claranet security

# Normes et référentiels existants


11 Janvier 2017

claranet
hosting | applications | networks

helping our customers
do amazing things

# Objectifs de ce cours

- Appréhender les différentes normes et référentiels

- Comprendre  et mesurer les contraintes légales

# PCI-DSS

claranet
hosting | applications | networks

helping our customers
do amazing things

# PCI-DSS

- **Payment Card Industry Data Security Standard**, créé en 2006 par les fournisseurs de cartes (visa, mastercard, American Express, Discover, JCB)

- Un référentiel de 229 mesures qui s'applique à tout entité qui **traite, stocke ou fait transiter** des **données bancaires**

| | | Data Element | Storage Permitted | Render Stored Data Unreadable per Requirement 3.4 |
|---|---|---|---|---|
| Account Data | Cardholder Data | Primary Account Number (PAN) | Yes | Yes |
| | | Cardholder Name | Yes | No |
| | | Service Code | Yes | No |
| | | Expiration Date | Yes | No |
| | Sensitive Authentication Data[2] | Full Track Data[3] | No | Cannot store per Requirement 3.2 |
| | | CAV2/CVC2/CVV2/CID[4] | No | Cannot store per Requirement 3.2 |
| | | PIN/PIN Block[5] | No | Cannot store per Requirement 3.2 |

# Données bancaires: c’est quoi?

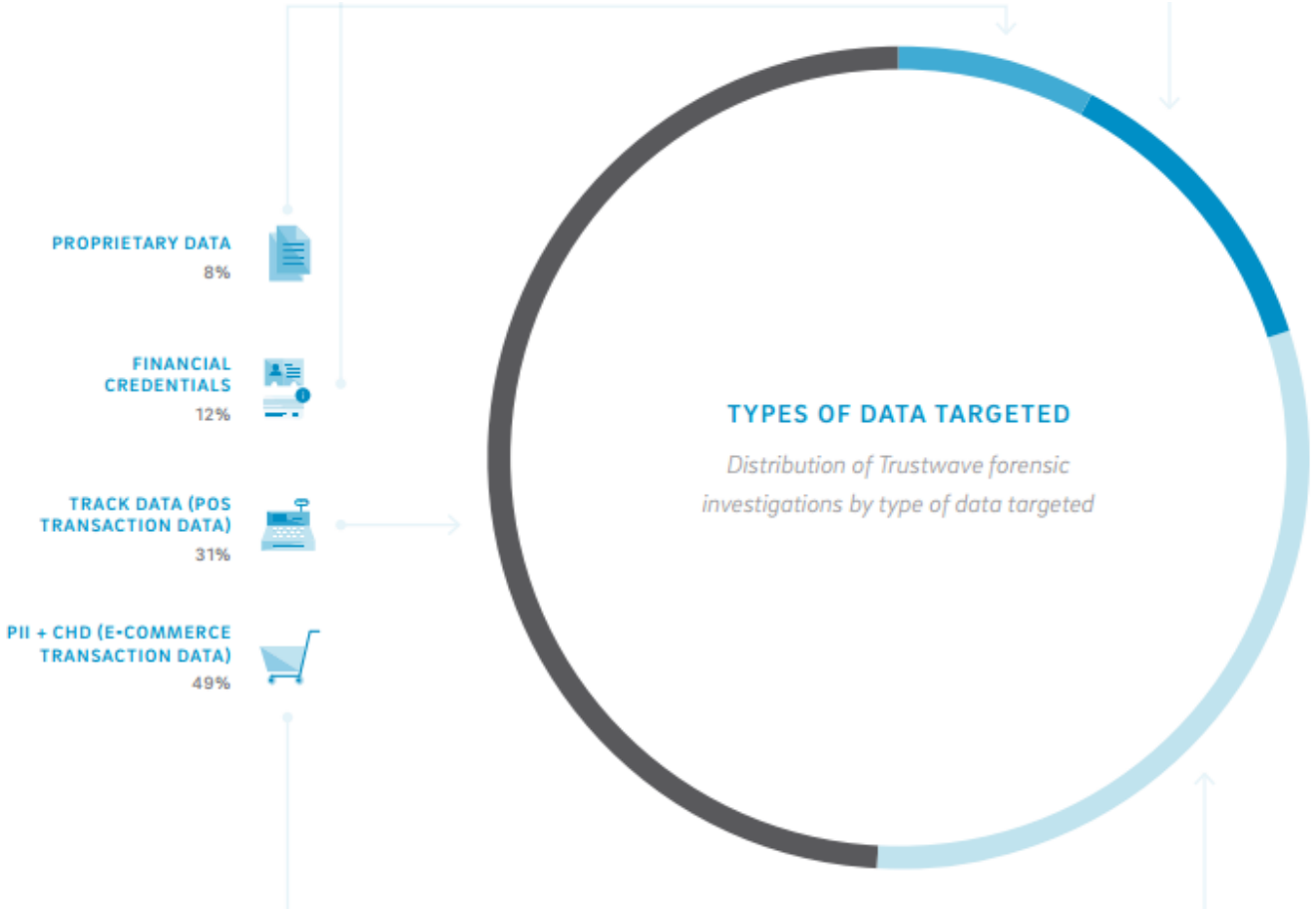
- 1 : PAN = Numéro de compte
- 2 : Nom du titulaire
- 3 : Code de service
- 4 : date d’expiration
- 5 : Données de bande magnétique

  ou puce (authentification)
- 6 : CVV ou Cryptogramme visuel
- 7 : Bloc PIN (version chiffrée du code PIN)

# Données bancaires: pourquoi les protéger ?

Données bancaires : une cible prisée par les cyber criminels

***(source : 2015 Trustwave Global Security Report – Verizon : 80% des attaques analysées)***




claranet
hosting | applications | networks

helping our customers do amazing things

# Données bancaires: pourquoi les protéger ?

- Une cible de choix qui est une belle source de revenus
  ***(Source : McAfee Labs)***

| Payment Card Number With CVV2 | United States | United Kingdom | Canada | Australia | European Union |
|---|---|---|---|---|---|
| Random | $5–$8 | $20–$25 | $20–$25 | $21–$25 | $25–$30 |
| With Bank ID Number | $15 | $25 | $25 | $25 | $30 |
| With Date of Birth | $15 | $30 | $30 | $30 | $35 |
| With Fullzinfo | $30 | $35 | $40 | $40 | $45 |

Estimated per card prices, in US$, for stolen payment card data (Visa, MasterCard, Amex, Discover).

Source: McAfee Labs.

# PCI-DSS: c’est quoi ?

- **229 mesures organisationnelles et techniques**

**PCI Data Security Standard – High Level Overview**

| | | |
|---|---|---|
| **Build and Maintain a Secure Network and Systems** | **1.** | Install and maintain a firewall configuration to protect cardholder data |
| | **2.** | Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | **3.** | Protect stored cardholder data |
| | **4.** | Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | **5.** | Protect all systems against malware and regularly update anti-virus software or programs |
| | **6.** | Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | **7.** | Restrict access to cardholder data by business need to know |
| | **8.** | Identify and authenticate access to system components |
| | **9.** | Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | **10.** | Track and monitor all access to network resources and cardholder data |
| | **11.** | Regularly test security systems and processes |
| **Maintain an Information Security Policy** | **12.** | Maintain a policy that addresses information security for all personnel |

# HIPAA & HaDS

claranet
hosting | applications | networks

helping our customers
do amazing things

# HIPAA & HaDS

- Le Health Insurance Portability and Accountability Act est une loi américaine de 1996 qui régit l'**utilisation**, le **stockage** et la **diffusion** de **données médicales personnelles**.

- La loi est applicable à toutes les entreprises ayant accès à de l'information sur la santé et particulièrement aux USA.

- Equivalent en France avec l'agrément de données de santés

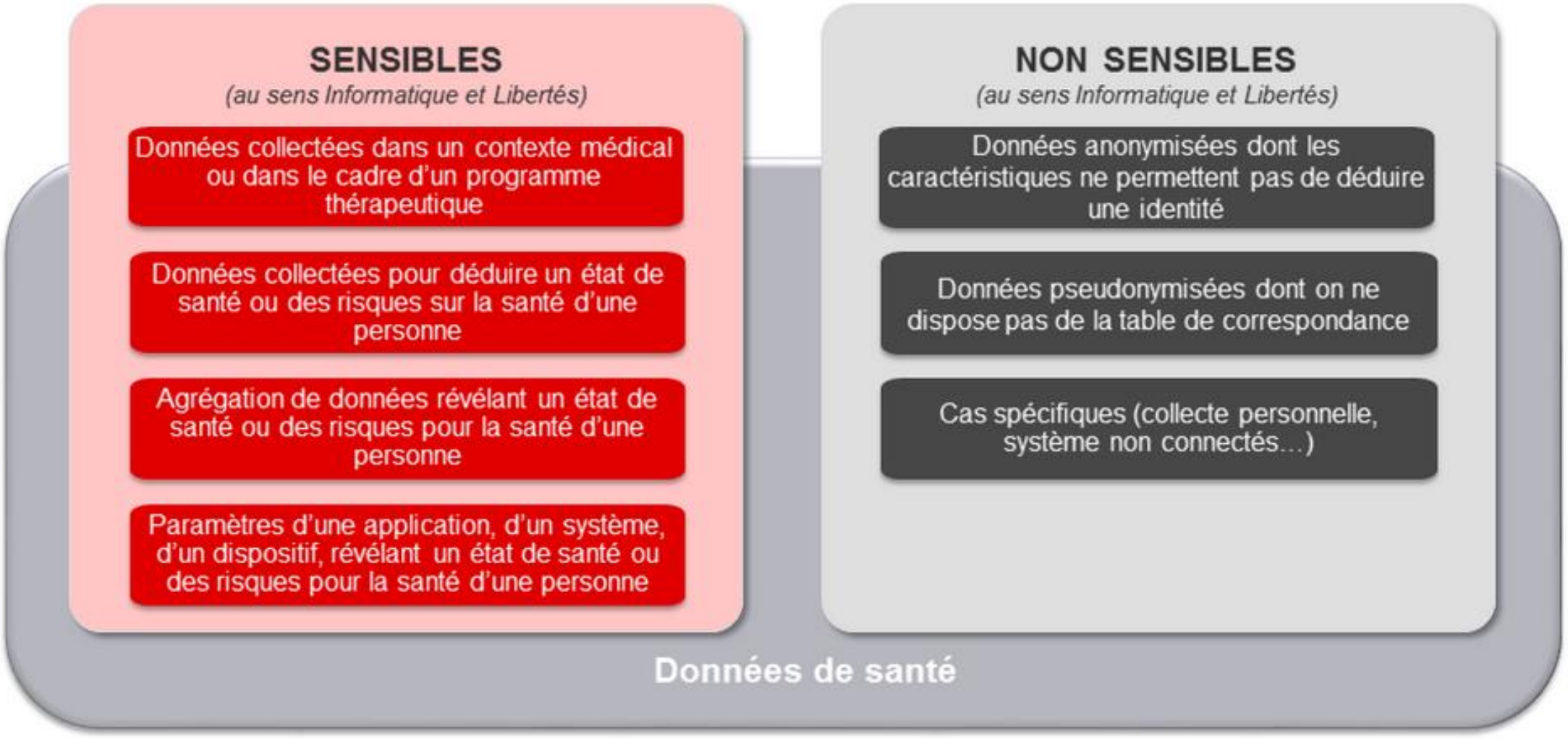
Qu’est ce que la donnée de santé ?

# Données de santé à caractère personnel

- *« Information relative à la santé d'une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »*

- *Toute information relative à la santé physique ou mentale d'une personne ou à la prestation de services de santé à cette personne. »*

# Sensibilité d'une donnée de santé



# Exemples de données de santé

| Donnée de santé | Non-sensibles | Sensibles |
|---|---|---|
| Dossier Médical Partagé (DMP) | | ✓ |
| Données sur les habitudes de fumeur ou de boisson | | ✓ |
| Statistiques médicales et hospitalières | ✓ | |
| Ordonnance / prescription de médicaments | | ✓ |
| Panier sur un site de e-pharmacie | ✓ | ✓ |

# Avez-vous vraiment compris ?


claranet
hosting | applications | networks

helping our customers
do amazing things

# Avez-vous compris ?

**Le poids est-il une donnée de santé sensible ?**


➔ Le **poids** ne représente pas une donnée de santé sensible : seule, cette donnée ne permet pas de déterminer un état de santé.



# Avez-vous compris ?

**Et qu'en est-il de l'association poids et taille ?**


➔ si vous **associez votre poids à d'autres informations** telle que la taille ou encore l'âge, alors **cet ensemble devient sensible** car il peut permettre de déterminer des facteurs de risque pour votre santé.

claranet
hosting | applications | networks
helping our customers do amazing things

# Avez-vous compris ?

**vos données de bien être sont-elles selon vous des données de santé ?**


➔ Toutes ces données : **sont personnelles car associées à votre nom.** Elles peuvent rapidement devenir **sensibles** car, suivies régulièrement ou **agrégées entres elles**, elles **peuvent révéler un état de santé** ou des risques concernant votre santé. Elles sont généralement hyper-connectées : stockées en ligne, partagées avec des professionnels de santé, sur les réseau sociaux, etc.



# HIPAA & HaDS


claranet
hosting | applications | networks

helping our customers do amazing things

# GDPR

claranet
hosting | applications | networks

helping our customers
do amazing things

# GDPR

- Le General Data Protection Regulation, est le nouveau règlement européen qui s'appliquera dès 2018 à toute entreprise qui **collecte**, **traite** et **stocke des données personnelles** dont l'utilisation peut directement ou indirectement identifier une personne.

- Il repose sur le droit fondamental inaliénable que constitue, pour chaque citoyen, la protection de sa vie privée et de ses données personnelles.

Qu’est ce que la donnée personnelle ?

# Données personnelles

- Art. 2 de la loi « Informatique et libertés »
- " Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ".
- " La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ".

# Données personnelles

- Une personne est identifiée lorsque par exemple son nom apparaît dans un fichier.

- Une personne est identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification (ex. : adresse IP, nom, n° d'immatriculation, n° de téléphone, photographie, éléments biométriques tels que l'empreinte digitale, ADN, numéro d'Identification Nationale Étudiant (INE), ensemble d'informations permettant de discriminer une personne au sein d'une population (certains fichiers statistiques) tels que, par exemple, le lieu de résidence et profession et sexe et âge,....).

# Données personnelles

- Des données que vous pourriez considérer comme anonymes peuvent constituer des données à caractère personnel si elles permettent d'identifier indirectement ou par recoupement d'informations une personne précise. Il peut en effet s'agir d'informations qui ne sont pas associées au nom d'une personne mais qui permettent aisément de l'identifier et de connaître ses habitudes ou ses goûts.

- En ce sens, constituent également des données à caractère personnel toutes les informations dont le recoupement permet d'identifier une personne précise. (ex. : une empreinte digitale, l'ADN, une date de naissance associée à une commune de résidence …).

- Les technologies de l'information et de la communication génèrent de nombreuses données personnelles (un appel passé par un téléphone portable, une connexion à Internet) et aussi des "traces informatiques" facilement exploitables grâce aux progrès des logiciels, notamment les moteurs de recherche.

# Exemples de données de données personnelles

**Sans contexte supplémentaire, existe-t-il des données personnelles parmi les déclarations suivantes ?**

« Le responsable de la société InTheCloud s'appelle Jean Dupond 

« C'est un homme brun, fils de notaire »

« La société WorldCompany vient de passer commande pour 50 000 € de boulons X35 type 32 »

« La fille du vétérinaire, installé avenue de Bretagne à Lille, est blonde et travaille dans le bar situé juste en face du cabinet de son père » 

# Avez-vous vraiment compris ?


claranet
hosting | applications | networks

helping our customers
do amazing things

# Avez-vous compris ?

**Une fiche de paye d'un employé, vis-à-vis d'un autre employé ?**


➔ Le 1er n'aura peut-être pas envie que le second sache quel est son salaire. C'est une donnée à caractère personnel.



# Avez-vous compris ?

## L'adresse IP est-elle une donnée à caractère personnel ?


➔ La CNIL considère qu'une adresse IP constitue une donnée à caractère personnel dès lors que celle-ci concerne des personnes physiques identifiées directement ou indirectement.

En effet, dans un communiqué en date du **2 août 2007**, elle relève que:
*"Cette analyse remet profondément en cause la notion de donnée à caractère personnel qui est très large. En effet, l'article 2 de la loi du 6 janvier 1978 modifiée en 2004 qui la définit, vise toute information relative à une personne physique qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à des éléments qui lui sont propres. Ce qui est le cas d'un numéro de plaque d'immatriculation de véhicule, d'un numéro de téléphone ou d'une adresse IP"*



# Un peu d'histoire..


claranet
hosting | applications | networks

helping our customers
do amazing things

# Le RGPD, ça change quoi ?

## Un règlement applicable à l'UE sans transposition

La déclinaison par chaque Etat Membre n'est plus possible. Certaines dispositions devront cependant être précisées par chacun.

## Un champ territorial étendu

Désormais une société établie en dehors de l'UE pourra être soumise au RGPD dès lors qu'elle offre des services ou des biens à des personnes concernées dans l'UE.

## Plus de responsabilités pour les sous-traitants

Désormais directement responsables de certaines dispositions, les sous-traitants pourront être sanctionnés par la CNIL et devront tenir un registre.

## Plus de données sensibles

La définition des données sensibles est élargie: on ajoute les données génétiques et biométriques. Leur traitement est, en principe, interdit.

## De nouveaux droits

Droit à la portabilité, à l'oubli, protection des mineurs, organiser le sort de ses données après sa mort, droit à la limitation.



## Accountability, LE principe à appliquer

Le régime déclaratif auprès de la CNIL est terminé, désormais les entreprises devront être capables de fournir la documentation, justifier leurs choix, tracer les actions et prouver leur conformité.

## Une ressource clé, le Data Protection Officer

Obligatoire pour les autorités/organismes publics et pour les responsables de traitements réalisés « à grande échelle » et leurs sous-traitants.

## Gestion par les risques via les Privacy Impact Assessments (PIA)

Les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés d'une personne devront faire l'objet d'une analyse d'impact. Si l'analyse confirme le risque élevé, la CNIL devra être consultée.

## Il faut notifier les violations de sécurité

Le responsable de traitement devra notifier les violations de sécurité à la CNIL dans les 72h. En cas de risque élevé, il notifie aussi les personnes concernées. Le sous-traitant notifie le responsable de traitement dans les meilleurs délais.

## Les sanctions sont plus lourdes

Une violation des obligations générales du responsable de traitement pourra couter 2% du CA annuel mondial d'une entreprise ou 10 millions d'euros (on retient le plus élevé), en cas de non respect d'une injonction, des principes de base d'un traitement, ou des transferts hors UE on « double la mise » (4% - 20 millions).

# Des obligations

- Les obligations du GDPR supposent qu'une entreprise doit à tout moment savoir de quelles données elle dispose, leur localisation, l'objectif de leur collecte et leur mode de gestion, stockage, sécurisation, transfert et effacement.

- Au-delà de cette quasi omniscience, elle doit être en mesure de déceler si leur intégrité a été compromise et y remédier promptement, tout en consignant et notifiant l'événement.

# Des sanctions

- En cas de non respect du règlement par les entreprises, des amendes allant ***jusqu'à 100 millions d'euros*** ou ***5% du chiffre d'affaire mondial*** pourront être appliquées.

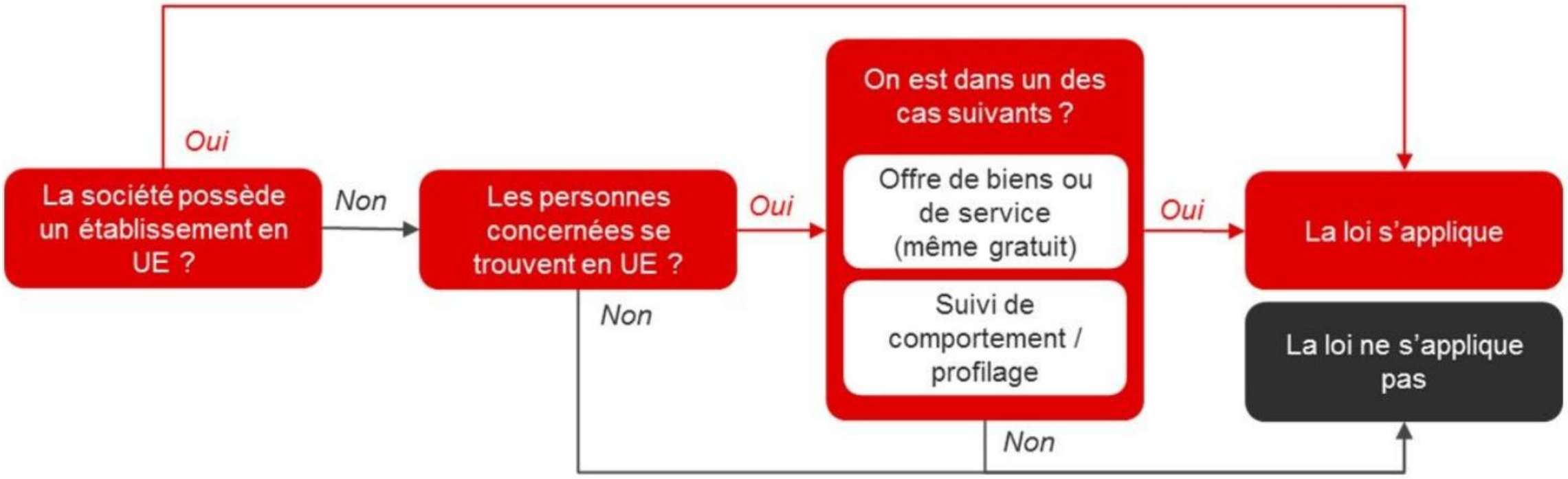
# Applicabilité du règlement

Une des **limites de la loi Informatique et libertés** aujourd'hui est **qu'elle s'applique aux entreprises** qui sont établies **en France** ou qui ont recours à des moyens de traitement en France. **Le RGPD** par contre, **s'appliquera** beaucoup **plus largement**.

Pour ne pas y être soumis, il faut :

- N'avoir aucune entité en UE
- Ne pas fournir un bien ou un service, même gratuitement à des personnes se trouvant en UE (pas des "européens" ! Des personnes sur le territoire de l'UE)
- Ne pas faire de profilage ou de suivi de comportement

# En résumé..




claranet
hosting | applications | networks

helping our customers
do amazing things

# CNIL

# CNIL

- « Dans l'univers numérique, la Commission Nationale de l'Informatique et des Libertés (CNIL) est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits. Elle analyse l'impact des innovations technologiques et des usages émergents sur la vie privée et les libertés. Enfin, elle travaille en étroite collaboration avec ses homologues européens et internationaux pour élaborer une régulation harmonisée. »

- La CNIL a été créée en 1978 avec la loi Informatique et Libertés.

- Il s'agit d'une autorité administrative indépendante.



CNIL.

# CNIL – ses missions

Informer les publics

Protéger les citoyens

Accompagner la conformité

Contrôler et sanctionner

Conseiller les pouvoirs publics

Agir au niveau européen

# Questions & Réponses