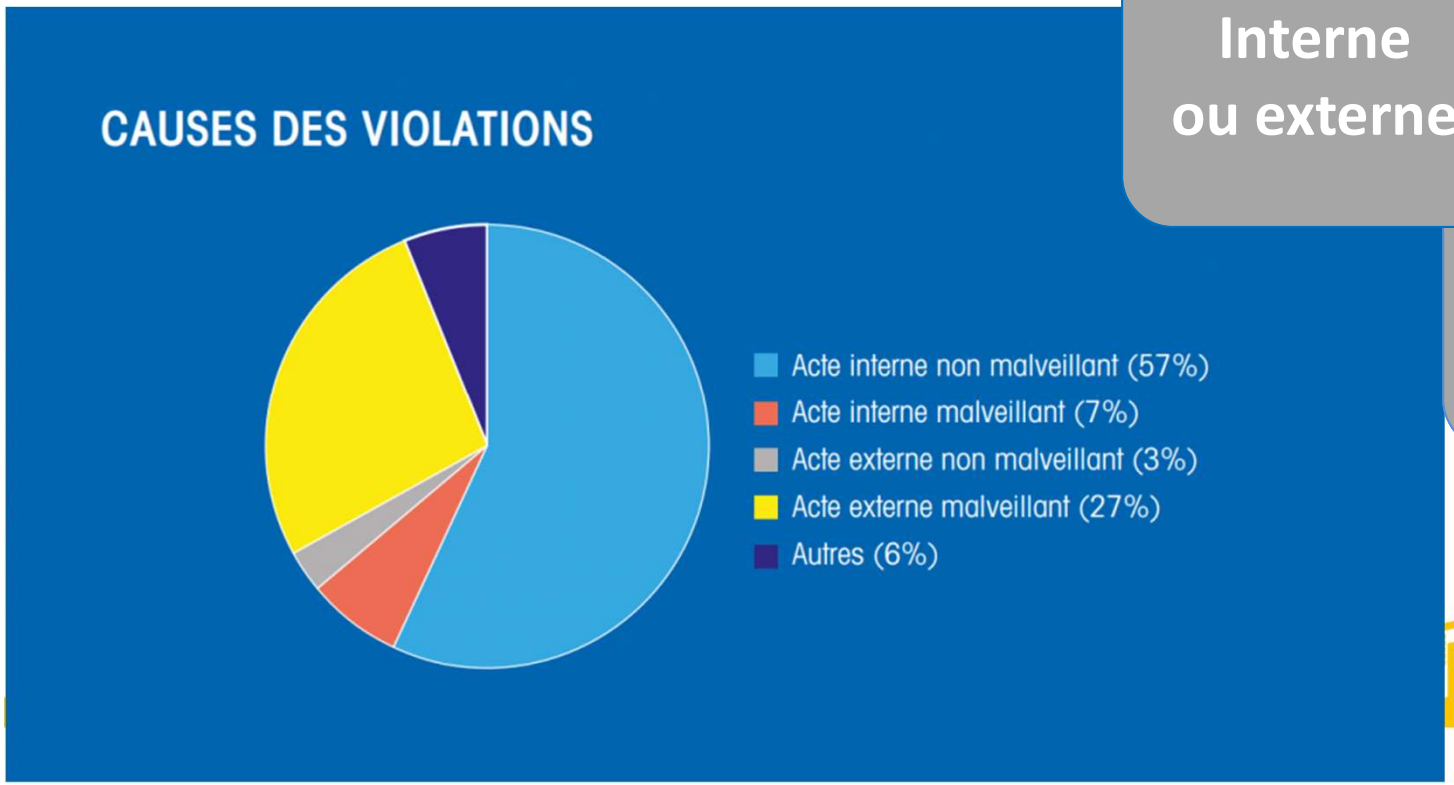
IV.3 La notification des violations de données

Une violation = une perte

- de **DISPONIBILITE** (disparition des données)
- de **CONFIDENTIALITE** (accès illégitime)
- d'**INTEGRITE** (modification non désirée)

Elle peut être **d'origine**

- **Interne ou externe**
- **Accidentelle ou illicite**



Quelques exemples de violation de données

Vol ou perte d'un PC, tablette, téléphone stockant des données personnelles

Données personnelles envoyées par courrier ou courriel par erreur

Fichiers papier (contenant des données sensibles) volés ou perdus

Transmission de données à un tiers non autorisé

Ransomware avec ou sans sauvegarde, avec ou sans exfiltration

Exfiltration de données d'entreprise par un salarié ou ancien salarié

En pratique

72H pour agir

AVERTISSEZ SANS DELAI LE DPO

4. LE DPO

Déléguée à la protection des données

SES MISSIONS

Informe et conseille

- Délivre des recommandations
- Sensibilise et forme
- Participe à l'élaboration des règles internes
- Est associé le + en amont à tout nouveau projet

Contrôle la conformité

- Participe au registre des traitements
- Effectue des audits
- S'assure du respect des règles

Conseils sur les AIPD

Rôle d'interface

CNIL, Personnes, interne

QUAND ?

- Au démarrage d'un nouveau projet
- Lorsque quelqu'un vous demande des données sur nos clients, nos locataires, sur nos collègues…
- Si vous apprenez que des données personnelles ont fuité
- Quand un traitement évolue
- Et plus largement en cas de question concernant la protection des données personnelles

Contacter le DPO

COMMENT ?

En externe : dpo@semcoda.com ou par courrier (Aubry)

En interne : mthomas.dimier@semcoda.com ou 04.74.50.98.51

Chaque salarié est acteur de la conformité

MERCI DE VOTRE ATTENTION