Droit de la protection des données personnelles.

Cours Magistral de 12h de Mr NETTER Emmanuel.
https://frama.link/RGPDS1 → visuel du cours

Examen :

Bibliographie :
A. Bensoussan et al., La protection des données personnelles de A à Z, Bruylant, 2017
C. Castets-Renard et al., Protection des données personnelles. Se mettre en conformité d'ici le 25 mai 2018, éditions législatives, 2017
A. Debet, J. Massot, N. Metallinos et al., Informatique et libertés : la protection des données à caractère personnel en droit français et européen, Lextenso, 2015
Martial et J. Rochfeld (dir.), Les spécificités du droit français au regard du RGPD, Dalloz, 2019
T. Douville, Le nouveau droit des données personnelles, Gualino, 2020

MOOC CNIL à faire à la fin du cours : https://atelier-rgpd.cnil.fr/apprenant/default.php
MOOC ANSII à faire à la fin du cours : https://secnumacademie.gouv.fr/
→ *délivrent des attestations pouvant être mise sur le CV.*

Plan du cours :

INTRODUCTION

Données personnelles : sujet nouveau très important.
La q° a surgit en France dans années 70
Loi informatique et liberté du 6 janvier 1978 est un véritable tournant dans la matière.
RGPD contient des articles et des considérant venant préciser l'article.

Cette matière intéresse, grâce notamment à E. Snowden qui a dénoncé les pg de surveillances de la NSA, il a amené tout le monde à prendre conscience de l'existence et de l'importance des données personnelles.

→ petit historique :
70's : début de l'informatisation.
Mise en place du projet « secret » SAFARI : le gouvernement veut rassembler toutes les données admin des français dans un même fichier pour faciliter les échanges entre administration.
Le projet est révélé au grand jour par un journaliste.
A la suite de cette révélation, le gvrnt décide de la mise en place d'une commission indépendante de réflexion qui va proposer un projet de loi.
Loi qui deviendra la loi « Informatique et libertés » en 1978 et qui va créer la CNIL chargée de faire respecter cette loi.

La CNIL est la 1ere AAI (Autorité Admin indépendante). Au départ, pas de pw de sanction, elle avait un simple pw de conseil.

L'Europe a ensuite pris le relais :
Directive 1995, transposé en 2004 : La CNIL se voit doter d'un véritable de pw de sanction (mais ces moyens restent aujourd'hui insuffisant).
RGPD adopté en 2016, entré en application le 25 mai 2018, à cette occasion on a re-modifié la loi Informatique et libertés.

Le RGPD est un règlement, pas une directive, il y a donc des zones d'ombre. Il faut donc le compléter avec la loi « Informatique et libertés ».

Que sont les données à caractère personnel ?

Art 4 RGPD donne la définition.
« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; 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 »

Est ce que l'information dont je dispose va me permettre d'identifier une personne précise ? Si oui, alors cette information est une donnée à caractère personnel.
Ex : les données qui correspondent à l'état civil (nom, prénom, adresse, nationalité, informations biométrique (ce qui nous distingue des autres, caractères physiques), réseaux veineux de la main, empreintes digitales, ADN, géolocalisation, adresse IP).

Art 4, 1 considérant 26 :
Avec ce considérant, le caractère de donnée personnelle est très rapidement attribué à une information.
Comment faire pour sortir de cette qualification de données personnelles ?

- La pseudonimisation ne suffit pas, donc le RGPD est tjrs applicable.

(ex : clinique change le nom de ses patients par des numéro/lettres, mais si le patient est tj identifiable , alors tjrs donnée personnelle).
Si anonyme, c'est à dire impossible d'identifier une personne précisément, alors pas de caractère personnel, donc on sort du RGPD.

- Pour appliquer le RGPD, il faut un traitement des données à caractère personnel.

La CNIL dit que consultation vaut traitement.
Souvent chaque opé sur une données est considérée comme une traitement.
→ Exception de traitement domestique : un traitement qui reste à la maison, qui n'a pas de conséquence pour le monde extérieur. Alors RGPD ne s'applique pas.
Ex : liste de personne qu'on invite à notre anniversaire. Traitement de données à caractère personnel ? Oui, mais traitement domestique, donc pas d'application du RGPD puisque personne d'autres ne peut la consulter.
Ex : CJUE, 10 juillet 2018, témoins de Jéhovah : porte à porte, ils notaient les noms,adresse, convictions religieuses. Témoins Jéhovah dit simple traitement domestique. CJUE répond que non, donc RGPD
Ex : Face ID. Compare l'image de la caméra à un « template »/image stockée dans le téléphone. RGPD ? Non, car traitement domestique puisque l'image template est stockée dans le téléphone seulement, sur une puce à l'intérieur, donc pas de consultation par d'autres personnes.

Lire article New York Times, septembre 2019 enquête géolocalisation
https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Https://twitter.com/loopsidernews/status/979640744926437376

G29 : regroupement de toutes les autorités de protection de l'UE, devenu le CEPD dans le RGPD
Il a un rôle d'harmonisation.

CHAPITRE 1 : Principes généraux du RGPD

- Art 5 RGPD : C'est le texte majeur du RGPD, tous les gds principes qui s'y trouvent irriguent tout le reste du RGDP. On pourrait quasi dire que le RGPD pour être seulement l'article 5.
  On peut tirer des gds pcpes de cet article relatifs au traitement.

A. Les principes de licéité, transparence, et loyauté.

Licéité : on ne peut pas traiter des données a caractère personnel si on a pas de fondement pour le faire.
L'art 6 contient une liste limitative de ces fondements. Le principal fondement est le consentement
La transparence : est l'idée que lorsqu'on traite ce genre de données, les individus concernés doivent être au courant que l'on traite leurs données, y compris quand on ne s'est pas fondé sur leur consentement.
Comment s'opposer au traitement des données ou demander le retrait des données si on ne sait pas que nos données sont collectées.
Loyauté : terme insaisissable/flou pour le moment. Le détournement de finalité / rapt déloyal, mais il existe aussi des pb de loyauté dans l'exploitation des données. La CNIL estime que dans la matière dont est mis en œuvre des algo, il faut respecter le pcpe de loyauté, les critères de l'algo ne doivent pas entré trop frontalement contre certains gds intérêts collectifs.
ex : au stade de la collecte : un internaute avait aspiré des données publiquement accessible, et les avait détourné de la finalité pour lesquelles elles avaient été mise en ligne.

B. Limitation des finalités.

En matière de RGPD on raisonne finalité par finalité.
On regarde tj en début le but du traitement, qu'est ce que ce traitement permet.
Une fois la finalité trouvée, il faut regarder si la finalité n'est pas détournée.
Un détournement de finalité est puni pénalement : Art 226-1 CP : 5 ans prison +300000e d'amende
Exemple 1 : Laurent Wauquiez a envoyé un SMS à tous les lycéens de la région Auvergne Rhône Alpes pour leur souhaiter bonne rentrée. Il a utilisé une base de données regroupant les numéros de portable. Alors que les lycéens avaient donné leur numéro au réseau de transport pour être averti en cas de panne/pb dans leur transport scolaire. Donc le fichier a été utilisé pour autre chose que prévenir les lycéens de panne. Wauquiez dit que c'est le président de la région qui gère les transports scolaires. La CNIL n'a pas donné de suite.
Exemple 2 : Facebook demande le numéro de portable pour double facteur d'authentification. Mais Facebook revendait les numéros de téléphone → détournement de finalité
Ex : sct d'assurance chargé d'assurer une mission de SP visant à verser des compléments de revenus aux retraités. Les sct d'assurance utilise ces adresses/info pour faire de la pub pour ses produits.

C. Le principe de minimisation.

Le but est le devoir d'utiliser les procédés les moins intrusifs, et à l'intérieur de ces procédés être le

plus sobre possible, ne demander que les infos strictement nécessaire.
On garde à l'esprit que notre traitement à une finalité.
On ne stock, traite, manipule que le minimum d'info nécessaire à la finalité et que si ces données ont un sens/utiles.
Si le minimum nécessaire alors pas de condamnation.
Ex : N'est pas sobre une appli de réseau social qui en 3 mois a accédé 150000 fois à la localisation, soit toutes les minutes jour et nuit.
Ce principe est très puissant, il permet beaucoup de chose.
Ex : La CNIL a réussi à mettre fin à une expérience : la mise en place de la reconnaissance faciale à l'entrée de 2 lycées impulsée par le président de la région PACA. La finalité de ce traitement c'est empêcher des personnes étrangères au lycée de rentrer. La CNIL dit qu'il existe d'autres façon moins liberticide, peu importe le coût que cela peut engendrer, et oblige à stopper cette expérience.

D. Le principe d'exactitude.

Il faut que les données personnelles soient des données qui reflètent la vérité, il ne faut pas de données erronées.
Une préoccupation importante de cette manière est donc de manier des données exactes.

E. La conservation limitée.

Pcpe important en pratique, qu'on peut voir comme un corollaire du pcpe de minimisation.
Quand on n'a pas besoin de conserver les données pour atteindre notre finalité, alors on doit arrêter le traitement et supprimer ces données.
Les services admin sont obligés de prévoir un temps de conservation.
(ex : image de vidéo surveillance dans une etp : max 1 mois)
Ex : Affr Cdiscount et Spartoo : ces etp avaient gardés trop de données trop longtemps : conservation des données de CB sans consentement durant 30 ans pour Cdiscount
Aff Spartoo : CNIL reproche beaucoup de chose : manqunt au pcpe de minimisation : enregistrement intégral et permanent reçus par les salariés du service client. Spartoo dit c'est pour former les salariés. CNIL dit qu'il y a seulement besoin d'un enregistrement par semaine pour former, Spartoo gardait données bancaires, et les comptes clients étaient conservés sans limite de temps (pls de 3millions de client non connectés durant 5 ans, et données tjrs gardées)
→ *Voir communiqué de la CNIL*

F. Intégrité et confidentialité

Intégrité : les données ne doivent pas être altérées (modifiées, pertes), elles doivent restées intègre, indemne de tout dommage, que ce soit par incident ou par malveillance.
Confidentialité : L'idée que les données ne doivent être portés à la connaissance que de leur destinataire légitime, elles ne doivent pas être accessible par n'importe qui que ce soit au sein d'une etp ou même en dehors de l'etp.
Ex : Site de rencontre infidèle : des pirates ont menacé de publier les noms des inscrits aux USA. Ils ont publié cette liste, obtenue par une fuite de données.

La CNIL peut être saisie par un particulier, mais elle peut aussi s'auto-saisir. La sanction qu'elle fixe est une amende administrative, donc le montant ne revient pas au particulier.
Mais il peut demander cessation d'atteinte et réparation d'un préjudice devant le juge civil.

Dans le RGPD, dans l'article relatif aux sanctions, il est prévu deux plafonds de sanction :
sur manquement peu grave 10M d'Euros ou 2% chiffre d'affaire mondial
sur manquement plus grave 20M d'euros ou 4% du chiffre d'affaire mondial

- Art 6 RGPD :

Pour traiter des données à caractère perso , il faut pouvoir se prévaloir d'au moins un fondement de l'art 6 du RGPD :

- le consentement
- la nécessité du traitement pour l'exécution d'un contrat
- le respect d'une obligation légale
- la sauvegarde des intérêts vitaux d'une personne physique
- l'exécution d'une mission d'intérêt public
- l'exécution à des fins d'intérêt légitime

A. Le consentement

Bien souvent le consentement est extorqué, car on donne un simple consentement de façade.
On accepte souvent les pops up, sans lire l'intégralité, donc consentement de façade.
Donc le RGPD se préoccupe de la qualité de ce consentement, mais le RGPD y répond par des exigences qui restent théorique :
Art 7 précise les conditions applicables au consentement.

- Le rp de traitement doit pouvoir prouver le consentement
- Si le consentement est donné de manière écrite, alors la demande de consentement doit être donnée à part, et non dans un bloc contenant plusieurs demandes
- Consentement sous une forme compréhensible en terme sobre, simple et clair.
- La personne concernée à le droit de retirer son consentement à tout moment

Le consentement n'est pas tj le bon fondement sur lequel se fonder.
Si on pose la question et que la personne répond non, et qu'on essaie de la convaincre, alors le consentement n'est pas forcément le fondement adéquat.

Il existe un régime spécifique pour le consentement des enfants.
Si un enfant de -16 ans, le consentement doit être donné ou autorisé par l'autorité parentale.
Toutefois, les états membres peuvent descendre cet âge à un minimum de 13 ans.
La demande de consentement doit être très claire, même plus que pour les adultes.

Délibération de la CNIL, 21 janvier 2019 : sanction de 50M d'€ infligée à Google.
Sanction faible pour Google au regard de leur chiffre d'affaire, mais cette jp menace le modèle économique de Google.
Plusieurs reproches à l'affaire:
Affr internationale, donc pb de compétence de la CNIL ? (AAI de la France). Cette dernière à considéré qu'elle était compétente, le CE a validé.
Sur le fond : CNIL reproche à Google une politique de confidentialité trop obscure en se fondant sur le fait que la proposition de traitement doit être claire et simple. Pour autant, la politique de conf de Google ne semble pas être la plus mauvaise/obscure, mais certains passages trop flous
Enseignement 1 : le niveau d'exigence de la CNIL en matière de protection des données est extrême.

B. La nécessité du traitement pour l'exécution d'un contrat

Si le rp de traitement prouve que le traitement mené est nécessaire à un contrat, alors traitement valide.
Ex : Amazon, veut livrer. L'adresse est nécessaire dans ce contrat de livraison, donc la commande inclut le consentement, pas besoin de demander spécialement le consentement.

C. Le respect d'une obligation

On traite une donnée car la loi nous l'ordonne.
Ex : La collecte du NIR (numéro sécu sociale) par employeur est une obligation légale.

D. La sauvegarde des intérêts vitaux de la personne.

Sert surtout à la médecine d'urgence.
Ex : on arrive à l'hôpital avec hémorragie massive, pas besoin du consentement pour que l'hôpital puisse prendre accès au dossier médical, groupe sanguin, etc.

E. Mission d'intérêt public

Très utile aux administrations (impôts, universités, FISC, etc..)
Ex : le fisc n'a pas à demander les informations fiscales aux particuliers pour traiter ces données.
Ex : fondement adéquat pour une application comme Stop Covid, la CNIL dit que le fdnt le plus spécifique est le consentement, donc consentement requis.

F. Intérêt légitime

Le rp de traitement qui ne se suffit pas des autres fdnt, peut dire que c'est dans son intérêt légitime
Mais ils oublient, qu'il faut montrer une nécessité pour IL.
Il faut un intérêt légitime, pas n'importe lequel (le seul intérêt de tirer du profit ne suffit pas)
En réalité on doit peser l'intérêt légitime du rp de traitement/tiers avec les intérêts et libt de la personne concernée par le traitement.
Cette balance est assez difficile à anticiper.
Ex : intérêt légitime admis : traitement pour essayer de détecter des vols de compte, usurpation d'identité attaques pirate,

Art 6-4 RGPD :

L'art 6-4 est une exception à la nécessité d'avoir un fdnt pour traiter des données :
Si les données sont traiter pour la finalité 1, mais qu'on veut les traiter à la finalité 2, c'est envisageable selon des conditions, il faut que les 2 finalités soient compatibles
Il faut aussi tenir compte de l'existence éventuelle d'un lien entre les 2 finalités, du contexte
Ex : contrat avec compagnie d'assurance pour un voiture. Dans le cadre de la nécessité pour exécution du contrat, l'assurance traite des données. Le contrat prend fin, donc la finalité prend aussi fin, en théorie on ne peut plus traiter les données. Mais l'assurance doit construire une base de données pour établir ses statistiques afin d'évaluer le montant des futures assurances donc obligés de continuer à traiter les données du contrat (si anonymisés pas de pb, ça entre plus dans RGPD) mais très dure à anonymiser ; donc le traitement des données pour établir des statistiques serait une finalité nouvelle : lien entre les 2 puisque les statistiques permettent d'établir contrat/prime.

Concernant les données sensibles :

- Art 9 RGPD : Dans le RGPD, on les appelle les « données a caractère personnel particulier »

« Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdit »

si ces données sont traités, il faut se demander si ce traitement correspond à une dex exceptions
Les objets connectés (montres, balances, tensiomètre, etc) traitent de ces données, de même que l'assurance maladie, ou facebook, ou encore les organisations gérant les demandes d'asile.
Ce principe de non traitement de ces données connaît des limites :
Dans quelles situations peut on traiter ces données ?

- Voir les exceptions de l'art 9-2 RGPD.
- Art 10 RGPD : données relatives aux condamnations pénales et aux infractions
  Pour traitement relatif aux enquêtes, poursuites, condamnation il existe la directive
- Directive e-privacy : elle régit à titre principal la question des bandeaux de cookies.

CHAPITRE 2 :
Obligations des responsables de traitement et des sous-traitants

Avant le RGPD : régime de formalités préalables. Selon les cas de traitement des données personnelles, on devait le déclarer à la CNIL et parfois solliciter l'autorisation de la CNIL.
Rapidement, il est devenu inenvisageable que la CNIL ait une connaissance personnelle de chaque traitement de données en France.
On a donc inventé des dispenses de déclaration, déclarations simplifiées, autorisations uniques (cahier des charges strictes à respecter pour le faire sans demander si on veut faire autrement alors il faut une demande d'autorisation) pour désengorger la CNIL
Avec le RGDP on change de philosophie : ajd idée de responsabilisation (« accountability ») : c'est au rp de traitement de convenir lui même les mesures à prendre pour respecter le RGPD.
Le pcpe est donc celui de la liberté, puis éventuellement un contrôle avec une sanction forte en cas de non respect au RGPD.
(Rappel : Avant RGPD sanction la + élevée : 150000€ ; aujourd'hui double plafond 20M ou 4% du CA mondial)
En réalité, ce principe n'est pas perçu comme un cadeau car ils se sentent seuls livrés à eux mêmes avec une peur de la sanction. Des RT/ST n'ont pas les moyens de payer des mises en conformité au RGPD.
Il faut garder à l'esprit que le RGPD a 2 objectifs : une vraie réglementation européenne et la libre circulation des biens/services et des données dans l'UE.

Art 35 RGPD pose que les traitements qui présentent un danger obligent à réaliser une analyse d'impact (PIA : *protection Impact Assessment*)
Qu'est ce que le PIA ?
Lorsqu'il y a un risque d'atteinte, il faut analyse d'impact : c'est une sorte d'auto diagnostic poussée avec différents critères (juridiques, techniques, etc), donc le PIA n'est pas obligatoire.
L'analyse est requise dans un certains nb de cas : Art 35-3
De plus chaque autorité de contrôle définie des listes des opérations pour lesquelles le PIA est obligatoire, mais aussi possible de faire une liste pour établir les op de nécessitant pas de PIA.
La CNIL a crée un logiciel PIA pour permettre de savoir si le PIA est nécessaire ou non et elle propose 3 guides détaillés sur les méthodes, référentielles, doc, etc pour aider, et met à disposition un exemple de PIA fictif rempli.
Si le PIA apparaît inquiétant, on doit consulter l'autorité et attendre sa réponse.
Les etp vont ils voir la CNIL pour dire que leur PIA est inquiétant ? Certains sont dans le déni, d'autres vont exagérer leur PIA pour avoir un avis/conseil de la CNIL, alors même que le PIA ne présente pas de danger (la CNIL doit examiner tous les PIA et répondre).

Art 25 RGPD pose le pcpe de la protection des données dès la conception.
des le départ de la conception d'un produit/service, on doit se préoccuper de la protection des données. C'est le but vers lequel tend le RGPD.
Mais ce principe est difficile à mettre en œuvre dans le domaine de la publicité et avec les modèles économique dits « service contre données ».
(ex : journal gratuit, met des pubs pour se rémunérer, mais si on bloque ces pubs/traqueurs, alors le journal n'a pas de rémunération).

Art 26 RGPD : la chaîne de traitement des données.
Il y a de RT (rp de traitement) et des ST (sous traitants) :
RT : la personne/service qui seul ou conjointement avec d'autres <u>détermine les finalités</u> (pour quoi

on traite) et les moyens du traitement (comment on traite) :
ST : celui qui traite des données pour le compte du RT.
Ex : Amazon WebService (AWS) fournit puissance stockage et de calcul, est un sous traitant.
Ex : Les avocats pour travailler ont besoin que le client apporte un dossier avec les données perso du client et des tiers : les avocats sont donc RT car ils déterminent les moyens et finalités du traitement.
Ex : Facebook est un RT

Régime juridique du RT et du ST
26 RGPD : Si 2 personnes sont RT conjointement
27 RGPD : Si RT/ST n'est pas dans l'UE, il doit désigner un représentant se trouvant sur le sol de l'UE.
28 RGPD : Lorsque qu'un traitement doit être effectué pour le compte du RT, celui ci doit faire appel à un ST qui présentent des garanties suffisantes quant à la mise en œuvre du RGPD. De plus le ST ne peut pas recruter un autre ST sans autorisation écrite, spécifique ou générale. Enfin, entre le RT et le ST, il faut un contrat ou autre acte juridique équivalent qui contient des clauses obligatoires imposées par le RGPD (oblig de sécurité ; confidentialité ; respect RGPD ; suppression ou transfert des données personnelles lorsque contrat prend fin ; le ST peut se faire auditer/inspecter par le RT).

CJUE 5 juin 2018 : création d'une « page fan » fb : est ce que cette création est un traitement de données ? La CJUE explique qu'en créant la page fan , on a agit comme un rabatteur d'utilisateurs vers fb, on a fournit un courant d'utilisateurs, donc on a contribué à amener de l'activité sur fb. La création d'une page fan implique de la part de l'admin une fonction de paramétrages/filtres (age, centre intérêt, genre etc) qui influent sur le traitement et font remonter des statistiques. On peut donc demander à obtenir/traiter les données des utilisateurs qui aiment la page. La cour conclut qu'il y a coresponsabilité de traitement entre fb et l'admin de la page.

20 juillet 2019 « bouton j'aime » : insérer dans une page dont on est l'éditeur un bouton de partage « j'aime » sur fb : le fait d'implémenter ces boutons ont des conséquences concrètes pour les utilisateurs. Quand l'utilisateur charge la page, l'adresse IP de l'utilisateur est envoyé à fb, même si l'utilisateur n'a pas de compte facebook.
La Belgique avait condamné fb pour avoir traité des données de personnes n'ayant pas de compte fb, donc pas consentement à être tracé par facebook.
Q) posée à la CJUE : comment traiter celui qui a mis un bouton j'aime sur sa page/blog ? Le gestionnaire d'un site internet qui insère sur son site un module social peut être considéré comme un RT. Mais cette rp est limitée aux op de traitement dont le gestionnaire détermine la finalité et les moyens. Donc la CJUE dit que les coresponsables ne sont pas forcément rp au même niveau.

Concernant le registre des activités de traitement :
Ce registre des activités de traitement est une documentation qui accompagne le PIA.
Il permet de relater le processus de la mise en conformité.
Qui doit tenir un registre des activités de traitement ? Chaque RT doit en tenir un.
Mais il existe des dispenses : pour les etp de -250 salariés, SAUF si pour certaines situations dangereuses.
La CNIL propose un modèle de registre et met à disposition son registre des traitements.

Concernant la sécurité du traitement :
Les données doivent ê protégées contre des altérations accident ou attaque) et contre des fuites internes ou externes au RT. Si des personnes qui ne sont pas habilités connaissent ces données, alors confidentialité non respectée.
Les mesures devant être prises sont : des mesures informatiques évidement, mais aussi des mesures

physiques dans les locaux.
Pour assurer la protection des données :

- il faut prendre des mesures suffisantes adéquates (art 32 RGPD) : anonymisation, chiffrement des données
  Le RGPD ne fait pas peser d'oblig de résultat sur les RT, mais plutôt des obligations de moyens.
  Le seul fait qu'il y ait eu incident de sécurité n'emporte pas forcément une sanction si le RT avait prit des mesures pour assurer la protection
- il faut une transparence : si il y a incident, les etp doivent le déclarer/notifier aux autorités de contrôle (art 33) sauf si pas de risques pour droits et libt, et aux personnes concernées (art34) en cas de risque élevé seulement.
  Il faut déclarer dans les meilleurs délais.
  En cas de doute sur le caractère grave de l'info volée, alors notifier tout de même la CNIL.
  Ex de sanction : mai 2019 : sanction infligée à une agence immobilière (CA 43M d'€/an). Le pb est que les candidats à la location via cette sct constituent un dossier en ligne et peuvent accéder aux autres dossier des autres clients en changeant l'url. Incident de sécurité involontaire 400k de sanction.

- DPO (Data Protection Officer) (délégué à la protection des données) : Qqn qui aide à la mise en conformité de l'etp à temps partiel ou à temps plein.
  Il n'y a pas de DPO dans ttes les etp/organismes, que ds certains cas : si traitement effectué par une autorité/organisme public (donc les communes doivent avoir un DPO)
  Art 38 : Il faut lui donner un certains nb de moyens, il doit être associé à ttes les q° relatives aux données personnelles, et il faut lui fournir des ressources matérielles et financières (local, matériel, budget etc)
  Il existe 2 figures de DPO qui co existe : DPO interne (salarié de l'etp à qui on demande d'être le DPO : l'avantage est qu'il est au quotidien dans l'etp et donc ça l'aide à voir les difficultés) et le DPO externe (prestataire rémunéré en honoraire, c'est une mission de conseil).
  Le DPO est celui, qui au quotidien, se bat pour imposer une certaine culture de protection des données
  Le RT veille à ce que le DPO ne reçoive aucune instructions, il est indépendant, il ne reçoit pas d'ordres (indépendance difficile pour les DPO internes.
  Le DPO fait directement son rapport au plus haut niveau de l'etp (les dirigeants).
  Les personnes dont les données sont traitées peuvent prendre contact avec le DPO pour exercer leurs droits.
  Le DPO est soumis à une obligation de confidentialité.
  Il peut exécuter d'autres missions et taches, mais il faut faire attention à ce qu'il n'y ait pas de conflits d'intérêts (ex : le DSI ne peut pas être DPO)
  Art 39 énumère les missions :
  - Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations du RGPD
  - Contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données
  - Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données
  - Coopérer avec l'autorité de contrôle et fait office de point de contact avec l'autorité de contrôle. Donc la CNIL peut poser des questions au DPO pour avoir des information
  (Pour être DPO pas obligatoire d'être certifié par la CNIL, mais on peut se faire certifier par la CNIL : 35h de protection des données + 2 ans d'expérience. Ce n'est pas la CNIL qui certifie mais un autre organisme : QCM de 100 questions.

CHAPITRE 3 : Droits de personnes concernées

Préalable indispensable Les obligations de transparence pèsent sur le RT qui visent à informer les personnes qu'on traite leur données, alors c'est la condition pour que les personnes puissent exercer leurs autres droits.
Si elles ne sont pas au courant que leurs données sont traitées, alors on aura pas l'idée d'exercer nos autres droits.
Art 13 concerne les collectes directes : qd le RT se trouve en contact avec celui ou celle dont il traite les données (ex : RT et la personne se sont rencontrés dans le monde physique)
Art 14 concerne les collectes indirectes : RT n'est pas en contact avec la personne (ex : RT achète une base de données)
Quelles info doit on donner ?
Art 13 :
Les info a tjrs fournir

- fournir l'identité et les coordonnées du RT , du DPO si il y en a un , les finalités du traitement, les bases juridiques du traitement. Qd le traitement est fondé sur l'intérêt légitime, alors il faut énoncer l'intérêt légitime en question.
- Les destinataires des données
- le cas échéant, le fait qu'on est l'intention de faire partir les données en dehors de l'UE
- durée de conservation des données, l'existence du dt de demande, l'accès, l'effacement, ect. Donc il faut avertir sur les dt des personnes concernées
- Qd traitement est fondé su consentement, il faut rappeler à la personne qu'elle peut retirer le consentement à n'importe quel moment (cessation du traitement, mais ne remet pas en question les info collectées avant)
- le dt d'avoir des infos, contextes pour savoir si le traitement se fait sur ordre de la loi
- l'existence d'une procédure automatisée (machine)
- seule possibilité de ne pas exécuter la transparence : si la personne dispose déjà de ces informations (la personne est déjà mise au courant)

Art 14 :
En cas de collecte indirecte, il faut donner les mêmes info en général que l'art 13 + il faut donner la source du proviennent les données (pas de face à face avec RT) ,
et les raisons pour lesquelles ont peut refuser la transparence :

- le même que le 13
- lorsque la fourniture de telles info est impossible car seulement pour recherche scientifique, statistiques
- qd obtention et communication des informations st prévus par loi ou dt de l'UE.
- les infos doivent rester confidentielles en vertu d'une obligation de secret professionnel

((HORS COURS : Avant de compter exercer nos droits devant le RT, on peut agir en amont de la collecte et semer moins de données derrière nous. Choisir un service plutôt qu'un autre revient à exposer nos données de manière différentes.
Ex : qwant et Google : Qwant rien n'est stocké.
CNIL a crée un logiciel data vise,
logiciel privacy badger
Série Do Not Track))

En aval de la collecte, donc une fois collectée, on a des outils juridiques mis à disposition par le RGPD :

- Le droit d'accès (art 15) : la personne concernée à le dt de la part du RT d'obtenir la confirmation ou non qu'il détient des données sur elle, et le droit d'avoir accès à ces données.
  Dt puissant inconditionnel (pas de motif nécessaire pour l'invoquer).
  Si le droit est exercé, alors l'accès DOIT être rendu effectif (obligation)
  Délai max 1 mois pour donner accès par les RT.
  Le dt d'obtenir une copie ne porte atteinte aux dt et libt d'autrui, seules les données concernant la personne qui demande doivent être données, pas d'autres info concernant d'autres personnes.
  Ex : on peut utiliser ce droit pour savoir si on figure dans un fichier qui nous porte préjudice ; pour savoir ce qu'un réseau social détient sur nous ; connaître les données présentes dans votre dossier médical →→ Faire ces démarches)
  (Sur fb nvx outils permettant de savoir quelles info hors fb, remontent sur fb : Off activiy)
  Il y a une tendance émergente : le dt d'accès comme stratégie pré contentieuse (ex : pour un salarié)
- Le droit de rectification et d'effacement (art 17) : ce dt n'est pas discrétionnaire, les RT peuvent refuser le droit à l'effacement (le fisc ne va pas suppr toutes nos données)
  On peut demander effacement quand les données ne sont plus nécessaires au but du traitement ; lorsque la personne retire son consentement et que le traitement n'est fondé sur aucun autre fondement ; la personne s'oppose au traitement ; les données ont fait l'objet d'un traitement illicite ; les données doivent être effacées en vertu de la loi.
  Cas particulier : les données perso d'enfants (avant 15ans) sur base du consentement, alors le dt à l'effacement devient discrétionnaire (obligatoire si demandé)
- le droit de déréférencement : il se fonde sur l'art 17.
  CJUE , 13 mai 2004, Google Spain c/Costeja : Costeja mauvais payeur, puis remboursement de ses dettes. 13 ans après, un journal publie un article sur Costeja. Lorsqu'on tapait son nom dans Google, le premier résultat était l'article de journal concernant la saisie de ses biens. Il assigne le journal et Google. La CJUE donne raison à Costeja « l'article va rester sur le journal, mais le résultat de recherche doit être retiré »
  La CJUE dit que Google ne doit pas faire preuve d'hypermnésie, et de ne pas fixer pour un individu ses actes passés à jamais.
  Du seul fait qu'une info soit obsolète, alors on peut exercer ce droit. Le droit de la personne qui formule la demande est mis en balance avec le droit à l'information du public. La demande sera envoyée devant une commission de Google, qui analyse la demande. Ceci s'inscrit dans un mouvement de privatisation de la police de l'expression en ligne (on laisse à des acteurs privées le choix de ce qui est dit et laissé sur internet). Police privée en matière de dt d'auteur, en matière de discours de haine (loi AVIA démontée par le Ccel), donc on laisse à Google choisir.
  Lorsque l'on obtient le déréférencement, celui ci est définitif (même si la personne concernée devient célèbre).
  Portée territoriale du dt au déréférencement : lorsque Google faisait l'objet 'un demande et qu'il l'accepté, il procédait au déréférencement seulement dans le pays de la personne concernée. La CNIL est intervenue, et Google a réagit en retirant le résultat de recherche lorsque la requête est effectuée dans l'UE (mais si on utilise un vpn, et qu'on se place aux USA, le résultat revient). La CNIL est re intervenue, et a imposé a Google que le déréférencement devait valoir pour le monde entier. Google répond non.
  La CJUE dit que rien dans le dt européen ne commande qu'il soit procédé à un retrait mondial MAIS le dt national est souverain pour décider de cette q°. Le CE n'a pas soutenu l'exigence de la CNIL.
- le droit de limitation au traitement (art 18 RGPD) :
  Limitation du traitement est l 'idée que le traitement doit être temporairement gelé/arreté, mais ce n'est pas une fin définitive du traitement. On l'arrêté temporairement
  durant plusieurs cas :

Qd une pers conteste l'exactitude des données, alors en attendant la vérification de l'info on stoppe le traitement
Qd le traitement est illicite, mais qu'elle ne veut pas l'effacement. La personne va vouloir mettre en pause pour garder une preuve que le traitement est illicite
Qd le traitement est nécessaire pour une action en justice, alors on peut demander à être en pause le traitement pour garder les données

- La portabilité (Art 20 RGPD) : les personnes concernées ont le dt de recevoir les données perso les concernant, sous forme de fichier informatique (alors que dt d'accès peut être envoyé sous forme papier) pour les réinjecter dans un autre système informatique (raison de vouloir cela : perspective concurrentielle : ex je veux changer de boite mails, donc je télécharge un fichier avec mes mails et contacts et je le réinjecte sur ma nvlle boite mail ; ou perspective « Self data » :
  La portabilité ne marche que pour 2 fdmt de licéité : consentement et contrat.
- Profilage : décision automatisée : c'est cette tendance de plus en plus forte à mettre des notes aux gens, à leur attribuer des profils sur la base d'un traitement algo des info personnelles. Ces algo de traitement sont dangereux (ex : Amazon essaie de sélectionner des CV avec du machine learning ; IA : Amazon donne une base de données avec les trajectoires pro, donc ceux qui réussissent : la base de données fait ressortir surtout des hommes blancs, donc l'algo trie les cv et fait remonter des hommes blancs).
  La personne a le dt de ne pas faire l'objet d'une décision uniquement automatisé produisant des effets juridiques ou effets aussi puissants (accepter de conclure un contrat, accepter de recruter) MAIS exception : qd la décision est fondée sur le consentement explicite de la personne, ou si autorisé par dt de l'UE ou national, ou si c'est nécessaire de recourir à une décision automatisée uniquement.
  Mais dans les cas de ces exceptions, les personnes ont une garantie : le dt d'obtenir une révision humaine de la décision, et elles peuvent exprimer leur point de vue et se défendre.
- Le droit à l'opposition : dt qui sert notamment à refuser la prospection commerciale, il suffit d'écrire à l'etp concernée, et elle sera obligée d'arrêter la prospection.

Q° des données après la mort : pas abordée par RGPD, mais abordée par loi informatique et libt.
Que deviendront nos données à notre mort ? Ces données (photo, fichiers, info, etc) ont fait l'objet de débat sur la transmission de ces données.
Si la personne s'est exprimée sur la transmission, alors pas de problème.
Si la personne n'a rien dit ?
Art 40-1 de la loi informatique et liberté : les héritiers peuvent accéder aux données dans la mesure nécessaire au règlement de la succession.

CHAPITRE 4 : La circulation internationale des données.

I. Le champs d'application territorial du règlement:
Art 3: le RGPD s'applique aux rp de traitement qui ont un établissement sur le territoire de l'Union.
Même si le traitement est effectué en dehors de l'UE.
Si dans l'UE, RGPD applicable que le traitement ait lieu ou non dans l'UE.
Si pas d'établissement dans l'UE ? Pas RGPD
Sauf lorsque le traitement est relatif à des personnes qui se trouvent dans l'UE alors RGPD s'applique même si le RT ou ST est en dehors de l'UE: seulement si
il y a une offre de bien/ service dirigée vers une personne dans l'UE (le public européen doit être visé) -> livraison dispo ds pays de l'UE ? site traduit en langue de l'UE? alors rgpd
il y a un suivi de comportement de personnes se trouvant dans l'UE (ex: géolocalisation de citoyens européens

II. L'export de DP
Art 44: un transfert vers un pays tiers ne peut avoir lieu que si les conditions définies par RGPD sont respectées, y compris pour les transferts ultérieures.
Art 45: plusieurs situations:
Décision d'adéquation lorsque la commission européenne a constaté que le pays tiers assure un niveau de protection adéquat: donc pas besoin d'autorisation spécifique.
———
Actualité
Google va tester un nvx de ciblage publicitaire : les FLOC en 2021. Les utilisateurs seront répartis groupes de centres d'intérêts, et non plus individuellement comme c'est ajd le cas