CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Le Règlement général sur la protection des données (RGPD)

Rencontres cybersécurité Bretagne – 07/06/2018

De quoi va-t-on parler ?

1. **La CNIL** : l'autorité administrative indépendante en charge de la protection des droits et libertés des personnes physiques contre les risques liés à leurs données depuis 1978

2. **Le Règlement général sur la protection des données (RGPD)** : le nouveau cadre qui harmonise la protection des données à caractère personnel dans l'Union européenne

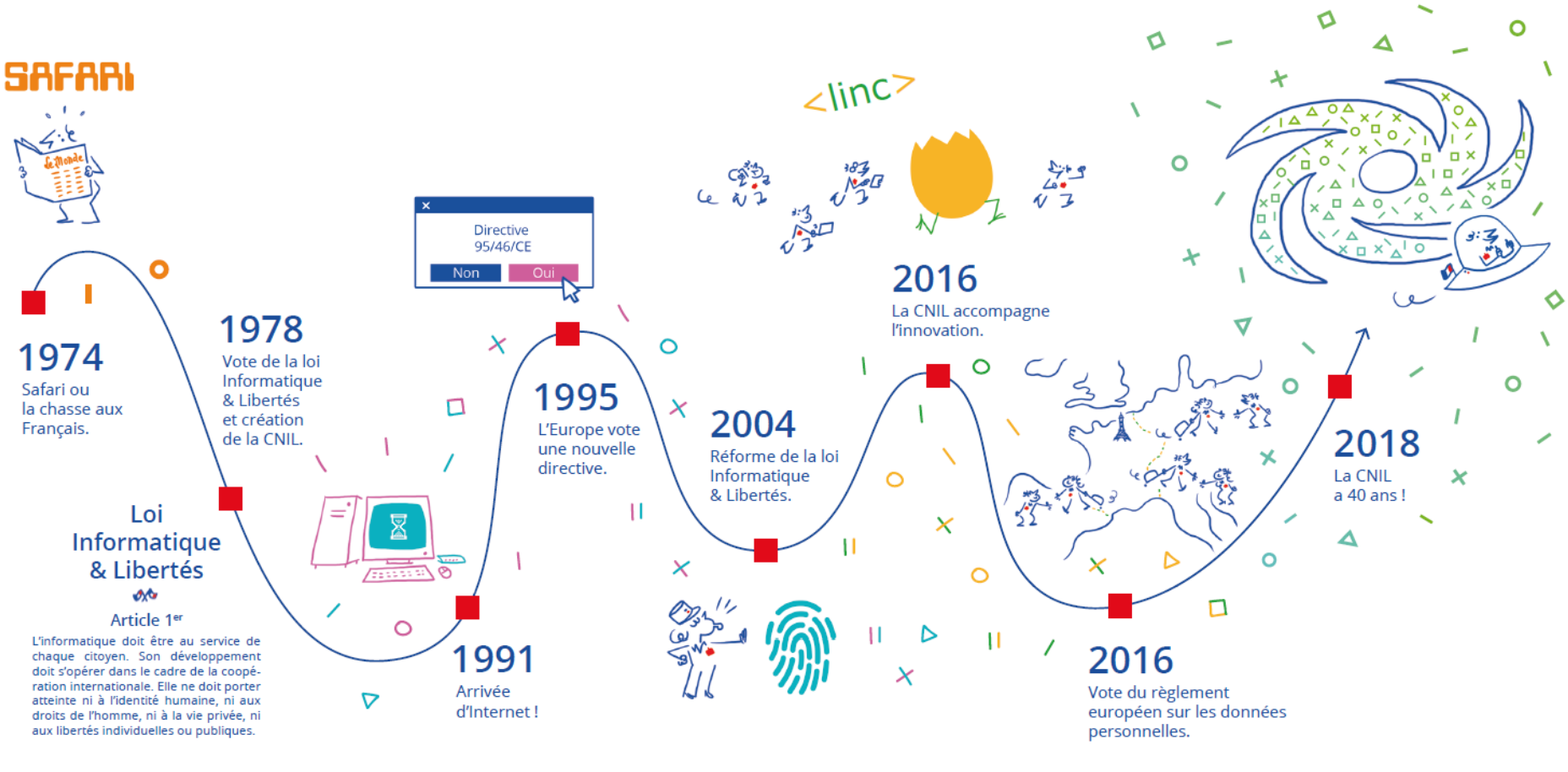
Annexes : **zooms** sur des sujets importants du RGPD

CNIL.

Présentation sur le RGPD

1. LA CNIL

Un peu d'histoire



CONSEILLER & RÉGLEMENTER

4 124 DÉCISIONS ET DÉLIBÉRATIONS DONT

2 964 AUTORISATIONS DE TRANSFERT DE DONNÉES HORS UE

810 AUTORISATIONS RECHERCHE MÉDICALE OU ÉVALUATION DES PRATIQUES DE SOINS

350 DÉLIBÉRATIONS DONT :

177 AVIS SUR DES PROJETS DE TEXTE

101 AUTORISATIONS

CONTRÔLER & SANCTIONNER

341 CONTRÔLES ONT ÉTÉ EFFECTUÉS DONT :

47 CONCERNANT LA VIDÉOPROTECTION

79 MISES EN DEMEURE

14 SANCTIONS DONT :

- **9** SANCTIONS FINANCIÈRES (6 PUBLIQUES)
- **5** AVERTISSEMENTS (2 PUBLICS)

RESSOURCES HUMAINES

BUDGET : **17 MILLIONS D'€**

198 emplois — **37%** **63%** — **40** ans Âge moyen

36% DES POSTES OCCUPÉS PAR DES JURISTES

26% PAR DES ASSISTANTS

14% PAR DES INGÉNIEURS / AUDITEURS

76% DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A

51% DES AGENTS TRAVAILLANT À LA CNIL SONT ARRIVÉS ENTRE 2012 ET 2017

8 ANS ANCIENNETÉ MOYENNE DES AGENTS DE LA CNIL

ACCOMPAGNER LA CONFORMITÉ

5 107 CIL SONT DÉSIGNÉS DANS :

18 802 ORGANISMES

98 DEMANDES DE LABELS REÇUES EN 2017

29 DEMANDES DE LABELS RGPD (labels Gouvernance ou Formation actualisés au regard du RGPD reçues)

117 DÉTENTEURS DE BCR DONT :

32 ONT DÉSIGNÉ LA CNIL COMME AUTORITÉ CHEF DE FILE

123 LABELS DÉLIVRÉS

PROTÉGER

8 360 PLAINTES

4 039 DEMANDES DE DROIT D'ACCÈS INDIRECT

(fichiers de police , de gendarmerie, de renseignement, etc.)

8 297 VÉRIFICATIONS EFFECTUÉES

+4,9 % PAR RAPPORT À 2016

INFORMER

155 000 APPELS

14 701 REQUÊTES SUR LA PLATEFORME « BESOIN D'AIDE » **+21%**

4,4 MILLIONS DE VISITES SUR CNIL.FR **+1,8** MILLION

320 INTERVENTIONS LORS DE CONFÉRENCES, COLLOQUES, SALONS, ETC.

93 500 FOLLOWERS SUR TWITTER

L’objectif : apporter la confiance

- **Sécurité et protection de la vie privée** apparaissent aujourd’hui comme des **conditions *sine qua non* pour apporter la confiance** aux usagers

- Dans un contexte où tout est donnée, où les menaces sont réelles et où la technologie nous dépasse parfois, **ce besoin de confiance devient un enjeu primordial**

CNIL.

Présentation sur le RGPD

2. LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Qu'est-ce que le RGPD ?

- Un cadre pour protéger les droits et libertés des personnes physiques contre les risques liés à leurs données
- La consécration des valeurs françaises et européennes
  - Continuité de la loi Informatique et libertés de 1978 et de la Directive européenne de 1995
- Une harmonisation dans tous les pays européens
- Une application élargie
  - Entreprises établies dans l'UE
  - Entreprises ciblant des personnes dans l'UE
- Règlement = application directe + spécificités locales (révision de la loi Informatique et libertés)

Les personnes physiques
L'individu est au cœur même du RGPD

- Vous (en tant qu'employé, internaute, ou citoyen européen) devez être **informé** de manière claire

- Vous devez pouvoir **exercer vos droits** :
  - De savoir : information et accès
  - De corriger : rectification et suppression + portabilité
  - D'être oublié : opposition et déréférencement
  - De prévoir : le sort de ses données après la mort

- Vos **données** doivent être **sécurisées** et vous devez être **averti en cas de violation** pouvant vous impacter gravement

- Vous avez différentes **voies de recours** (contre une entreprise ou la CNIL, recours collectif, réparation)

- Les **mineurs** doivent être protégés

Les personnes physiques
Sur le site de la CNIL

- Besoin d'aide : posez votre question, la CNIL vous répond https://www.cnil.fr/fr/cnil-direct
- Plaintes en ligne https://www.cnil.fr/fr/plaintes
- Explications, conseils et outils

COMPRENDRE VOS DROITS

Comment accéder à vos données personnelles, les rectifier, les supprimer ?

> Découvrir vos droits

MAÎTRISER VOS DONNÉES

mment protéger sa vie privée dans le monde numérique ?

> Découvrir les bonnes pratiques

AGIR

omment faire valoir ses droits sur ses données ou agir en cas de problème ?

> Découvrir vos moyens d'actions

Les entreprises
Moins de formalités, plus de responsabilité

- Qui est concerné ?
  - Entreprises établies en UE et celles ciblant des européens
  - « Responsables de traitements » et « sous-traitants »
- Qu'est-ce qui change ?
  - Moins de formalités (déclarations, demandes d'autorisations, *etc*.)
  - Le principe d'« *Accountability* » : se mettre en conformité et pouvoir le démontrer
- Quels sont les principes à respecter ?
  - Finalité légitime déterminée, limitation des données et de leurs durées de conservation, information claire, droits des personnes, sécurité, *etc*.
  - *Privacy by design* : intégrer la protection de la vie privée au plus tôt
- Quels sont les outils ?
  - Le délégué (DPO)
  - Le registre des traitements
  - Des outils pour établir la confiance : référentiels de la CNIL, certifications, codes de conduite, *etc*.

Les entreprises
Sur le site de la CNIL

- Nombreux **guides et outils**

https://www.cnil.fr/fr/rgpd-passer-a-laction
https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
https://www.cnil.fr/cnil-direct?visiteur=pro

- Outil pour générer ses **mentions d'information**

https://www.cnil.fr/fr/modeles/mention

- Formulaire de désignation de **DPO**

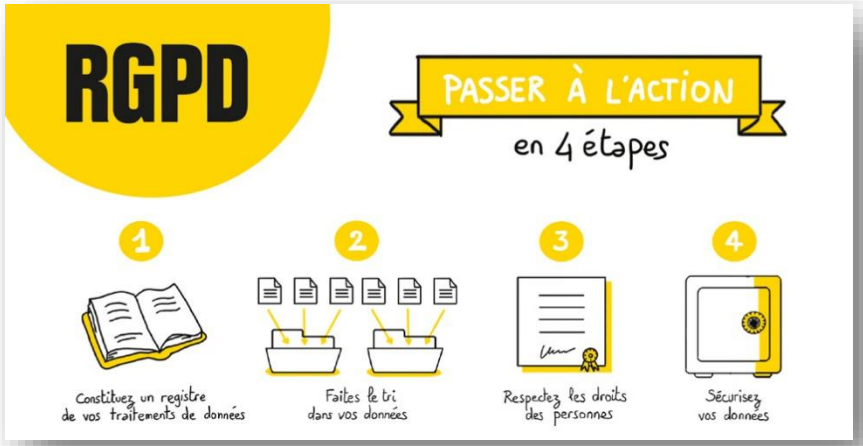
https://www.cnil.fr/fr/designation-dpo

- Modèles de **registre**

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique

- Formulaire pour notifier une **violation de données**

https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles



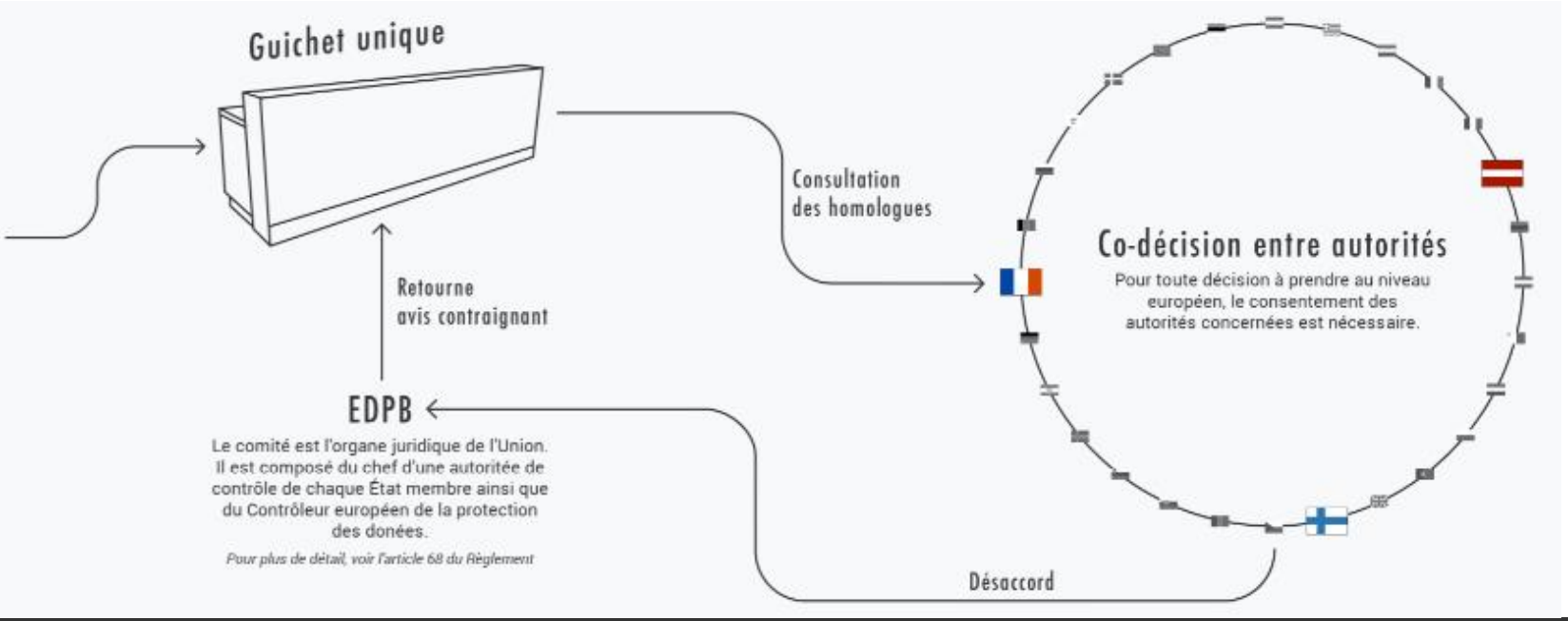
Les entreprises
Étude de cas : une association

- Contexte
  - Association loi 1901, 250 membres
  - Activités non sensibles (échanges entre professionnels d'un même secteur)
  - Informatique hébergée en France

- Actions
  - Cadrer la **gestion des membres** (respecter le cadre et appliquer les modalités)
    https://www.cnil.fr/fr/dispense/di-008-associations-gestion-des-membres-et-donateurs
  - Identifier ce qui sortirait du cadre pour les gérer dans un second temps
  - Créer un **registre**
    https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique
  - Revoir/créer les **mentions d'information** utilisées notamment lors de la collecte/rectification des données
    https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation
  - Faire un **plan d'action**
    - Pratiques sortent du cadre : transferts hors UE, collecte de photos, *etc.*
    - Amélioration des pratiques : en profiter pour faire le ménage dans les données, formaliser les procédures, améliorer la sécurité, *etc.*

Les autorités de protection des données
Harmonisation et crédibilité

- La continuité du rôle de la CNIL
  - Accompagner les entreprises
  - Faire respecter la Loi
  - Sensibiliser et aider les personnes
  - Conseil législatif/réglementaire
- Les nouveautés
  - Guichet unique
  - Coopération entre autorités
  - Sanctions renforcées
  - Certification, codes de conduite, *etc*.

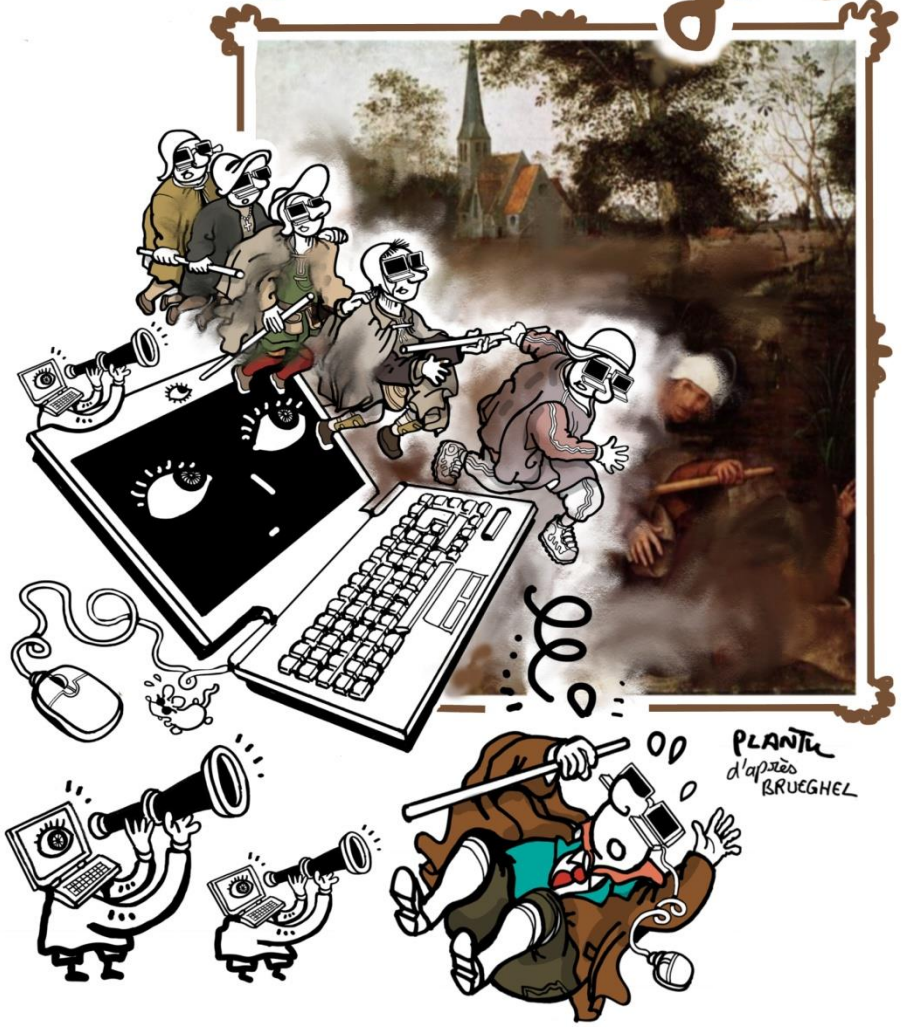


Conclusion

- Les derniers conseils
  - Dans une logique de *Privacy by design* : intégrer la protection de la vie privée dans tous les projets, au plus tôt, et de manière proportionnée aux risques sur les personnes
    - Mettre systématiquement en place les mesures élémentaires (guide sécurité, *etc.*)
    - Gérer les risques sur les services susceptibles d'engendrer des risques élevés
  - Dans une logique d'*Accountability* : faire son possible, planifier le reste, tout documenter
  - Recourir à, voire créer, des référentiels (codes de conduite, certification, PIAF, *etc.*)
  - En cas de violation ou de contrôle : transparence et coopération

- La CNIL est là pour vous aider
  - Une vraie mission de conseil / d'accompagnement
  - Des outils pratiques pour aider à comprendre et à faire
  - Privilégier les actions groupées (questions, référentiels, *etc.*)

La Parabole des aveugles



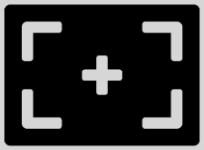
CNIL.

Présentation sur le RGPD

ANNEXES : ZOOMS SUR DES SUJETS IMPORTANTS DU RGPD

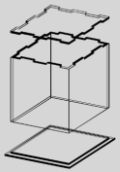
Qu'est-ce qu'une donnée à caractère personnel (DCP) ?

Quels sont les grands principes ?



Limitation des finalités

Minimisation des données



Licéité, loyauté, transparence

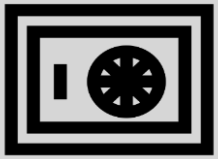
+

Respect des droits des personnes:

- Information
- Consentement
- Rectification, opposition
- Accès, rectification
- Portabilité

Exactitude

Limitation de la conservation



Sécurité

Le sous-traitant
Une répartition des rôles plus réaliste

- Qui est sous-traitant ?
  - Ceux qui agissent pour le compte de « responsables de traitements » (qui eux, déterminent la finalité et les moyens de traitements)
  - Pas concernés : éditeurs de logiciels ou fabricants de matériels (qui n'ont pas accès et ne traitent pas de données)
  - NB : un sous-traitant est généralement responsable de traitement pour les traitements qu'il réalise pour son propre compte (ex : gestion de son personnel)

- Quelles obligations ?
  - Transparence et traçabilité
  - Prendre en compte la protection de la vie privée dès la conception
  - Garantir la sécurité des données
  - Assister, alerter, conseiller (violations, PIA, *etc*.)

- Quels outils ?
  - Le DPO
  - Le registre
  - Les clauses contractuelles

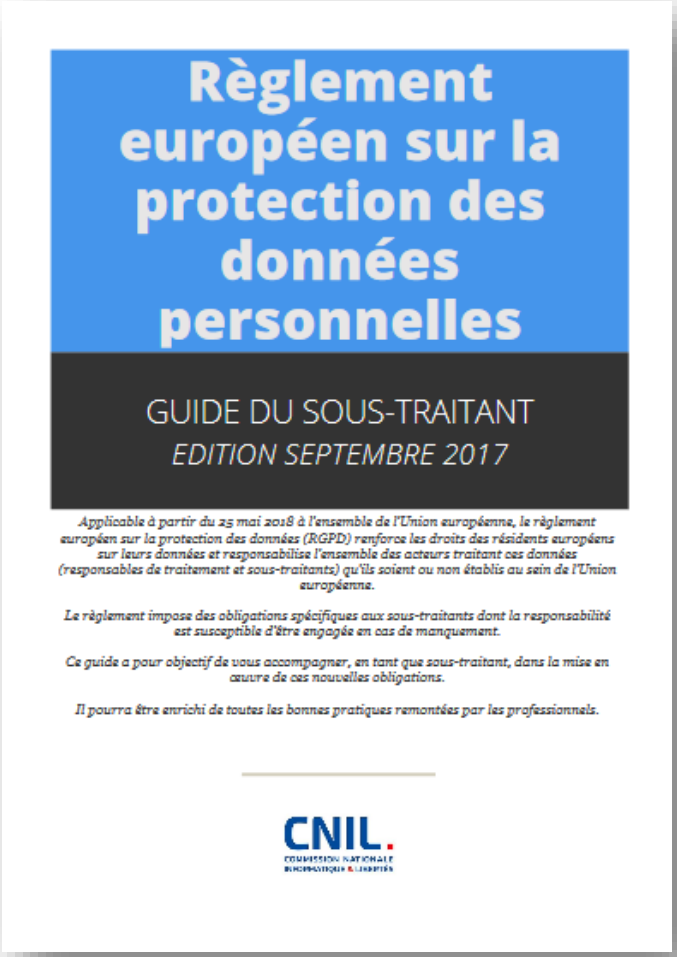
Le sous-traitant
Sur le site de la CNIL

- Le guide du sous traitant

  https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants

- Des clauses types

  https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses



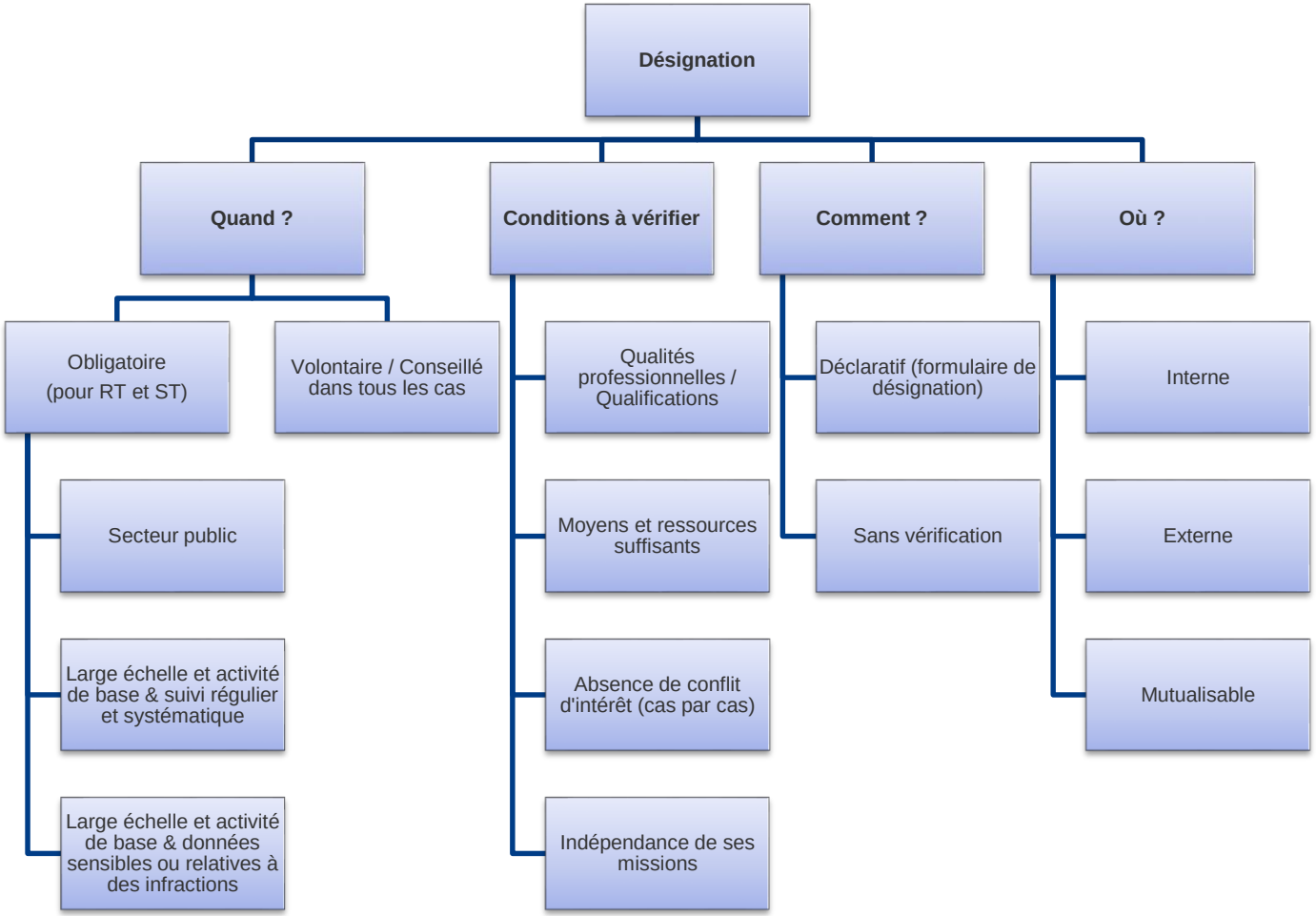
Le délégué à la protection des données
Ses missions, en synthèse

1. Informer / Conseiller
2. Contrôler le respect du RGPD
3. Coopérer avec l'autorité / Être le point de contact
4. Conseiller sur l'analyse d'impact / Vérifier son exécution
5. S'assurer de la bonne tenue de la documentation

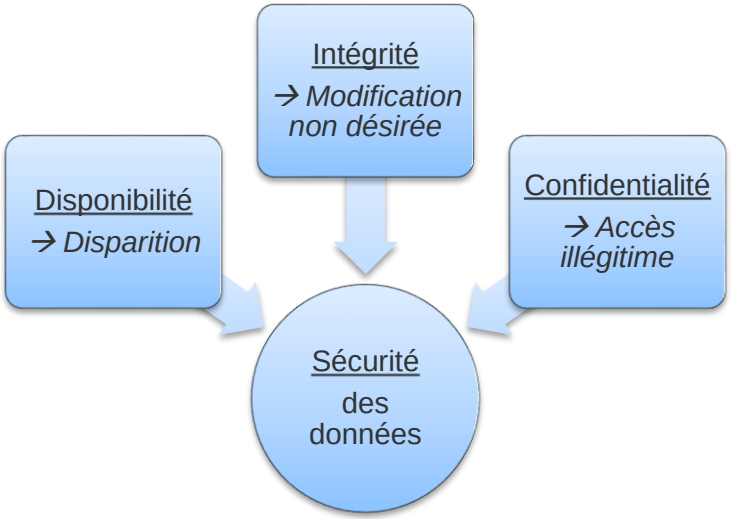
L'article « Devenir délégué à la protection des données » : https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

Le formulaire de désignation : https://www.cnil.fr/fr/designation-dpo

Le délégué à la protection des données
Sa désignation



La sécurité
Proportionnalité aux risques



Risques ⟷ **Traitements**

> « *Degré de probabilité* »
(vraisemblance)
> Gravité

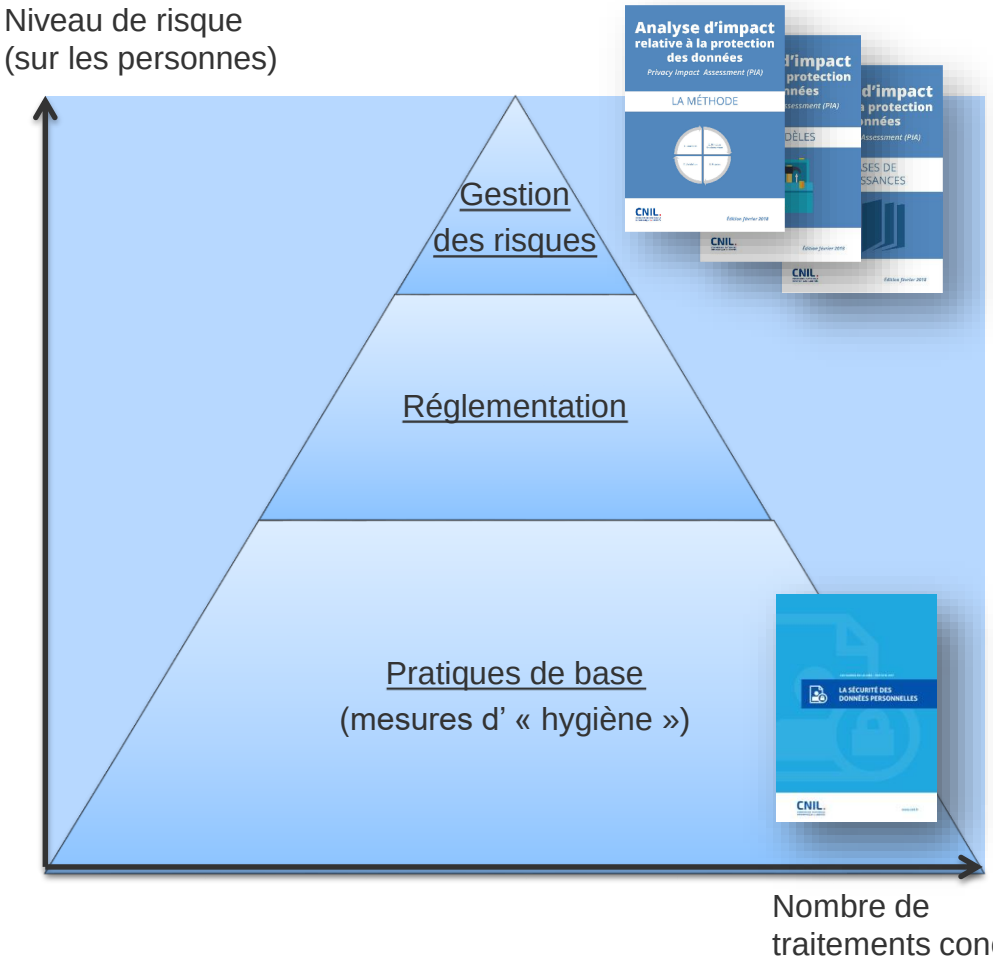
> Nature
> Portée
> Contexte
> Finalités

Mesures

> « *Niveau de sécurité **adapté** au risque* » (mesures proportionnées aux risques)
> Techniques et organisationnelles
> Prise en compte de l'état des connaissances et des coûts de mise en œuvre

Responsables de traitements
+
Sous-traitants

La sécurité
La logique générale



3. Enfin, les risques devraient être étudiés en détail sur les traitements susceptibles d'engendrer des risques élevés
   - Exemples d'outils : Guides et logiciel PIA

2. Ensuite, les règles applicables (réglementation, politiques internes, normes, *etc*.) devraient être mises en œuvre
   - Exemples d'outils : PSSI de l'organisme

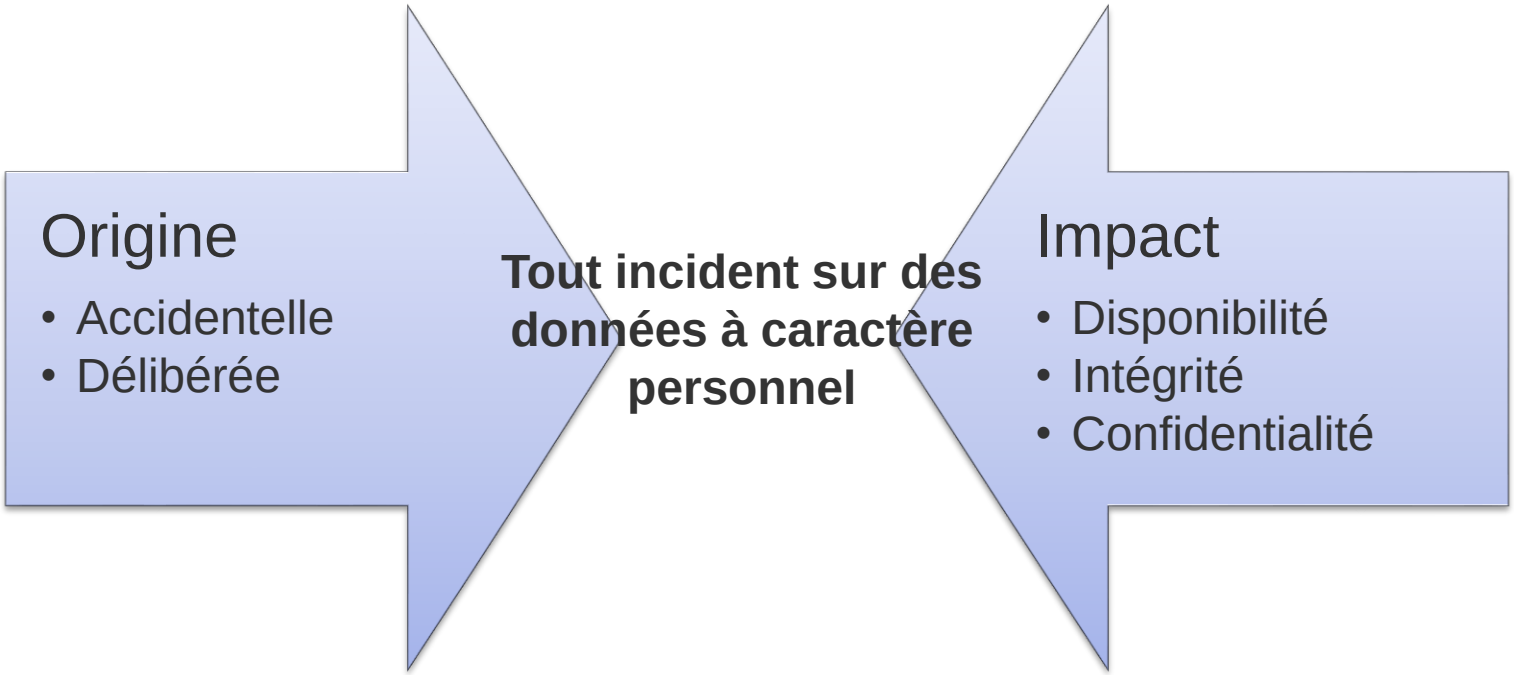
1. En premier lieu, les pratiques de base devraient être mises en place de manière systématique
   - Exemples d'outils : Guide « La sécurité des données personnelles »

La sécurité
Se référer à des sources « fiables »

- Publications de l'ANSSI
  - Référentiel général de sécurité (RGS)
    https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
  - Guide d'hygiène informatique
    https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
  - Bonnes pratiques
    https://www.ssi.gouv.fr/administration/bonnes-pratiques/
  - Notes d'information du CERT-FR
    https://www.cert.ssi.gouv.fr/information/
- Publications de la CNIL
  - Guide « La sécurité des données personnelles »
    https://www.cnil.fr/fr/un-nouveau-guide-de-la-securite-des-donnees-personnelles
  - Guides et logiciel PIA
    https://www.cnil.fr/fr/PIA-privacy-impact-assessment
  - Recommandations sur les mots de passe
    https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires
- Normes internationales
  - ISO/IEC 27001 : exigences pour un système de management de la sécurité de l'information (SMSI)
  - ISO/IEC 27002 : catalogue de bonnes pratiques pour la sécurité de l'information

Les violations de données

Qu’est-ce qu’une violation de données ?



Les violations de données
Différents cas de notifications

Pour les personnes concernées, la violation engendre :	Aucun risque	Un risque	Un risque élevé
Documentation en interne par le RT sous forme d'un registre interne des différentes violations dont il est victime	X	X	X
Notification à l'autorité de contrôle, c'est-à-dire la CNIL en France, si possible en 72h	-	X	X
Information des personnes concernées dans les meilleurs délais, hors cas particuliers	-	-	X

Le formulaire de notification :
https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

L'analyse d'impact (PIA)

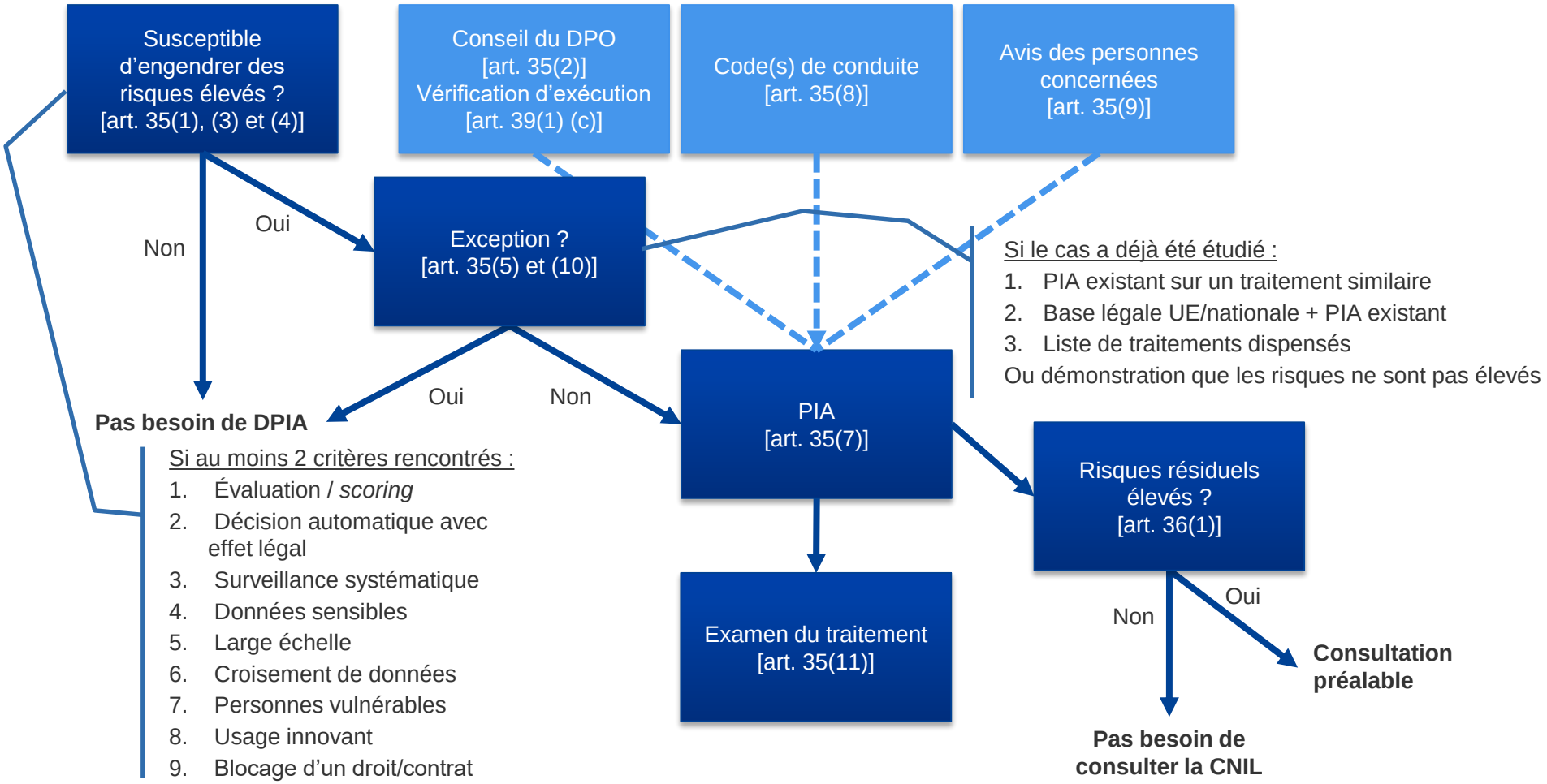
Un PIA repose sur deux piliers

- Les principes et droits fondamentaux (finalité, information, *etc*.), « non négociables », fixés par la loi, devant être respectés et ne pouvant faire l'objet d'aucune modulation

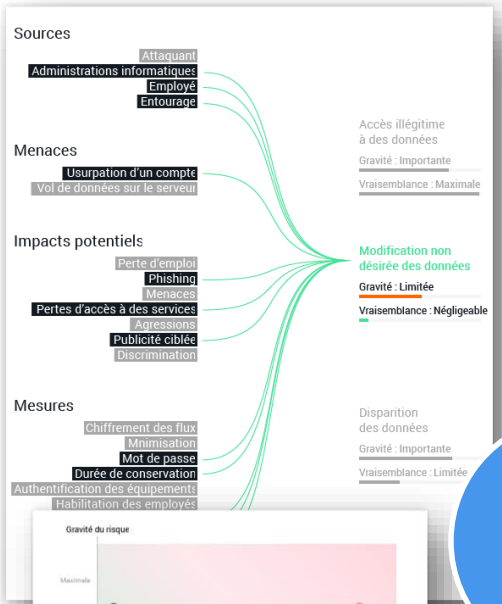
- La gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données

- Le *Privacy Impact Assessment* (PIA) est un moyen de **se mettre en conformité** et **de le démontrer** (notion d'*accountability*)

L'analyse d'impact (PIA)
La logique générale



L'analyse d'impact (PIA)
Sur le site de la CNIL



http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083