

FONDAMENTAUX DE LA PROTECTION DES DONNÉES 1ÈRE PARTIE

ALEXANDRA GUÉRIN-FRANÇOIS



PLAN

1^{ère} partie (jour 1)

- La protection des données : contexte
- Concepts fondamentaux
- Principes fondamentaux



LA PROTECTION DES DONNÉES: CONTEXTE

1. RAPPEL HISTORIQUE

Le projet SAFARI

• • • LE MONDE — 21 mars 1974 — Page 9

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une « division de l'informatique » au ministère de la Justice, celui de l'Intérieur met la dernière main à la mise en route d'un ordinateur

puissant destiné à rassembler la masse énorme des renseignements grappillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à donner chaque Français par un « identifiant », qui ne distingue que lui, maintenant fermée, est l'objet de conversations ardentes; le ministère de l'Intérieur y souhaitait

jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale.

Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebuté : celui des rapports des libertés publiques et de l'informa-

tique. Son importance exigeait qu'il en soit, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministre de la Justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

« Safari » ou la chasse aux Français



1974

Safari ou la chasse aux Français.

Loi
Informatique
& Libertés

Article 1^{er}

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

1978

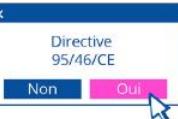
Vote de la loi Informatique & Libertés et création de la CNIL.

1995

L'Europe vote une nouvelle directive.

1991

Arrivée d'Internet !



2016

La CNIL accompagne
l'innovation.



2018

La CNIL
a 40 ans !



Vote du règlement européen sur les données personnelles.

LA LOI INFORMATIQUE ET LIBERTÉS

6 janvier 1978 : LIL I

6 août 2004 : LIL II

20 octobre 2005 : décret d'application

7 octobre 2016 : loi pour une République numérique

LIL III

- **25 mai 2018** : entrée en application du RGPD

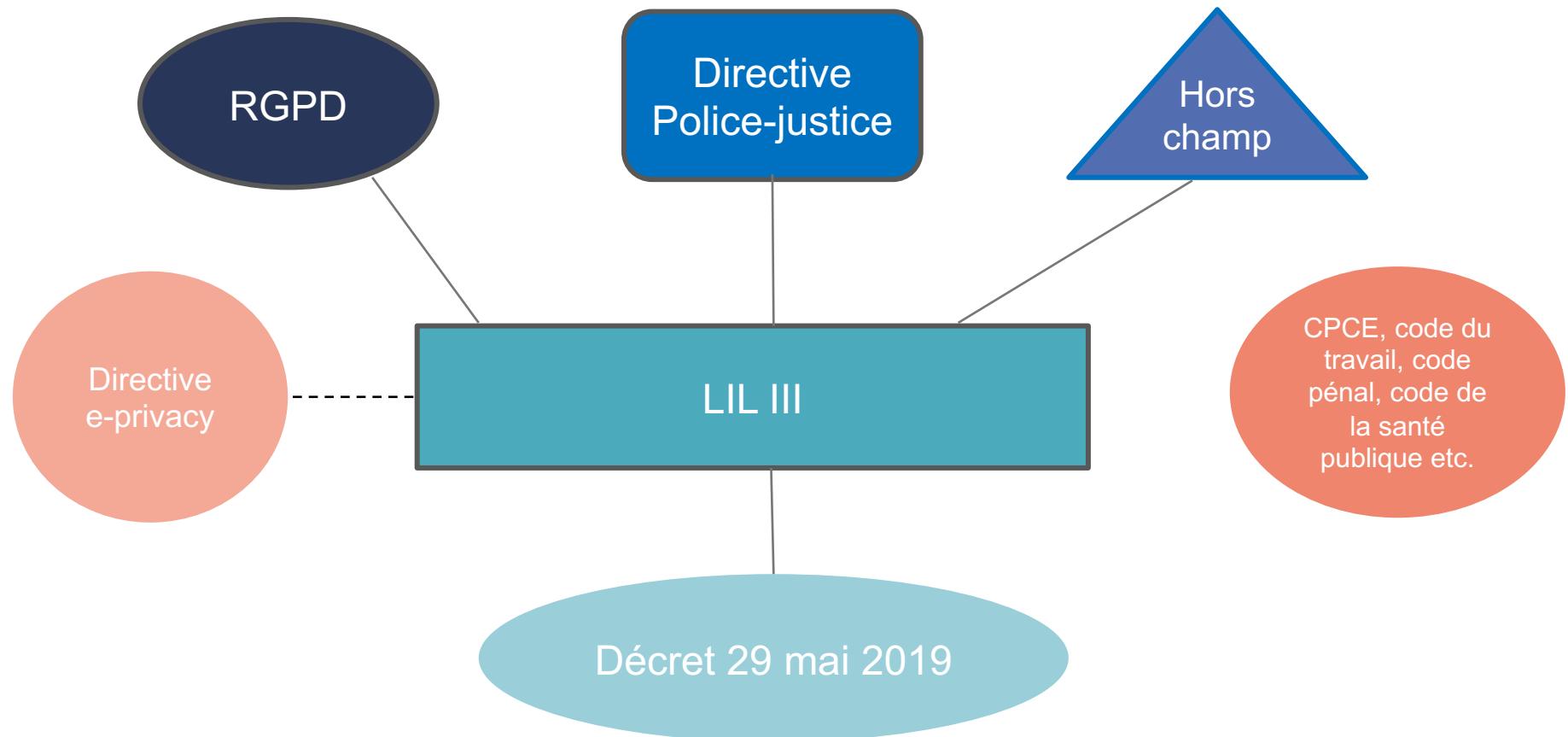
- **20 juin 2018** : loi d'adaptation du RGPD + transposition directive « police justice »

- **1er août 2018** : décret d'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

- **12 décembre 2018** : ordonnance n° 2018-1125 en vigueur au plus tard en juin 2019, (en même temps que le nouveau décret d'application de la loi Informatique et Libertés)

- **29 mai 2019** : décret d'application de la LIL III

ARTICULATION





https://www.youtube.com/watch?v=i_k8ozkY2I4

2. CONCEPTION EUROPÉENNE



- 1970: le land de Hesse adopte la 1ère loi sur la protection des données au monde
- 1978 : la France adopte la Loi Informatique et libertés suite au projet Safari

CONCEPTION EUROPÉENNE



- **Droit fondamental :**

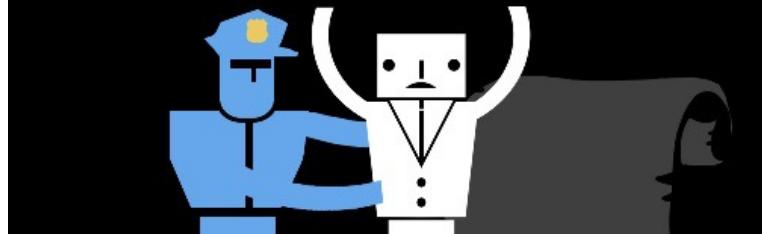
Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel : 1^{er} instrument international juridiquement contraignant adopté dans le domaine

Les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (**respect de la vie privée et la protection des données à caractère personnel**) / L'article 16 du traité Lisbonne

- **Donnée personnelle = attribut de la personnalité**
- **Encadrement strict** : Toute exploitation de données constitue une violation potentielle d'un droit fondamental, et devra être justifiée (ex: par un intérêt légitime, un consentement, l'exécution d'un contrat..).
- **Autorité de contrôle indépendante** : en France, la CNIL

CONCEPTION AMÉRICAINE

FOURTH AMENDMENT



- **Une protection hétéroclite :**

Au niveau de la Constitution fédérale (4^{ème} Amdt) : droit de protection de la vie privée, mais uniquement à l'égard du gouvernement.

Au niveau de l'Etat fédéral : des lois spécifiques protégeant les données personnelles dans des secteurs spécifiques (santé, banque, assurance, enfants, FTC Act...)

Au niveau de chaque Etat : la « common law » et des lois particulières reconnaissent un droit à la protection de la vie privée à l'égard d'acteurs privés

- En dehors de secteurs très régulés, les entreprises sont libres d'exploiter des données pour autant que les entreprises ne commettent pas de « pratique déloyale ».

Donnée personnelle = bien marchand

Federal Trade Commission : Protecting Consumer Privacy

'Surveillance is the business model of the internet,' Berkman and Belfer fellow says

By LIZ MINEO/HARVARD STAFF WRITER, August 25, 2017

GAZETTE: But Google and Facebook face more restrictions in Europe than in the United States. Why is that?

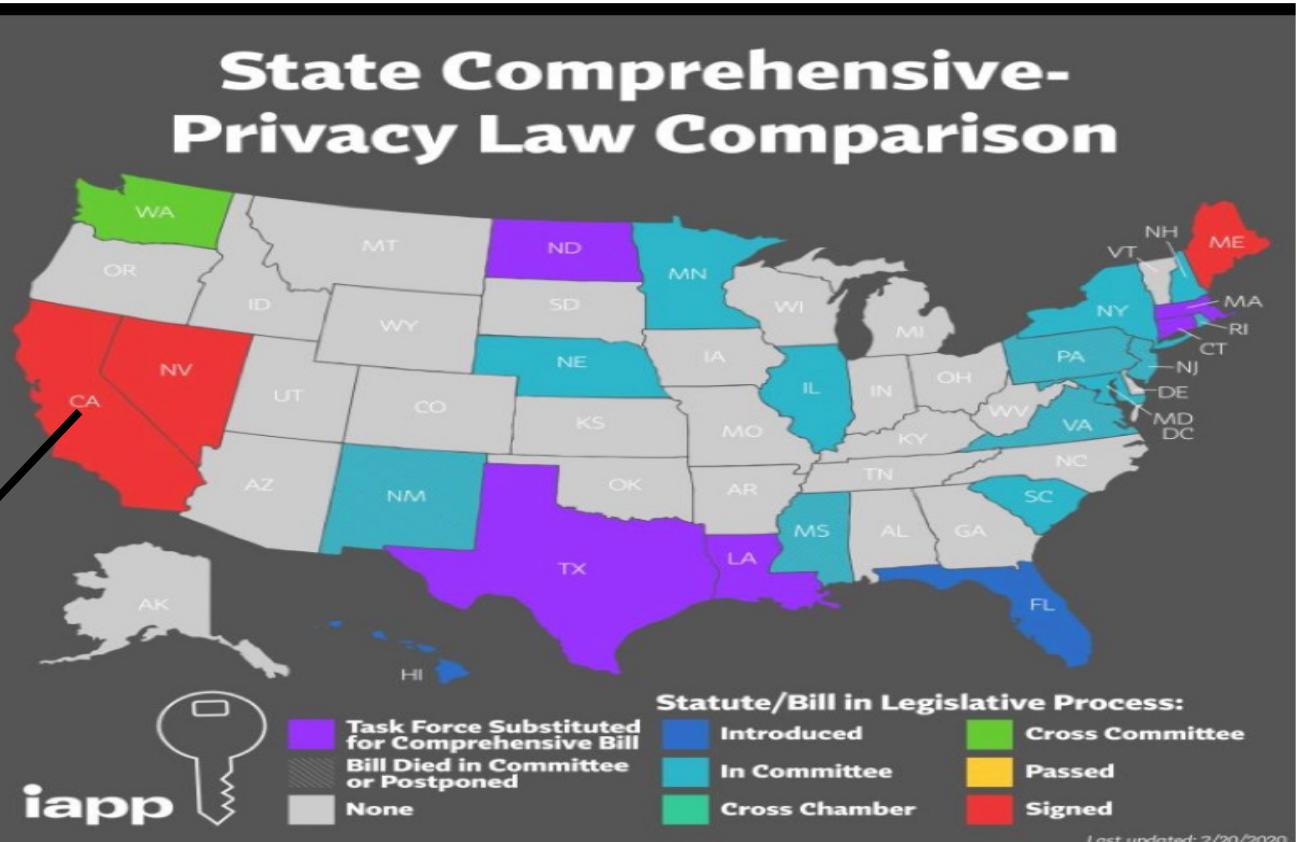
SCHNEIER: Europe has more stringent privacy regulations than the United States. In general, Americans tend to mistrust government and trust corporations. Europeans tend to trust government and mistrust corporations. The result is that there are more controls over government surveillance in the U.S. than in Europe. On the other hand, Europe constrains its corporations to a much greater degree than the U.S. does. U.S. law has a hands-off way of treating internet companies. Computerized systems, for example, are exempt from many normal product-liability laws. This was originally done out of the fear of stifling innovation.

GAZETTE: It seems that U.S. customers are resigned to the idea of giving up their privacy in exchange for using Google and Facebook for free. What's your view on this?

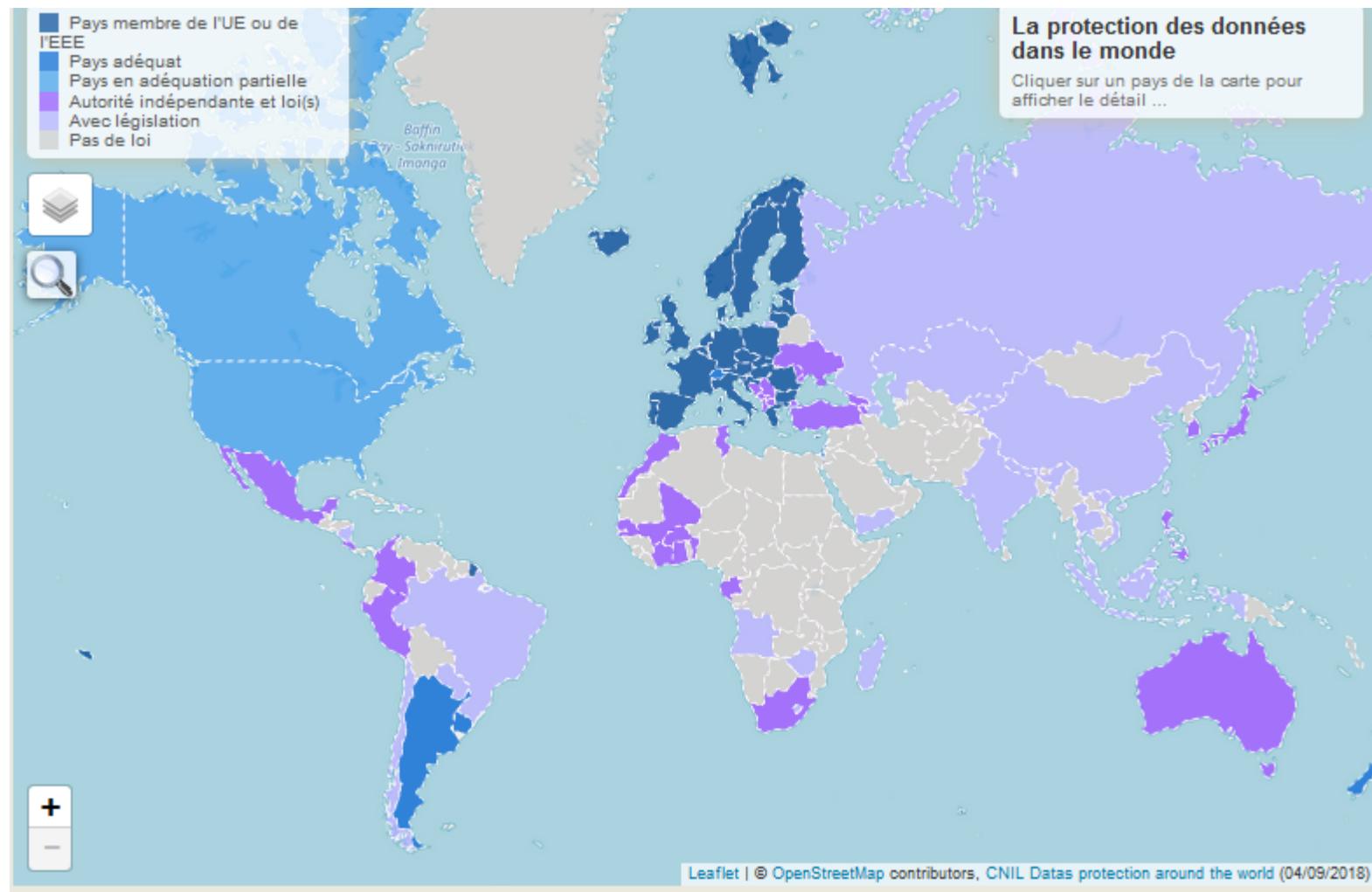
SCHNEIER: The survey data is mixed. Consumers are concerned about their privacy and don't like companies knowing their intimate secrets. But they feel powerless and are often resigned to the privacy invasions because they don't have any real choice. People need to own credit cards, carry cellphones, and have email addresses and social media accounts. That's what it takes to be a fully functioning human being in the early 21st century. This is why we need the government to step in.



CALIFORNIA CONSUMER PRIVACY ACT



ÉVOLUTION INTERNATIONALE



3. LE RGPD, UNE RÉVOLUTION?



SANCTIONS

			
Avertissement	Rappel à l'ordre	Suspension du traitement des données	Amende
			<p>Jusqu'à 20 millions d'EUR</p> <p>ou</p> <p>4 % du chiffre d'affaires annuel mondial</p>

Démarchage téléphonique : La Cnil condamne une société d'isolation à 500.000 euros d'amende

HARCELEMENT L'entreprise Futura Internationale refusait de supprimer les contacts des personnes ne souhaitant plus être démarchées par téléphone

20 Minutes avec agences

|  Publié le 27/11/19 à 14h25 — Mis à jour le 27/11/19 à 14h25



UK privacy watchdog to fine Facebook 18 mins of profit (£500,000) for Cambridge Analytica

Wow, Mark Zuckerberg must be really, really terrified

Le Monde

Consulter
le journal

ACTUALITÉS ▾ ÉCONOMIE ▾ VIDÉOS ▾ OPINIONS ▾ CULTURE ▾ M LE MAG ▾

PIXELS • CNIL

Données personnelles : la CNIL condamne Google à une amende record de 50 millions d'euros

Le gendarme français de la vie privée reproche au géant américain de ne pas informer assez clairement ses utilisateurs.

Le Monde avec AFP • Publié le 21 janvier 2019 à 15h42 - Mis à jour le 22 janvier 2019 à 06h33

UN OBJECTIF D'HARMONISATION



News Connect Train Certify Resources Conferences Join

STORE



apologize for any inconvenience. If you are interested in purchasing an exam or submitting your CPE's, please email us at certification@iapp.org and we will notify you when we're back up and running.

X DISMISS

ResourceCenter

All the privacy tools and information you need in one easy-to-find place



Resources



Tools



Research

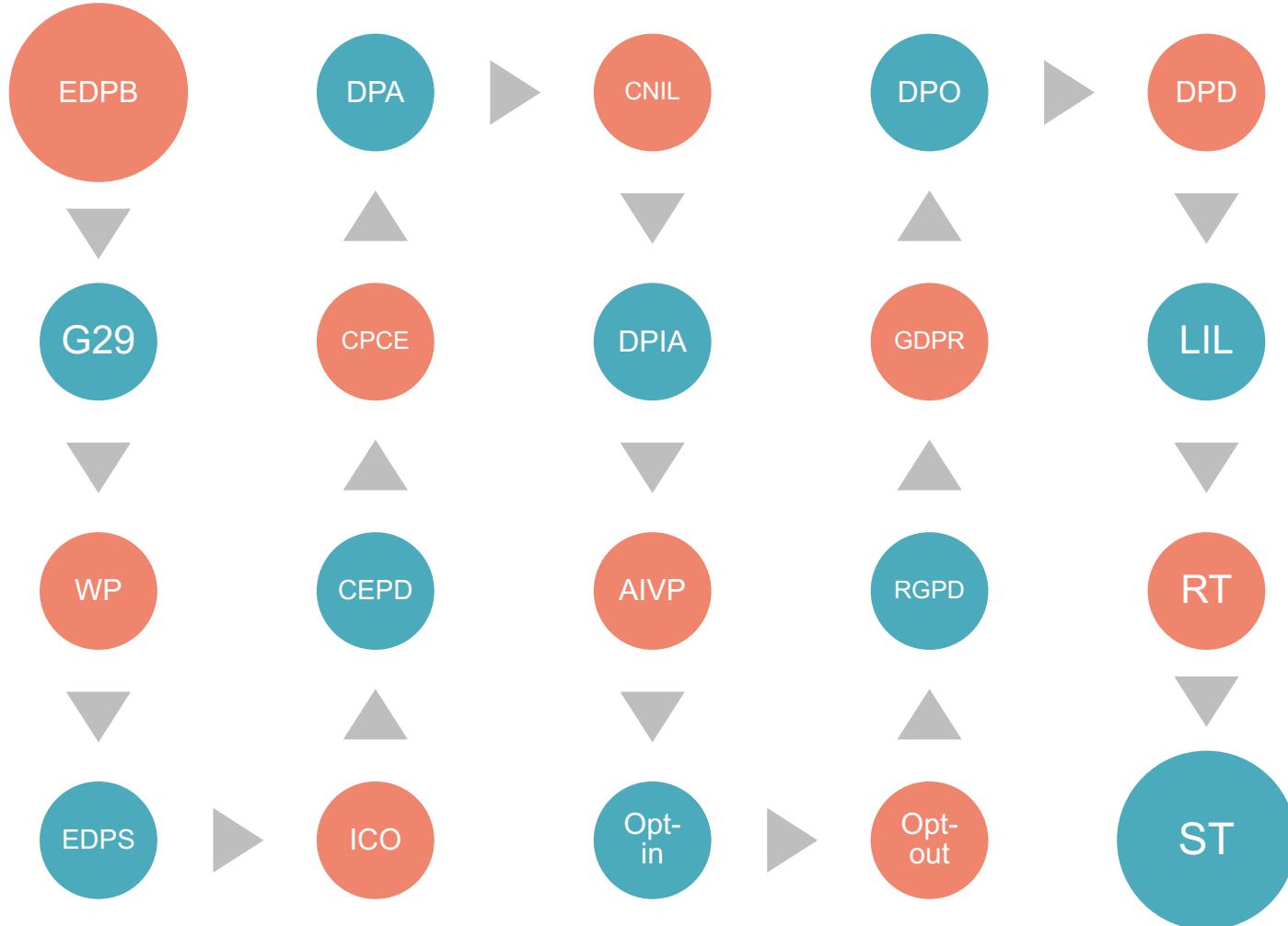


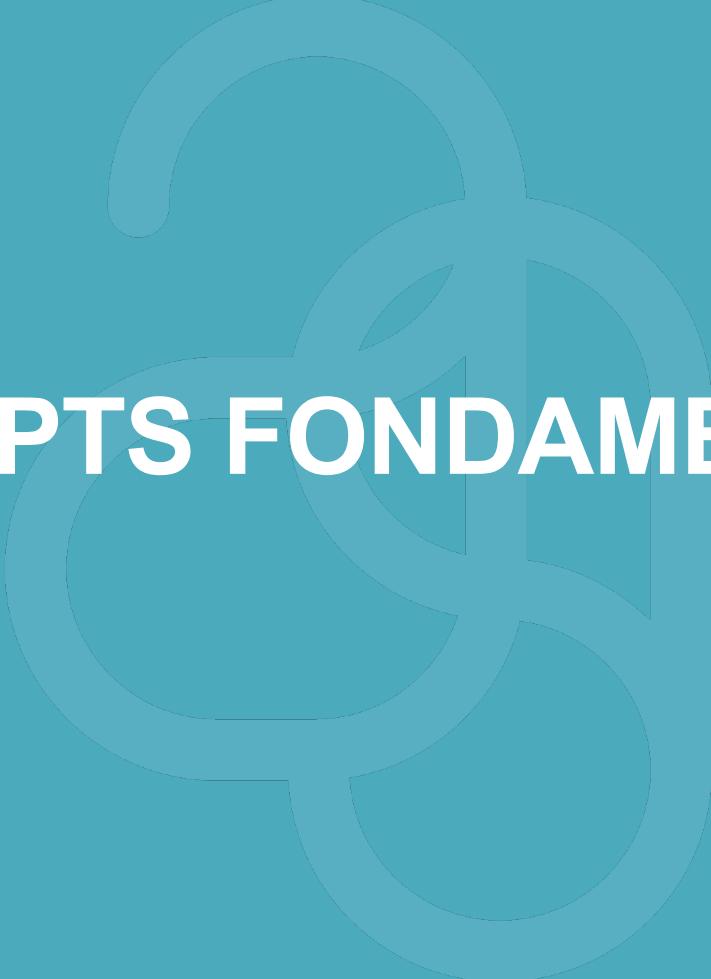
Glossary



EU Member State GDPR Derogation Implementation Tracker

QUELQUES ACRONYMES





CONCEPTS FONDAMENTAUX

RÉFÉRENCES

Les textes

- RGPD
- Loi 20 août 2018 et son décret d'application / ordonnance 12 décembre 2018
- Directive « vie privée » (e-privacy)
 - art. L34-5 code postes et communications électroniques

Les interprétations/ recommandations

- Avis de l'EDPB (ex-G29) https://edpb.europa.eu/edpb_fr
- Référentiels, guides, anciennes normes de la CNIL

LE RGPD : TABLE DES MATIÈRES

CHAPITRE I Dispositions générales

Article premier Objet et objectifs

Article 2 Champ d'application matériel

Article 3 Champ d'application territorial

Article 4 Définitions

CHAPITRE II Principes

Article 5 Principes relatifs au traitement des données à caractère personnel

Article 6 Licéité du traitement

Article 7 Conditions applicables au consentement

Article 8 Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information

Article 9 Traitement portant sur des catégories particulières de données à caractère personnel

Article 10 Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions

Article 11 Traitement ne nécessitant pas l'identification

CHAPITRE III Droits de la personne concernée

Section 1 - Transparence et modalités

Article 12 Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée

Section 2 - Information et accès aux données à caractère personnel

Article 13 Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée

Article 14 Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée

Article 15 Droit d'accès de la personne concernée

Section 3 - Rectification et effacement

Article 16 Droit de rectification

Article 17 Droit à l'effacement ("droit à l'oubli")

Article 18 Droit à la limitation du traitement

Article 19 Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement

Article 20 Droit à la portabilité des données

Section 4 - Droit d'opposition et prise de décision individuelle automatisée

Article 21 Droit d'opposition

Article 22 Décision individuelle automatisée, y compris le profilage

Section 5 - Limitations

Article 23 Limitations

CHAPITRE IV Responsable du traitement et sous-traitant

Section 1 - Obligations générales

Article 24 Responsabilité du responsable du traitement

Article 25 Protection des données dès la conception et protection des données par défaut

Article 26 Responsables conjoints du traitement

Article 27 Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union

Article 28 Sous-traitant

Article 29 Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant

Article 30 Registre des activités de traitement

Article 31 Coopération avec l'autorité de contrôle

Section 2 - Sécurité des données à caractère personnel

Article 32 Sécurité du traitement

Article 33 Notification à l'autorité de contrôle d'une violation de données à caractère personnel

Article 34 Communication à la personne concernée d'une violation de données à caractère personnel

Section 3 - Analyse d'impact relative à la protection des données et consultation préalable

Article 35 Analyse d'impact relative à la protection des données

Article 36 Consultation préalable

Section 4 - Délégué à la protection des données

Article 37 Désignation du délégué à la protection des données

Article 38 Fonction du délégué à la protection des données

Article 39 Missions du délégué à la protection des données

Section 5 - Codes de conduite et certification

Article 40 Codes de conduite

Article 41 Suivi des codes de conduite approuvés

Article 42 Certification

Article 43 Organismes de certification

CHAPITRE V Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales

Article 44 Principe général applicable aux transferts

Article 45 Transferts fondés sur une décision d'adéquation

Article 46 Transferts moyennant des garanties appropriées

Article 47 Règles d'entreprise contraignantes

Article 48 Transferts ou divulgations non autorisés par le droit de l'Union

Article 49 Dérogations pour des situations particulières

Article 50 Coopération internationale dans le domaine de la protection des données à caractère personnel

CHAPITRE VI Autorités de contrôle indépendantes

Section 1 - Statut d'indépendance

Section 2 - Compétence, missions et pouvoirs

Article 59 Rapports d'activité

CHAPITRE VII Coopération et cohérence

Section 1 - Coopération

Section 2 – Cohérence

Section 3 - Comité européen de la protection des données

CHAPITRE VIII Voies de recours, responsabilité et sanctions

Article 77 Droit d'introduire une réclamation auprès d'une autorité de contrôle

Article 78 Droit à un recours juridictionnel effectif contre une autorité de contrôle

Article 79 Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant

Article 80 Représentation des personnes concernées

Article 81 Suspension d'une action

Article 82 Droit à réparation et responsabilité

Article 83 Conditions générales pour imposer des amendes administratives

Article 84 Sanctions

CHAPITRE IX Dispositions relatives à des situations particulières de traitement

Article 85 Traitement et liberté d'expression et d'information

Article 86 Traitement et accès du public aux documents officiels

Article 87 Traitement du numéro d'identification national

Article 88 Traitement de données dans le cadre des relations de travail

Article 89 Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

Article 90 Obligations de secret

Article 91 Règles existantes des églises et associations religieuses en matière de protection des données

CHAPITRE X Actes délégués et actes d'exécution

Article 92 Exercice de la délégation

Article 93 Comité

CHAPITRE XI Dispositions finales

Article 94 Abrogation de la directive 95/46/CE

Article 95 Relation avec la directive 2002/58/CE

Article 96 Relation avec les accords conclus antérieurement

Article 97 Rapports de la Commission

Article 98 Réexamen d'autres actes juridiques de l'Union relatifs à la protection des données

OBJECTIFS

CHAPITRE I

Dispositions générales

Article premier

Objet et objectifs

1. Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.
2. Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.
3. La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.



CHAMP D'APPLICATION MATÉRIEL

Article 2

Champ d'application matériel

1. Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.
2. Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué:
 - a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union;
 - b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne;
 - c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique;
 - d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.
3. Le règlement (CE) n° 45/2001 s'applique au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union. Le règlement (CE) n° 45/2001 et les autres actes juridiques de l'Union applicables au traitement des données à caractère personnel sont adaptés aux principes et aux règles du présent règlement conformément à l'article 98.
4. Le présent règlement s'applique sans préjudice de la directive 2000/31/CE, et notamment de ses articles 12 à 15 relatifs à la responsabilité des prestataires de services intermédiaires.

➤ Personne physique v. personne morale

- Consommateur/ professionnel
- Personne physique professionnelle
- En vie / décédée

LIL III : art.84 et suiv. Dispositions régissant les traitements de données à caractère personnel relatives aux personnes décédées → mort numérique

➤ Activité strictement personnelle

DONNÉE PERSONNELLE

ART.4 : DEFINITION

- 1) «données à caractère personnel», 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;

CONSIDERANT

- (26) Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche.
- (27) Le présent règlement ne s'applique pas aux données à caractère personnel des personnes décédées. Les États membres peuvent prévoir des règles relatives au traitement des données à caractère personnel des personnes décédées.

IDENTIFICATION

À quoi correspondent les données à caractère personnel?



VOUS COLLECTEZ,
STOCKEZ,
UTILISEZ
DES DONNÉES?

Vous devez respecter les règles.

Vous traitez des données pour
le compte d'autres entreprises?
Vous êtes aussi concerné.

- Directement v. indirectement identifiable
- Une seule donnée v. croisement d'un ensemble de données
- Open data
- « catégories particulières » / données biométrique (v. photo)

ADRESSE IP

15 Les adresses IP sont des suites de chiffres qui sont attribuées à des ordinateurs connectés à Internet pour permettre la communication entre eux par ce réseau. Si un site Internet est consulté, l'adresse IP de l'ordinateur appelant est communiquée au serveur sur lequel le site consulté est hébergé. Cette communication est nécessaire pour que les données consultées puissent être transférées au bon destinataire.

16 Par ailleurs, il ressort de la décision de renvoi et du dossier dont dispose la Cour que les ordinateurs des utilisateurs d'Internet se voient conférer par les fournisseurs d'accès à Internet **soit une adresse IP « statique », soit une adresse IP « dynamique »**, à savoir une adresse IP qui change à l'occasion de chaque nouvelle connexion à Internet. À la différence des adresses IP statiques, les adresses IP dynamiques ne permettraient pas de faire le lien, au moyen de fichiers accessibles au public, entre un ordinateur donné et le branchement physique au réseau utilisé par le fournisseur d'accès à Internet.

44 **Le fait que les informations supplémentaires nécessaires pour identifier l'utilisateur d'un site Internet sont détenues non pas par le fournisseur de services de médias en ligne, mais par le fournisseur d'accès à Internet de cet utilisateur, n'apparaît ainsi pas de nature à exclure que les adresses IP dynamiques enregistrées par le fournisseur de services de médias en ligne constituent, pour celui-ci, des données à caractère personnel au sens de l'article 2, sous a), de la directive 95/46.**

47 Or, si la juridiction de renvoi précise dans sa décision de renvoi que le droit allemand ne permet pas au fournisseur d'accès à Internet de transmettre directement au fournisseur de services de médias en ligne les informations supplémentaires, nécessaires à l'identification de la personne concernée, il semble toutefois, sous réserve des vérifications à effectuer à cet égard par cette juridiction, qu'il existe des voies légales permettant au fournisseur de services de médias en ligne de s'adresser, notamment en cas d'attaques cybernétiques, à l'autorité compétente afin que celle-ci entreprenne les démarches nécessaires pour obtenir ces informations auprès du fournisseur d'accès à Internet et pour déclencher des poursuites pénales.

48 Il semble ainsi que le fournisseur de services de médias en ligne dispose de **moyens susceptibles d'être raisonnablement mis en œuvre afin de faire identifier, à l'aide d'autres personnes, à savoir l'autorité compétente et le fournisseur d'accès à Internet, la personne concernée sur la base des adresses IP conservées.**

49 Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la première question que l'article 2, sous a), de la directive 95/46 doit être interprété en ce sens qu'une adresse IP dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne.

EN PRATIQUE

Option 1: Nom : M. Martin

Option 2 : Nom : Ban Tran

Option 1 : Ville de résidence : Paris

Option 2: Ville de résidence : La chapelle Baloue

Option 1 : Date de naissance : 01/02/1989

Option 2 : tranche d'âge : entre 30 et 40 ans

Option 1 : Nationalité : française

Option 2 : Nationalité : américaine (resident en France)

Profession : responsable ressources humaines

Option 1 : Groupe de 15.000 collaborateurs

Option 2: PME de 50 personnes à Libourne

Numéro de matricule : 13245

Entreprise : CNAM Paris



TRAITEMENT/ FICHIER

- 2) «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;
- 6) «fichier», tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

CJUE Grande Chambre 13 mai 2014 Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja G.
→ **lecture (&21-31)**

RESPONSABLE DU TRAITEMENT

V. SOUS-TRAITANT

- 7) «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;
- 8) «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

Sous-traitant v. prestataire

CJUE Grande Chambre 13 mai 2014 Google Spain SL, Google Inc. / Agencia Española de Protección de Datos (AEPD), Mario Costeja G.
→ lecture (&32-41)

INDICES

Indices	Le prestataire pourra être qualifié de sous-traitant	Le prestataire pourra être qualifié de responsable de traitement
Transparence : Le prestataire de service se présente-t-il sous son nom propre ou sous le nom de son client ?	L'employé du centre d'appel en Tunisie se présente sous le nom du client.	Le centre d'appel en Tunisie se présente sous son propre nom.
Niveau d'instruction : Le niveau d'instruction donné par le client indique le degré d'autonomie laissé au prestataire. Par conséquent, il permet d'apprécier s'il est plus qu'un simple sous-traitant.	Le contrat de prestation et les directives données au cours de son exécution sont très précis dans les instructions et le niveau de qualité demandé.	Le contrat de prestation et les directives données au cours de l'exécution sont très généraux en termes d'instruction et laissent expressément une grande autonomie au prestataire.
Niveau de contrôle : Le degré de contrôle du client sur les prestations et sur les données révèle également la liberté dont peut disposer le prestataire.	La société audite son prestataire et lui demande des comptes régulièrement.	La société ne s'intéresse pas à la façon dont le prestataire réalise ses prestations et le laisse libre d'utiliser les données comme bon lui semble.
Expertise : Un prestataire qui dispose d'une expertise peut ainsi décider des moyens à mettre en place dans le cadre de la réalisation des prestations.	Le prestataire utilise l'infrastructure technique du client pour réaliser sa prestation.	Le prestataire expert dans son domaine impose des outils au client qui n'a pas de pouvoir de négociation, ne peut les modifier parce qu'il n'a pas les compétences, ou parce que l'outil est un outil qui ne fait pas l'objet d'un développement spécifique.

Source CNIL

CHECKLISTS ICO

The following checklists set out indicators as to whether you are a controller, a processor or a joint controller. The more boxes you tick, the more likely you are to fall within the relevant category.

Are we a processor?

- We are following instructions from someone else regarding the processing of personal data.
- We were given the personal data by a customer or similar third party, or told what data to collect.
- We do not decide to collect personal data from individuals.
- We do not decide what personal data should be collected from individuals.
- We do not decide the lawful basis for the use of that data.
- We do not decide what purpose or purposes the data will be used for.
- We do not decide whether to disclose the data, or to whom.
- We do not decide how long to retain the data.
- We may make some decisions on how data is processed, but implement these decisions under a contract with someone else.
- We are not interested in the end result of the processing.



CO-RESPONSABILITÉ

Article 26

Responsables conjoints du traitement

1. Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. Un point de contact pour les personnes concernées peut être désigné dans l'accord.
2. L'accord visé au paragraphe 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.
3. Indépendamment des termes de l'accord visé au paragraphe 1, la personne concernée peut exercer les droits que lui confère le présent règlement à l'égard de et contre chacun des responsables du traitement.

- 36 Dans ce cadre, il ressort des indications soumises à la Cour que la création d'une page fan sur Facebook implique de la part de son administrateur une action de paramétrage, en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, qui influe sur le traitement de données à caractère personnel aux fins de l'établissement des statistiques établies à partir des visites de la page fan. Cet administrateur peut, à l'aide de filtres mis à sa disposition par Facebook, définir les critères à partir desquels ces statistiques doivent être établies et même désigner les catégories de personnes qui vont faire l'objet de l'exploitation de leurs données à caractère personnel par Facebook. Par conséquent, l'administrateur d'une page fan hébergée sur Facebook contribue au traitement des données à caractère personnel des visiteurs de sa page.
- 37 En particulier, l'administrateur de la page fan peut demander à obtenir – et donc que soient traitées – des données démographiques concernant son audience cible, notamment des tendances en matière d'âge, de sexe, de situation amoureuse et de profession, des informations sur le style de vie et les centres d'intérêt de son audience cible ainsi que des informations concernant les achats et le comportement d'achat en ligne des visiteurs de sa page, les catégories de produits ou de services qui l'intéressent le plus, de même que des données géographiques qui permettent à l'administrateur de la page fan de savoir où effectuer des promotions spéciales ou organiser des événements et, de manière plus générale, de cibler au mieux son offre d'informations.
- 38 S'il est vrai que les statistiques d'audience établies par Facebook sont uniquement transmises à l'administrateur de la page fan sous une forme anonymisée, il n'en demeure pas moins que l'établissement de ces statistiques repose sur la collecte préalable, au moyen de cookies installés par Facebook sur l'ordinateur ou sur tout autre appareil des personnes ayant visité cette page, et le traitement des données personnelles de ces visiteurs à de telles fins statistiques. En tout état de cause, la directive 95/46 n'exige pas, lorsqu'il y a une responsabilité conjointe de plusieurs opérateurs pour un même traitement, que chacun ait accès aux données à caractère personnel concernées.
- 39 Dans ces circonstances, il y a lieu de considérer que l'administrateur d'une page fan hébergée sur Facebook, tel que Wirtschaftsakademie, participe, par son action de paramétrage, en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page fan. De ce fait, cet administrateur doit être, en l'occurrence, qualifié de responsable au sein de l'Union, conjointement avec Facebook Ireland, de ce traitement, au sens de l'article 2, sous d), de la directive 95/46.
- 40 En effet, le fait pour un administrateur d'une page fan d'utiliser la plateforme mise en place par Facebook, afin de bénéficier des services y afférents, ne saurait l'exonérer du respect de ses obligations en matière de protection des données à caractère personnel.
- 41 Au demeurant, il importe de souligner que les pages fan hébergées sur Facebook peuvent être visitées également par des personnes qui ne sont pas utilisateurs de Facebook et qui ne disposent donc pas d'un compte utilisateur sur ce réseau social. Dans ce cas, la responsabilité de l'administrateur de la page fan à l'égard du traitement des données à caractère personnel de ces personnes apparaît encore plus importante, car la simple consultation de la page fan par des visiteurs déclenche automatiquement le traitement de leurs données à caractère personnel.
- 42 Dans ces conditions, la reconnaissance d'une responsabilité conjointe de l'exploitant du réseau social et de l'administrateur d'une page fan hébergée sur ce réseau en relation avec le traitement des données personnelles des visiteurs de cette page fan contribue à assurer une protection plus complète des droits dont disposent les personnes qui visitent une page fan, conformément aux exigences de la directive 95/46.
- 43 Cela étant, il y a lieu de préciser, ainsi que l'a relevé M. l'avocat général aux points 75 et 76 de ses conclusions, que l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel. Au contraire, ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce.
- 44 Au regard des considérations qui précèdent, il y a lieu de répondre aux première et deuxième questions que l'article 2, sous d), de la directive 95/46 doit être interprété en ce sens que la notion de « responsable du traitement », au sens de cette disposition, englobe l'administrateur d'une page fan hébergée sur un réseau social.

Arrêt CJUE « Wirtschaftsakademie » du 5 juin 2018

DESTINATAIRE V. TIERS

- 9) «destinataire», la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;
- 10) «tiers», une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;



CHAMP D'APPLICATION TERRITORIALE

Article 3

Champ d'application territorial

1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.
2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:
 - a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
 - b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.
3. Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.

Guidelines 3/2018 sur le champ territorial (version 2.1)

L'ÉTABLISSEMENT

- (22) Tout traitement de données à caractère personnel qui a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union devrait être effectué conformément au présent règlement, que le traitement lui-même ait lieu ou non dans l'Union. L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

Jurisprudence

- le traitement de données n'a pas besoin d'être effectué par l'établissement lui-même mais uniquement dans le cadre des activités de celui-ci (CJUE 13 mai 2014, aff. C-131/12)
 - lecture (& 45-60)
- la présence d'un seul représentant dans un État membre peut, dans certaines circonstances, constituer un établissement stable (CJUE 1^{er} oct. 2015, aff. C-230/14, Weltimmo)

CRITÈRE DE RATTACHEMENT AU LIEU DE SITUATION DES PERSONNES CONCERNÉES

Activité de traitement liée à l'offre de biens ou de services

- (23) Afin de garantir qu'une personne physique ne soit pas exclue de la protection à laquelle elle a droit en vertu du présent règlement, le traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait être soumis au présent règlement lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non. Afin de déterminer si un tel responsable du traitement ou sous-traitant offre des biens ou des services à des personnes concernées qui se trouvent dans l'Union, il y a lieu d'établir s'il est clair que le responsable du traitement ou le sous-traitant envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union. Alors que la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union, peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'Union.

CRITÈRE DE RATTACHEMENT AU LIEU DE SITUATION DES PERSONNES CONCERNÉES

Activité de traitement lié au suivi du comportement

- (24) Le traitement de données à caractère personnel de personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait également être soumis au présent règlement lorsque ledit traitement est lié au suivi du comportement de ces personnes dans la mesure où il s'agit de leur comportement au sein de l'Union. Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.

ART.4 : Définition

- 4) «profilage», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

LIL III

Art. 3.-I.-Sans préjudice, en ce qui concerne les traitements entrant dans le champ du règlement (UE) 2016/679 du 27 avril 2016, des critères prévus par l'article 3 de ce règlement, l'ensemble des dispositions de la présente loi s'appliquent aux traitements des données à caractère personnel effectués dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire français, que le traitement ait lieu ou non en France.

II.- Les règles nationales prises sur le fondement des dispositions du même règlement renvoyant au droit national le soin d'adapter ou de compléter les droits et obligations prévus par ce règlement s'appliquent dès lors que la **personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France.**

Toutefois, lorsque est en cause un des traitements mentionnés au 2 de l'article 85 du même règlement, les règles nationales mentionnées au premier alinéa du II sont celles dont relève le responsable de traitement, lorsqu'il est établi dans l'Union européenne.

CRITÈRE DE RATTACHEMENT AU LIEU OÙ LE DROIT D'UN ÉTAT MEMBRE S'APPLIQUE EN VERTU DU DROIT INTERNATIONAL PUBLIC

- (25) Lorsque le droit d'un État membre s'applique en vertu du droit international public, le présent règlement devrait s'appliquer également à un responsable du traitement qui n'est pas établi dans l'Union, par exemple qui se trouve auprès de la représentation diplomatique ou consulaire d'un État membre.

EN PRATIQUE

1. Une société chinoise d'e-commerce dont les opérations sont réalisées en Chine ouvre un bureau à Berlin pour réaliser des campagnes de prospection commerciale et de marketing en Europe.
2. Un hôtel en Afrique du Sud propose des offres dans diverses langues (français, espagnol etc.). La société n'a pas de bureau en France.
3. Une entreprise française propose des services de covoiturage au Moyen-Orient. Aucun service en Europe proposé. Toutes les données sont traitées en France.
4. Une entreprise de marketing américaine analyse pour le compte d'un centre commercial français les passages des clients via un suivi wifi.

LE REPRÉSENTANT AU SEIN DE L'UE

ART.4 : Définition

- 17) «représentant», une personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du présent règlement;

Article 27

Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union

1. Lorsque l'article 3, paragraphe 2, s'applique, le responsable du traitement ou le sous-traitant désigne par écrit un représentant dans l'Union.

2. L'obligation prévue au paragraphe 1 du présent article ne s'applique pas:

a) à un traitement qui est occasionnel, qui n'implique pas un traitement à grande échelle des catégories particulières de données visées à l'article 9, paragraphe 1, ou un traitement de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10, et qui n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement; ou

b) à une autorité publique ou à un organisme public;

3. Le représentant est établi dans un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi.

4. Le représentant est mandaté par le responsable du traitement ou le sous-traitant pour être la personne à qui, notamment, les autorités de contrôle et les personnes concernées doivent s'adresser, en plus ou à la place du responsable du traitement ou du sous-traitant, pour toutes les questions relatives au traitement, aux fins d'assurer le respect du présent règlement.

5. La désignation d'un représentant par le responsable du traitement ou le sous-traitant est sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement ou le sous-traitant lui-même.

LE GUICHET UNIQUE

- (124) Lorsque le traitement des données à caractère personnel a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant dans l'Union et que ce responsable du traitement ou ce sous-traitant est établi dans plusieurs États membres, ou que le traitement qui a lieu dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant dans l'Union affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres, l'autorité de contrôle dont relève l'établissement principal ou l'établissement unique du responsable du traitement ou du sous-traitant devrait faire office d'autorité chef de file. Elle devrait coopérer avec les autres autorités concernées dans le cas où le responsable du traitement ou le sous-traitant a un établissement sur le territoire de l'État membre dont elles relèvent, dans le cas où les personnes concernées résidant sur le territoire dont elles relèvent sont affectées sensiblement ou encore dans le cas où une réclamation leur a été adressée. En outre, lorsqu'une personne concernée ne résidant pas dans cet État membre a introduit une réclamation, l'autorité de contrôle auprès de laquelle celle-ci a été introduite devrait également être une autorité de contrôle concernée. Dans le cadre de ses missions liées à la publication de lignes directrices sur toute question portant sur l'application du présent règlement, le comité devrait pouvoir publier des lignes directrices portant, en particulier, sur les critères à prendre en compte afin de déterminer si le traitement en question affecte sensiblement des personnes concernées dans plusieurs États membres et sur ce qui constitue une objection pertinente et motivée.

Article 56

Compétence de l'autorité de contrôle chef de file

1. Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60.

Considérants 36/ 37

ART.4 : Définition

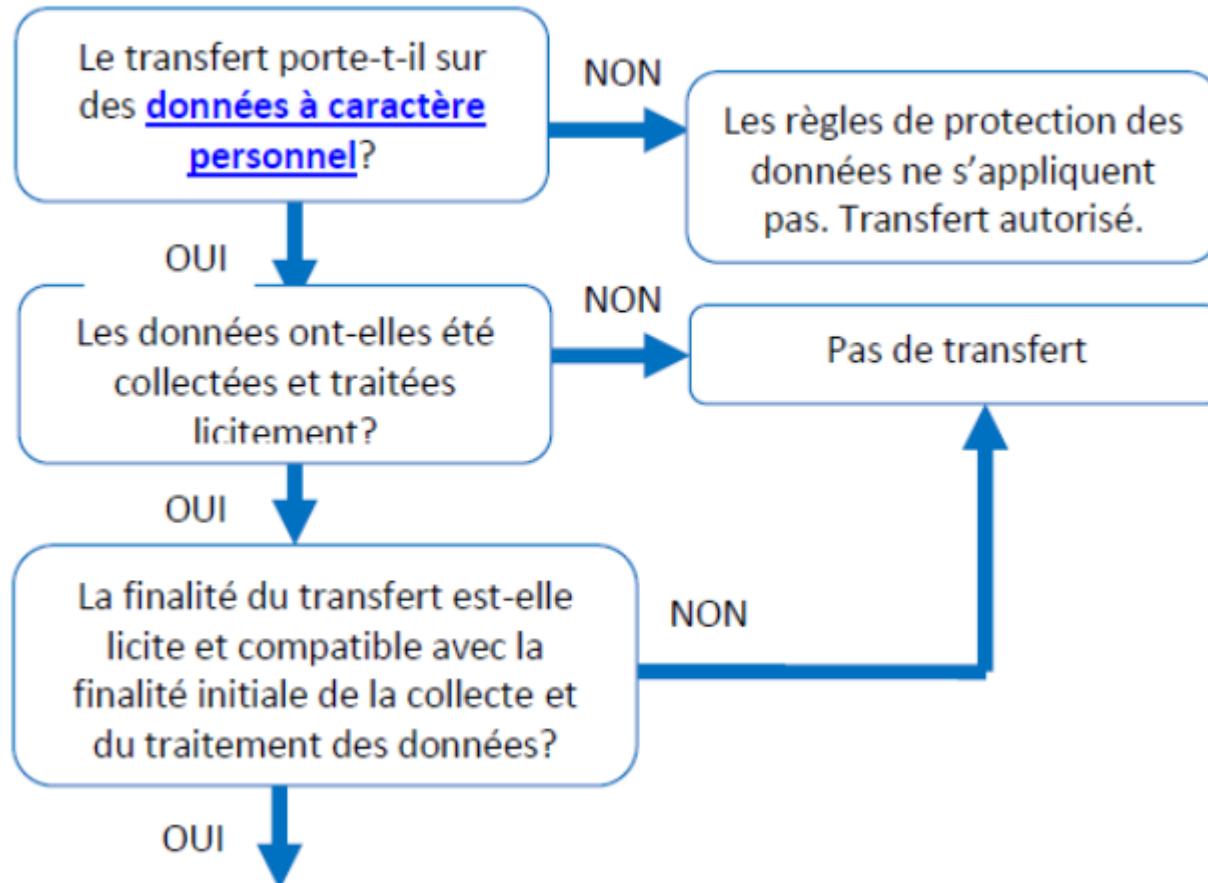
16) «établissement principal»;

- a) en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal;
- b) en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement;

TRANSFERTS DE DONNÉES HORS UE

(116) Lorsque des données à caractère personnel franchissent les frontières extérieures de l'Union, cela peut accroître le risque que les personnes physiques ne puissent exercer leurs droits liés à la protection des données, notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations. De même, les autorités de contrôle peuvent être confrontées à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées en dehors de leurs frontières. Leurs efforts pour collaborer dans le contexte transfrontalier peuvent également être freinés par les pouvoirs insuffisants dont elles disposent en matière de prévention ou de recours, par l'hétérogénéité des régimes juridiques et par des obstacles pratiques tels que le manque de ressources. En conséquence, il est nécessaire de favoriser une coopération plus étroite entre les autorités de contrôle de la protection des données, pour les aider à échanger des informations et mener des enquêtes avec leurs homologues internationaux. Aux fins d'élaborer des mécanismes de coopération internationale destinés à faciliter et à mettre en place une assistance mutuelle internationale pour faire appliquer la législation relative à la protection des données à caractère personnel, la Commission et les autorités de contrôle devraient échanger des informations et coopérer dans le cadre d'activités liées à l'exercice de leurs compétences avec les autorités compétentes dans les pays tiers, sur une base réciproque et conformément au présent règlement.

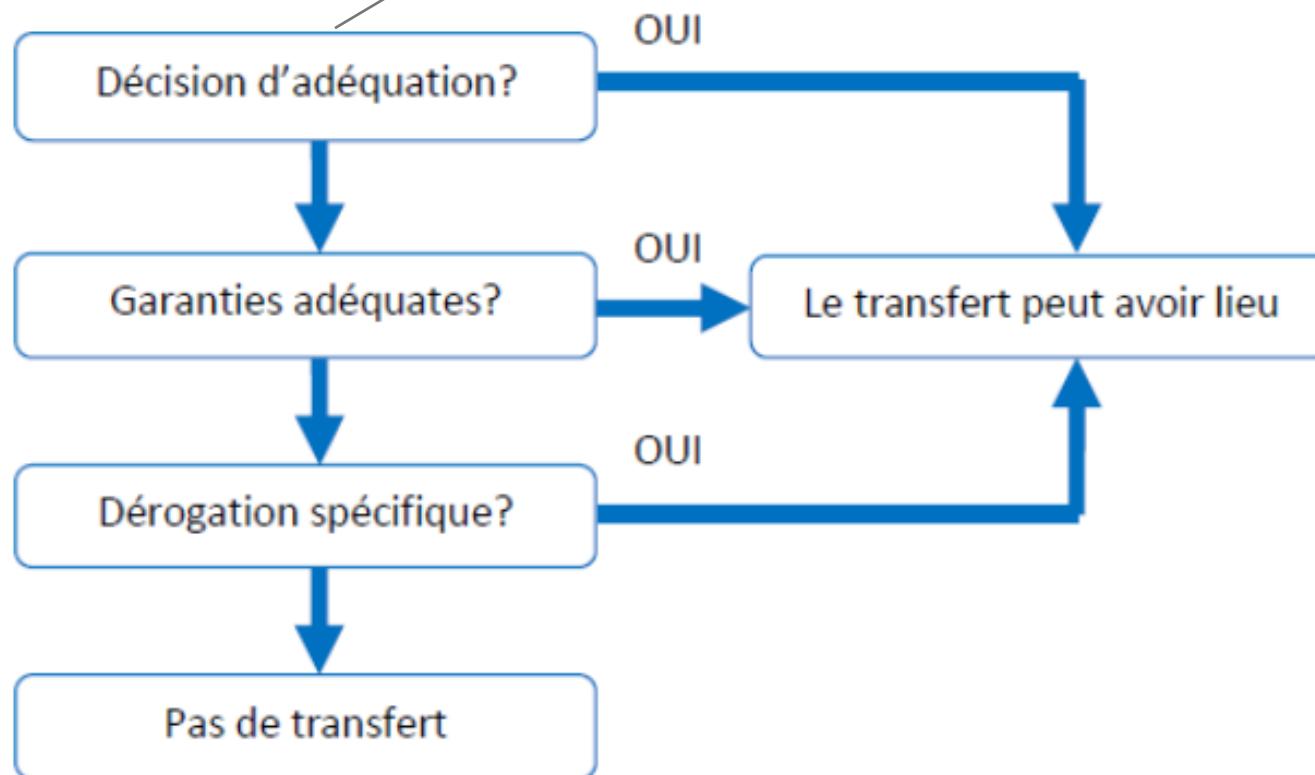
Étape n° 1:



Source : EDPS

Andorre, Argentine, Canada (commercial organisations),
Faroe Islands, Guernsey, Israel, Isle of Man, Japon, Jersey,
Nouvelle Zélande Switzerland, Uruguay

Étape n° 2:



Source : EDPS

Le Privacy shield

Il est possible de se référer au Privacy Shield pour transférer des données personnelles vers les USA, à condition que les entreprises destinataires des données soient référencées et respectent les obligations et les garanties de fond ...

[> Qu'est-ce que le Privacy Shield ?](#)

Les Clauses Contractuelles Types de la Commission Européenne

Les Clauses Contractuelles Types sont des modèles de contrats de transfert de données personnelles adoptés par la Commission européenne. Les modèles de clauses contractuelles types sont toujours d'actualité et peuvent être ...

[> Que sont les CCT ?](#)

Les règles d'entreprise contraignantes (BCR)

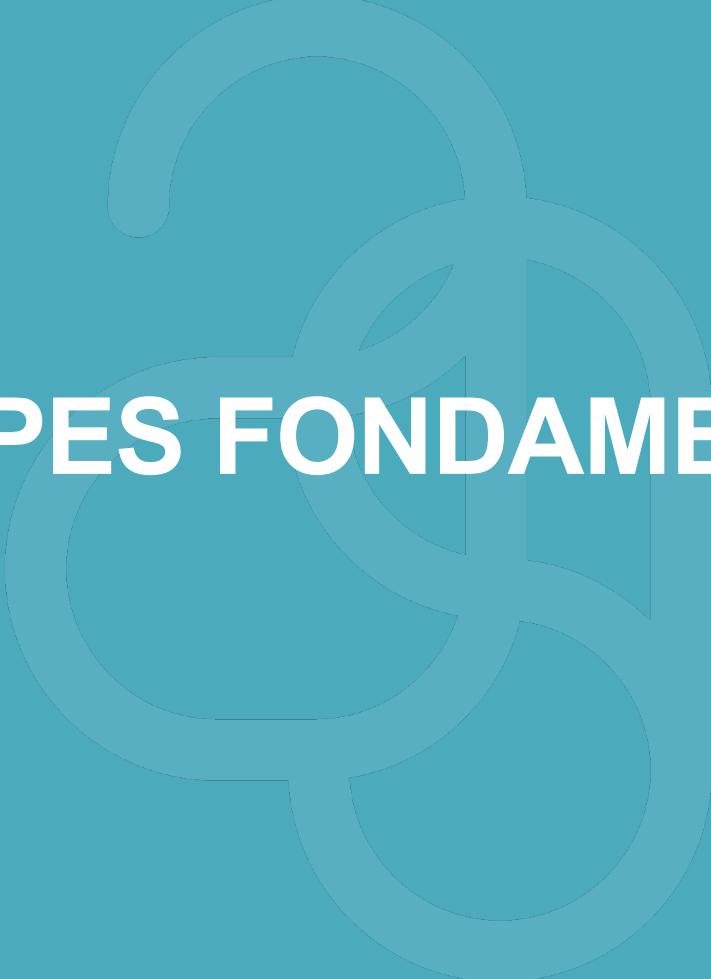
Les Binding Corporate Rules (BCR) constituent un code de conduite, définissant la politique d'une entreprise en matière de transferts de données personnelles. Elles permettent d'offrir une protection adéquate aux données transférées.

[> Que sont les BCR ?](#)

Les dérogations pour des situations particulières

Certaines dérogations au principe d'encadrement général des transferts vers un Etat non membre de l'Union sont prévues par l'article 49 du RGPD. Ces exceptions ne peuvent être mobilisées que dans des situations particulières.

[> Que sont ces dérogations ?](#)



PRINCIPES FONDAMENTAUX

Principes

Article 5

Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être:

- a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);
- b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);
- c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
- d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);
- e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);
- f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

1. LE PRINCIPE DE FINALITÉ ET DE PROPORTIONNALITÉ

- Pourquoi je collecte des données?
- Quelle est la raison pour laquelle je vais traiter ces données?
- Est-ce pertinent?
 - ❖ Finalité secondaire

Mise en demeure de cinq sociétés d'assurance pour détournement de finalité des données des assurés

18 octobre 2018

La Présidente de la CNIL met en demeure des sociétés des groupes HUMANIS et MALAKOFF-MÉDÉRIC de cesser d'utiliser pour de la prospection commerciale des données personnelles collectées exclusivement afin de payer les allocations retraite.

Clôture de la mise en demeure : février 2019

Les nombreux échanges entre la Commission et les groupes concernés ont permis de considérer que le manquement avait cessé, ce qui a été confirmé à l'occasion d'un nouveau contrôle sur place.

En effet, les sociétés ont modifié leur système informatique afin que les données en lien avec la retraite ne soient plus connues ni utilisées par les services en charge de l'assurance. Elles ont, en outre, supprimé l'intégralité des données illégalement acquises par ce biais. La CNIL a constaté que les données sont aujourd'hui traitées conformément aux règles applicables.

Enfin, les sociétés ont mis en place un programme de formation de leurs équipes afin de les sensibiliser à l'utilisation des données à caractère personnel de leurs clients.



LA PROPORTIONNALITÉ

Est-ce que je ne collecte que les données nécessaires? (minimisation)

- **Données sensibles**
- **Bloc notes / zones commentaires**

CLIENT TRES AGRESSIF , N'A PAS DE CERVEAU , LE CLIENT EST CHIANT , CLIENT TRES CON , LA CLIENTE EST UNE GROSSE CONNASSE QUI SE CROIT TOUT PERMIS , CLIENT CASSE COUILLE , FOLLE , FORT ACCENT AFRICAIN , CLIENTE DE CONFESSTION JUIVE , CLIENTE AVEC PROBLEME CARDIAQUE , CLIENTE A UNE MALADIE NEUROLOGIQUE , CLIENT ALCOOLIQUE , ME PASSE SON MARI ATTEINT DE PARKINSON , CLIENT C'EST FAIT OPERE DUNE HERNIE DISCAL IL Y A 3 MOIS .

Décision n°2015-063 du 26 juin 2015 (mise en demeure)

LA PROPORTIONNALITÉ

La reconnaissance faciale dans les lycées :

Après un examen attentif du projet, la CNIL a considéré que le dispositif projeté est contraire aux grands principes de proportionnalité et de minimisation des données posés par le RGPD (Règlement général sur la protection des données).

En effet, les objectifs de sécurisation et la fluidification des entrées dans ces lycées peuvent être atteints par des moyens bien moins intrusifs en termes de vie privée et de libertés individuelles, comme par exemple un contrôle par badge.

<https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>



2. LA BASE LÉGALE

Article 6

Licéité du traitement

1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:
 - a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
 - b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
 - c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
 - d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
 - e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
 - f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.



La CNIL propose des fiches pratiques à destination des professionnels qui peuvent les aider à comprendre les bases légales et à choisir celles qui seront les plus adaptées à leurs traitements de données.

Ouiii !

Consentement



Obligation légale



Contrat



Mission
d'intérêt public



Sauvegarde
des intérêts vitaux



Intérêt légitime

EN PRATIQUE... POUR LA CNIL

A titre général, la CNIL a suivi le raisonnement suivant :

1. La CNIL met en œuvre de nombreux traitements « métier », tournés vers ses usagers et nécessaires à l'exécution de ses missions telles que définies par les textes applicables. **Elle choisit donc la base légale de la mission d'intérêt public pour fonder ces traitements.**
2. D'autres traitements mis en œuvre ne sont pas directement nécessaires à l'exercice de ces missions d'intérêt public mais sont rendus obligatoires par différentes lois applicables dans le cadre de son activité (par exemple, certains traitements liés à la gestion administrative de ses personnels). **L'obligation légale est retenue pour ces traitements.**
3. Certains traitements sont sans rapport particulier avec les spécificités des missions d'intérêt public confiées à la CNIL et ne sont pas imposés par des dispositions légales, même s'ils sont mis en œuvre dans le cadre de ses missions (par exemple, certains traitements de gestion documentaire ou d'information interne). Dès lors qu'ils respectent certaines conditions, **un intérêt légitime de la CNIL peut en constituer la base légale.**
4. Pour un traitement bien particulier, la CNIL se fonde enfin sur la base légale du **contrat**.
5. En revanche, la CNIL ne fonde aucun de ses traitements sur la sauvegarde des intérêts vitaux ni sur le **consentement**, quand bien même les données sont collectées avec l'accord des personnes concernées.

LE CAS PARTICULIER DU CONSENTEMENT

- 11) «consentement» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

Article 7

Conditions applicables au consentement

1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.
3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.
4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

LES SUBTILITÉS DU CONSENTEMENT

- WP 259 sur le consentement (2018)
 - Libre
 - Spécifique
 - Éclairé : Information (WP260 sur la transparence)
- Manifestation positive
- Distinction entre les manifestations de volonté (contrat/ essai clinique)
- Preuve du consentement

LE DÉSÉQUILIBRE DE POUVOIR

EXEMPLE : ESSAIS CLINIQUES

« Il convient de garder à l'esprit que, même si les conditions nécessaires à un consentement éclairé fixées par le règlement relatif aux essais cliniques sont réunies, une **situation claire de déséquilibre des pouvoirs entre le participant et le promoteur/l'investigateur impliquera que le consentement n'a pas été «donné librement» au sens du RGPD.**

À titre d'exemple, le comité considère que c'est le cas lorsqu'un participant n'est pas en bonne santé, lorsque des participants appartiennent à une catégorie défavorisée sur le plan économique ou social ou lorsqu'ils sont dans une situation de dépendance institutionnelle ou hiérarchique.

Par conséquent, et comme expliqué dans les lignes directrices du groupe de travail «Article29» sur le consentement, ce dernier ne constituera pas la base juridique appropriée dans la plupart des cas, et il faudra se fonder sur d'autres bases juridiques que le consentement (voir les autres bases juridiques possibles ci-dessous). Dès lors, le comité estime que les responsables du traitement des données devraient analyser les circonstances de l'essai clinique de manière particulièrement approfondie avant de se fonder sur le consentement des personnes comme base juridique pour le traitement de données à caractère personnel aux fins des activités de recherche dudit essai. »

Avis 3/2019 concernant les questions et réponses sur l'interaction entre le règlement relatif aux essais cliniques et le règlement général sur la protection des données (RGPD)[article70, paragraphe1, point b)]

LE DÉSÉQUILIBRE DE POUVOIR EXEMPLE : RECONNAISSANCE FACIALE DANS LES LYCÉES

« Il ressort des pièces du dossier que la région PACA a entendu justifier légalement le traitement de données biométriques en cause **par le consentement préalable** des lycéens concernés ou, dans le cas où ces derniers sont mineurs, par celui de leurs représentants légaux. En se bornant toutefois à prévoir que ce consentement serait recueilli par la seule signature d'un formulaire, alors que **le public visé se trouve dans une relation d'autorité à l'égard des responsables des établissements publics d'enseignement concernés**, la région ne justifie pas avoir prévue des garanties suffisantes afin d'obtenir des lycéens ou de leurs représentants légaux qu'ils donnent leur consentement à la collecte de leurs données personnelles de manière libre et éclairée. »

→ La délibération du conseil régional de Provence-Alpes-Côte d'Azur du 14 décembre 2018 est annulée en tant qu'elle a lancé l'expérimentation du dispositif de contrôle d'accès virtuel dans les lycées.

Tribunal administratif de Marseille N° 1901249 audience du 3 février 2020/ lu en audience publique le 27 février 2020

EN PRATIQUE

First name *

Last Name *

Email *

Confirm Email *

I agree to receive news from ██████████ *

I agree to receive news from █████XX█'s partners

How did you hear about █████XX█? *

I need an invoice

I accept the [terms of service](#) *

BACK

NEXT

EXEMPLE - COOKIE



Figure 1 - Le détail des finalités est disponible sous un bouton de déroulement que l'utilisateur peut activer sur le premier niveau d'information.



Figure 5 - Il est possible de proposer des boutons d'acceptation et de refus globaux via par exemple la présentation de boutons intitulés « tout accepter » et « tout refuser » mis en évidence de la même façon.

Projet de recommandation sur les modalités pratiques de recueil du consentement prévu par l'article 82 de la loi du 6 janvier 1978 modifiée, concernant les opérations d'accès ou d'inscription d'informations dans le terminal d'un utilisateur (recommandation « cookies et autres traceurs ») – soumis à consultation publique

LECTURE

Décision n° MED 2018-042 du 30 octobre 2018
mettant en demeure la société VECTAURY

Clôture de la décision n° MED-2018-042 du 30 octobre
2018 mettant en demeure la société VECTAURY

Article 8

Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information

1. Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.

L 119/38

FR

Journal officiel de l'Union européenne

4.5.2016

2. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.

3. Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.



LES ENFANTS

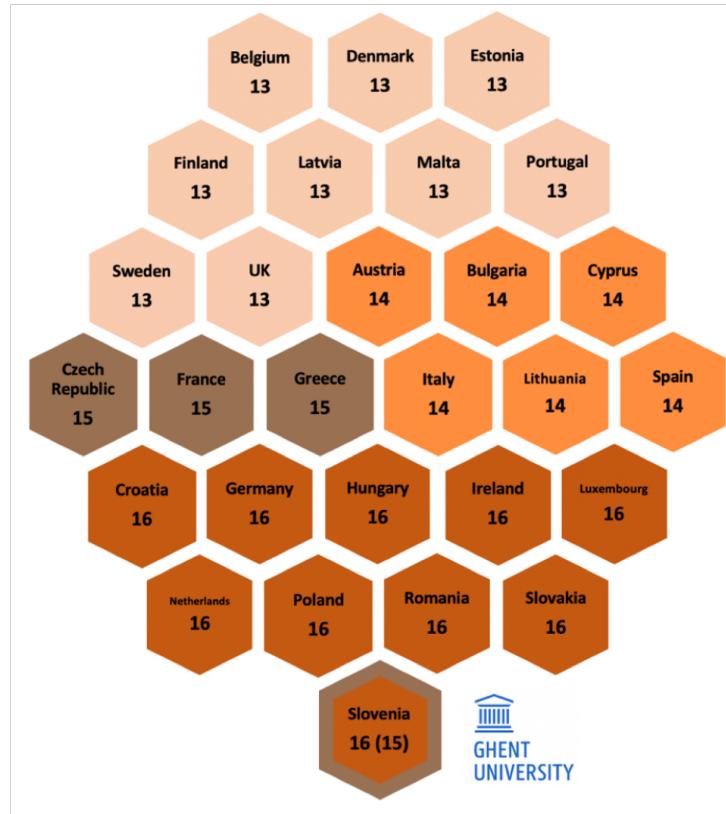
ART.4 : Définition

- 25) «service de la société de l'information», un service au sens de l'article 1^{er}, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil (¹);

Considérant

- (38) Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. Le consentement du titulaire de la responsabilité parentale ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant.

ÂGE EN EUROPE



L'ARTICULATION AVEC LES CATÉGORIES PARTICULIÈRES

Article 9

Traitement portant sur des catégories particulières de données à caractère personnel

1. 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 interdits.
2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie:
 - a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;
 - b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée;
 - c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;
 - d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées;

- f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle;
- g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée;
- h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;
- i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel;
- j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

3. Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.

4. Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé.

Article 10

Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions

Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

LILIII

Titre I Chapitre III NIR

Titre II Chapitre III Section 3 Traitements dans le domaine de la santé

EXEMPLE DES ESSAIS CLINIQUES

- Conditions de licéité du traitement afin de distinguer les activités de traitement liées à **la fiabilité et à la sécurité** pouvant découler directement d'**obligations légales** du responsable du traitement et qui relèvent de la condition de licéité de l'article6, paragraphe1, point c), lu conjointement avec l'article9,paragraphe1, point i), du RGPD.
- **Pour toutes les autres activités de traitement**, qualifiées dans le présent avis d'opérations de traitement purement liées aux activités de recherche, 3 conditions de licéité différentes possibles, en fonction de l'ensemble des circonstances liées à un essai clinique donné:
 - l'exécution d'une mission **d'intérêt public** au sens de l'article6, paragraphe1, pointe),lu conjointement avec l'article9, paragraphe2, points i) ou j), du RGPD;
 - ou **les intérêts légitimes** du responsable du traitement au sens de l'article6, paragraphe1,pointf), lu conjointement avec l'article9, paragraphe2, point j), du RGPD;
 - ou dans des **circonstances particulières**, lorsque toutes les conditions sont remplies, le **consentement explicite** de la personne concernée au sens de l'article6, paragraphe1, pointa),et de l'article9, paragraphe2, point a), du RGPD

Avis3/2019 concernant les questions et réponses sur l'interaction entre le règlement relatif aux essais cliniques et le règlement général sur la protection des données (RGPD)[article70, paragraphe1, point b)]

3. LA DURÉE DE CONSERVATION

Les bonnes questions à se poser (cf. CNIL)

- ✓ Jusqu'à quand ai-je vraiment besoin des données pour atteindre l'objectif fixé ?
- ✓ Ai-je des obligations légales de conserver les données pendant un certain temps ?
- ✓ Dois-je conserver certaines données en vue de me protéger contre un éventuel contentieux ? Lesquelles ?
- ✓ Jusqu'à quand puis-je faire valoir ce recours en justice ?
- ✓ Quelles informations doivent être archivées ? Pendant combien de temps ?
- ✓ Quelles sont les règles de suppression des données ?
- ✓ Quelles sont les règles d'archivage des données ?

Délibération du 11 octobre 2015 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel

EN PRATIQUE

Définir la durée de conservation :

- Pour la prospection commerciale
 - D'un commerce de détail
 - D'un vendeur de voiture de luxe
- Pour les données des collaborateurs / candidats

4. LA QUALITÉ DES DONNÉES

Mise à jour :

- Par le responsable du traitement
- Par la personne
 - À tout moment
 - Sur demande



Alexandra GUÉRIN-FRANÇOIS
Protection des données / RGPD
aguerin@agprivacy.com