POLYTECH NANCY

Les obligations réglementaires de sécurité et de protection des données

SEANCE DE TD : AIPD
Analyse d'impact sur la protection des données

Patrice Thiriot

POLYTECH NANCY

Réglementation européenne de protection des données

Les implications dans le secteur informatique

RAPPEL COURS PRECEDENT

L'analyse d'impact relative à la protection des données (Art. 35)

|

La prescription pour les traitements les plus risqués

ETUDE D'IMPACT OBLIGATOIRE si le traitement de données figure sur la liste des AIPD obligatoires ou si il rempli deux critères ci dessous

Evaluation, Scoring *(y compris profilage)*	**Données sensibles ou hautement personnelles** *(santé, géolocalisation …)*	**Personnes vulnérables** *(patients, personnes âgées, enfants …)*
Décision automatique avec effet légal	Collecte à large échelle	Usage innovant *(utilisation d'une nouvelle technologie)*
Surveillance systématique	Croisement de données	Exclusion du bénéfice d'un droit ou d'un contrat

DPO  **RSSI**

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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

Privacy Impact Assessment (PIA)

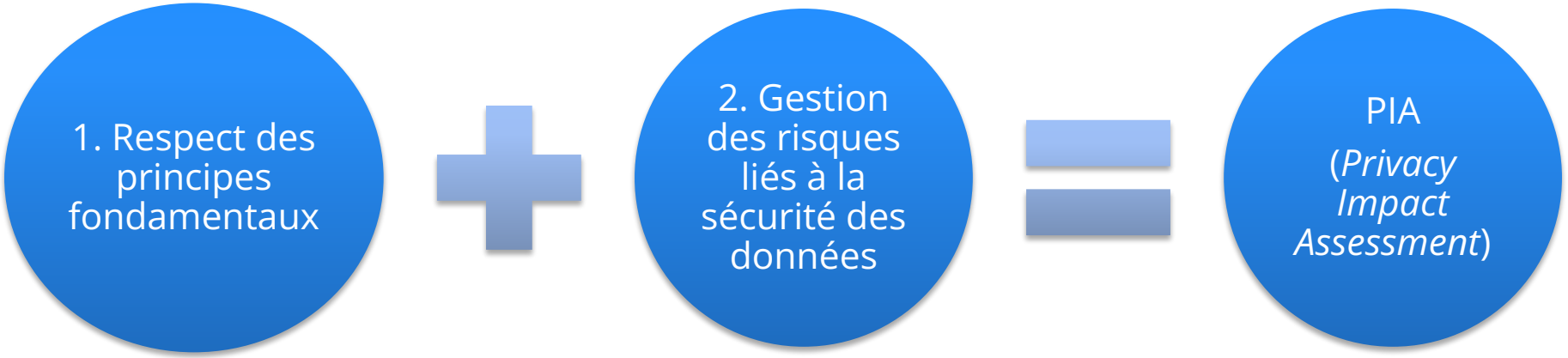
Atelier

Comment mener un PIA ?

LA DÉMARCHE MÉTHODOLOGIQUE

Un PIA repose sur deux piliers

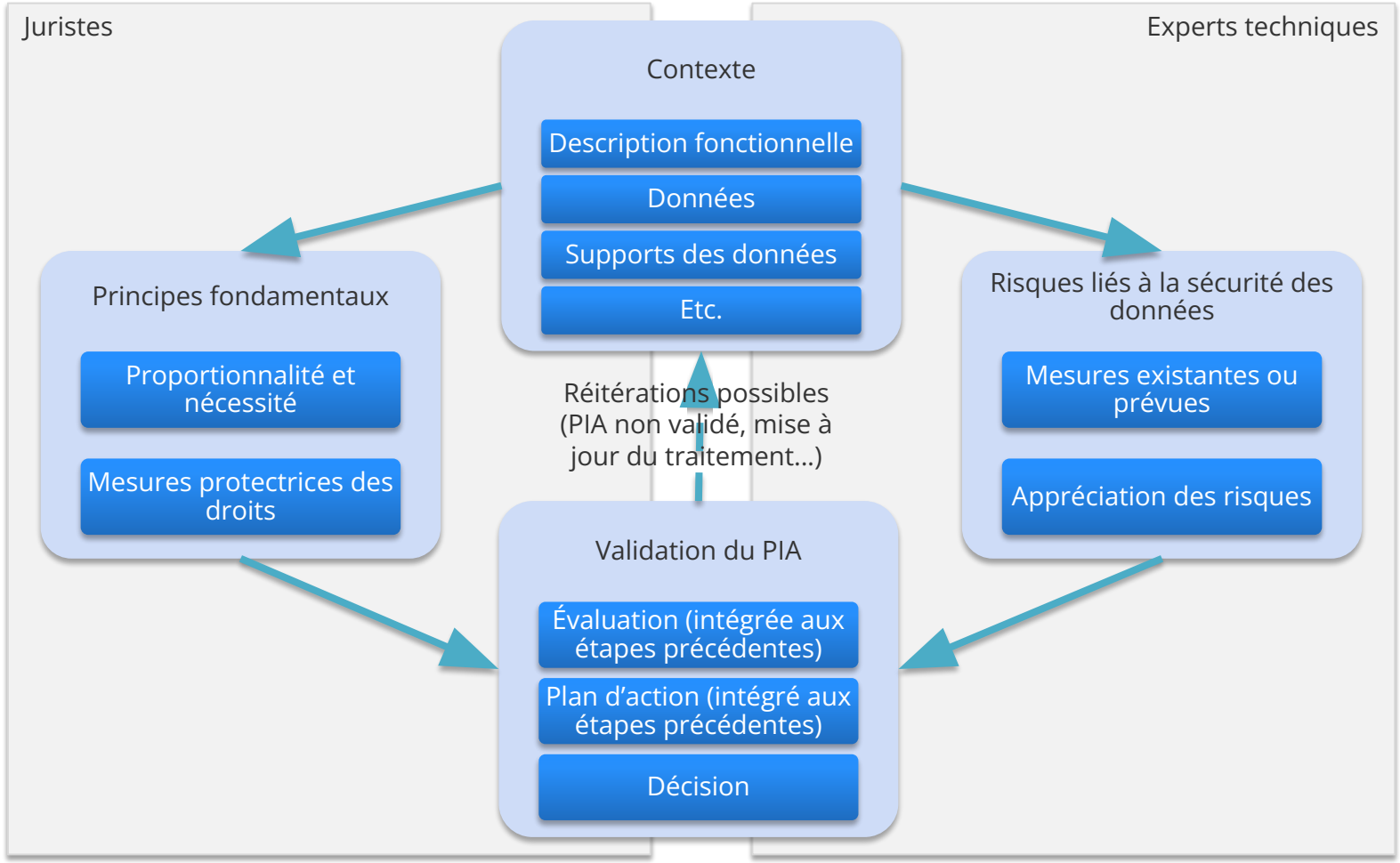
Que signifie être conforme au Règlement ?



- Les principes et droits fondamentaux (finalité, information…), « 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)

Démarche méthodologique

Adaptation des guides PIA



Étape 1 – Le contexte

De quoi parle-t-on ?

- Le traitement de données à caractère personnel
  - Quelle est sa finalité ?
  - Quels sont ses apports ? (pour l'organisme, pour les personnes concernées, pour la société…)

- Le plus important : comprendre le cycle de vie des données
  - Quelles sont les données ?
  - Qui sont les destinataires ?
  - Qui peut y accéder ?
  - Quelle est leur durée de conservation ?
  - Sur quoi reposent-elles ?
  - Quelles sont les étapes du traitement ?

Étape 2 – Les principes fondamentaux

Quel est le dispositif prévu ?

- Analyse des mesures garantissant la proportionnalité et la nécessité du traitement
  - Finalité(s) (déterminée, explicite et légitime – interdiction du détournement de finalité) [art. 5.1 (b)]
  - Fondement/licéité du traitement [art. 6]
  - Données adéquates, pertinentes, non excessives (minimisation), exactes et tenues à jour [art. 5 (c)]
  - Durée de conservation limitée [art. 5 (e)]

Étape 2 – Les principes fondamentaux

Quel est le dispositif prévu ?

- Analyse des mesures protectrices des droits des personnes des personnes concernées
  - Information des personnes (traitement loyal et transparent) [art. 12, art. 13, art. 14]
  - Droit d'accès et droit à la portabilité
  - Droit de rectification, d'effacement, d'opposition et de limitation du traitement
  - Sous-traitance [art. 28]
  - Transferts [art. 44 et suivants]

Étape 3 – Les risques

Quelles sont les mesures de sécurité ? [art. 32]

Mesures sur les données du traitement

- Chiffrer
- Anonymiser
- Cloisonner
- Contrôler les accès logiques
- Journaliser
- Contrôler l'intégrité
- Archiver
- Sécuriser les documents papier

Mesures générales de sécurité

- Sécuriser l'exploitation
- Lutter contre les logiciels malveillants
- Gérer les postes clients
- Sécuriser les sites web
- Sauvegarder
- Maintenance
- Sécuriser les canaux informatiques
- Tracer l'activité du système
- Contrôler l'accès physique
- Réduire les vulnérabilités des matériels
- S'éloigner des sources de risques
- Se protéger des sources de risques non humaines

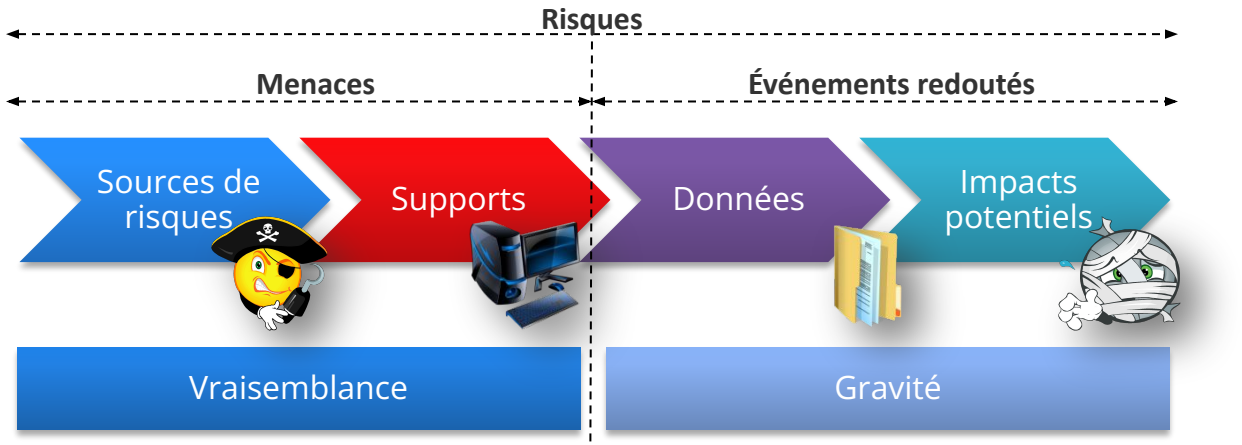
Mesures organisationnelles

- Gérer l'organisation de la protection de la vie privée
- Gérer la politique de protection de la vie privée
- Gérer les risques
- Intégrer la protection de la vie privée dans les projets
- Gérer les incidents de sécurité et les violations de données
- Réduire les vulnérabilités du personnel
- Relations avec les tiers
- Superviser le protection de la vie privée

Étape 3 – Les risques

Que peut-il arriver aux personnes concernées ?

- Un risque sur la « vie privée » est un scénario décrivant un événement redouté et toutes les menaces qui le rendent possible. Il est estimé en termes de gravité et de vraisemblance



- Sources de risques
  - Personnes externes
  - Personnes internes
  - Sources non humaines
- Supports
  - Matériels
  - Logiciels
  - Réseaux
  - Personnes
  - Supports papier
  - Canaux papier
- Données
  - Données du traitement
  - Données liées aux mesures
- Impacts potentiels
  - Vie privée
  - Identité humaine
  - Droits de l'homme
  - Libertés publiques

Étape 3 – Les risques

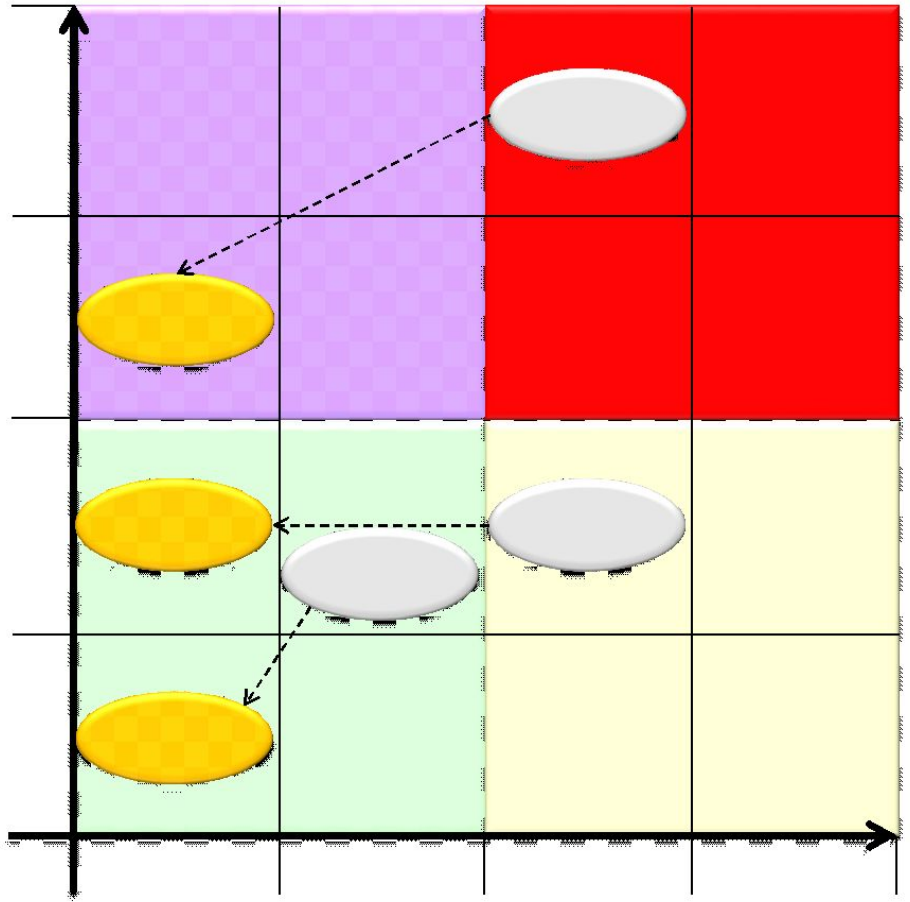
Comment les décrire ?

	Accès illégitime à des données	Modification non désirée de données	Disparition de données
Sources de risques			
Impacts potentiels			
Menaces			
Mesures			
Gravité			
Vraisemblance			

- Notes :
  - Les impacts sont ceux sur la vie privée des personnes concernées, et non ceux sur l'organisme
  - Les menaces sont tous les moyens que les risques se concrétisent
  - Les mesures sont celles qui contribuent à traiter le risque parmi celles identifiées
  - La gravité est essentiellement estimée en fonction des impacts potentiels
  - La vraisemblance est essentiellement estimée en fonction des vulnérabilités exploitables

Étape 3 – Les risques

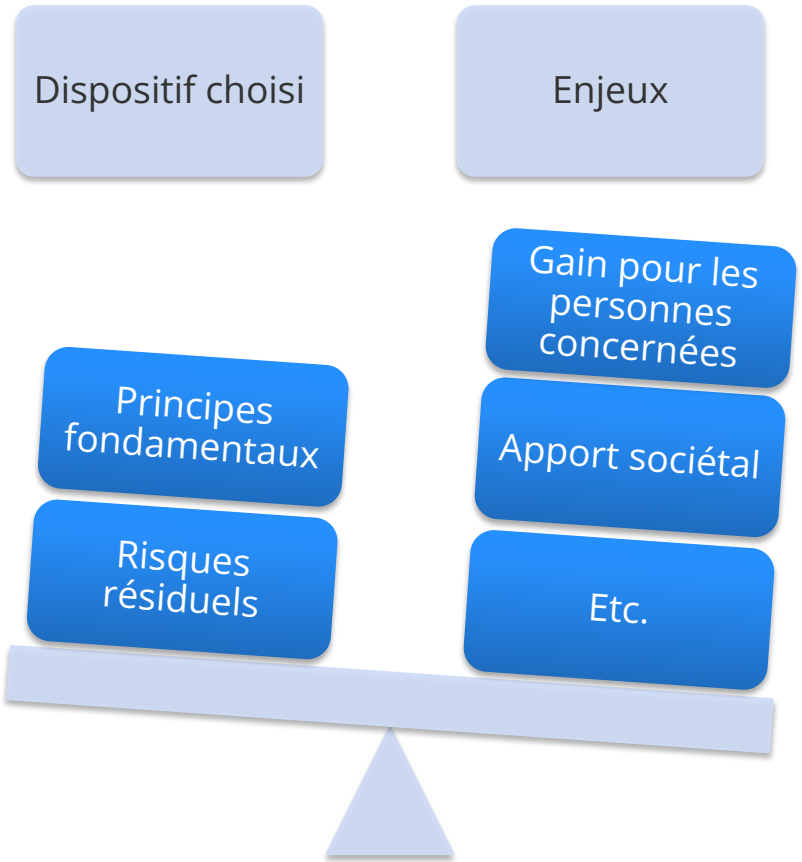
Comment les présenter ?



- Une cartographie des risques permet de comparer visuellement les risques les uns par rapport aux autres
- Elle permet également de faciliter la détermination des objectifs pour les traiter (par « zones »)

Étape 4 – La décision

Les risques résiduels sont-ils acceptables ?



- Si les mesures prévues (pour respecter les principes fondamentaux et traiter les risques) sont jugées suffisantes et les risques résiduels acceptables, alors le rapport de PIA peut être validé par le responsable de traitement

- Sinon, alors il convient d'identifier les objectifs pour y parvenir et de refaire une itération de la démarche

MERCI DE VOTRE ATTENTION