Soirée SMP 08.10.2024

11 idées reçues

Sur la «nLPD»

Eric Sinot, academy-agile.ch

Guide de montagnes informatiques

academy-agile.ch

Idée reçue n°1 : «nLPD» → nouvelle, vraiment ?

nLPD → **Nouvelle** Loi sur la Protection des Données : **septembre 2023**

→ application très récente,

→ tolérance au démarrage de la mise en place …

→ … comme le moteur de ce véhicule.

Idée reçue n°1 :
«nLPD» → nouvelle, vraiment ?

1ère version Loi fédérale sur la Protection des Données (LPD) : **1992**
1er alignement au RGPD de l'UE : **2019**

→ Loi éprouvée ; déjà en vigueur depuis longtemps ;
PFPDT & autres parties prenantes expérimentées

→ **appliquer LPD dès maintenant** (sans excuse nouveauté)

projets → appliquer LPD sur données projet, même rétroactivement

academy-agile.ch

Idée reçue n°1.1 :

Victime ← l'un ou l'autre → Fautif

Autre loi → **VICTIME !!!**

nLPD → responsible, fautif, en même temps ???

→ *pas compatible … alors Victime ?*

→ comme dans cette histoire attendrissante ?…

academy-agile.ch

Idée reçue n°1.1 :
Victime ← l'un ou l'autre → Fautif

→ **SI ! Les deux !!!**

Dans quasi-toutes violations de sécurité.
(par pirate, employé, inadvertance …)

LPCR, même victime, serait aussi coupable d'avoir divulgué des données personnelles de sa mère-grand, dont sa localisation …

→ **appliquer LPD dès maintenant** (sans excuse victimisation)

projets → id.

academy-agile.ch

Idée reçue n°2 :

RGPD de l'UE ← l'un ou l'autre → **LPD** suisse

Soumis à l'un, ou à l'autre, mais pas aux deux en même temps …
(Similaire : jamais de double peine ...)

academy-agile.ch

Idée reçue n°2 :

RGPD de l'UE ← l'un ou l'autre → **LPD** suisse

Soumis à l'un, ou à l'autre, mais pas aux deux en même temps …
*(Similaire : **jamais de double peine ???**...)*

→ **SI ! Les deux !!!** Dans certaines circonstances.
(heureusement exigences semblables)

→ **appliquer LPD & RGPD**, en parallèle & en cumulant
projets → analyse préalable risque LPD **&** RGPD

academy-agile.ch

Idée reçue n°3 :
Ce sont les **données de** la société XYZ.

Google, La Poste, Migros, … la société XYZ …
sont propriétaires de ces données personnelles …

(Car elles ont fait l'effort de les collecter dans leurs systèmes …)

→ Ces propriétaires peuvent traiter ces données **comme bon leur semble.**

(elles sont des biens immatériels, c'est moins important …)

academy-agile.ch

Idée reçue n°3 :
Ce sont les **données de** la société XYZ.

→ Plutôt : **“Ces données personnelles** sont **traitées** par XYZ.”

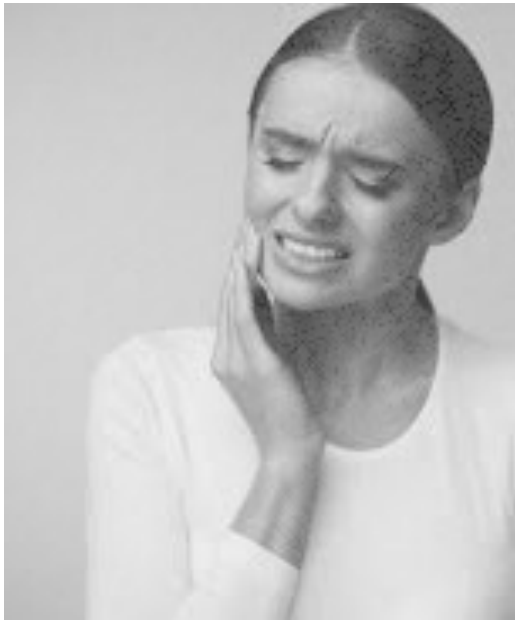
projets → **XYZ est donc responsable** de ses traitements - dès ses projets …

academy-agile.ch

Idée reçue n°4 :
Données personnelles **sensibles** → à protéger

Comme le mot «sensible» l'indique,
ces données valent la peine d'être protégées.
(médical / santé ; biométriques …)

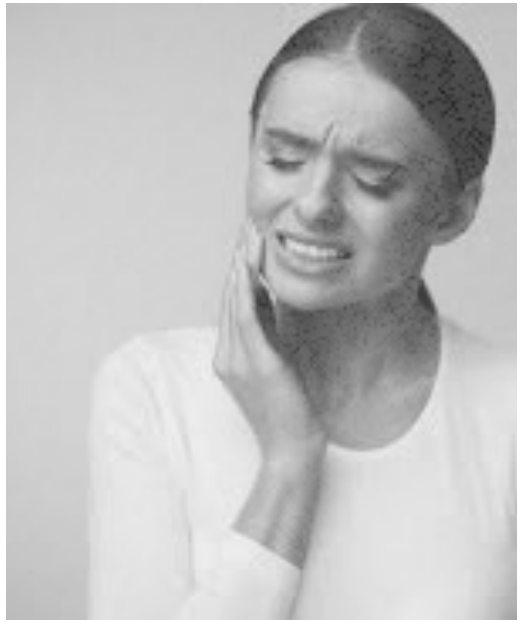
→ **Seules** ces données sensibles sont à protéger
(et en l'absence de donnée sensible : rien n'est à protéger).



Idée reçue n°4 :
Données personnelles **sensibles** → à protéger

→ Plutôt : **“Les données personnelles sensibles sont à protéger particulièrement.**

projets → inventaire de **toutes les données à protéger**, y compris celles sensibles.



Idée reçue n°5 :
avec un **fournisseur (re)connu**, tout va bien

Microsoft, Google, … sont des fournisseurs (re)connus.
Comme client, ma sécurité est assurée, sur le plan légal aussi.
Leurs systèmes sont sécurisés par défaut.

→ **Avec ce type de fournisseur re(connu),** rien d'autre à faire 👍

Comme l'usage d'une l'automobile d'un constructeur reconnu …

Idée reçue n°5 :
avec un **fournisseur (re)connu**, tout va bien

→ **Avec ce type de fournisseur re(connu),**
il faut tout de même : 🙏
Comme l'usage d'une l'automobile d'un constructeur reconnu …

→ faire **l'effort** de l'usage **conforme à la loi** de ces produits
signer des **contrats spécifiques**
(seule la vente des produits de ces fournisseurs étant légale par défaut) ;

projets → doivent préparer dès l'amont un usage conforme (cible).

Idée reçue n°6 :
LPD → Loi → phénomène **juridique**

Loi LPD & son ordonnance (OPDo) → juridiques → phénomène juridique

→ **Des compétences juridiques sont l'essence.**

Pour l'usage conforme à la LCR d'une l'automobile, des compétences …

Idée reçue n°6 :
LPD → Loi → phénomène **juridique**

Pour l'usage conforme à la LCR d'une l'automobile, des compétences de conduite d'une automobile ?… juridiques ?... sont essentielles ?

→ Plutôt : compétences juridiques pour les formalismes ;
Maîtrise de ses propres traitements de données &
technologies de traitement des données, pour la substance.

projets → préparer avec double compétence.

Idée reçue n°7 :
salaires → données **sensibles** ???

Une donnée si confidentielle et personnelle, pour l'employeur, et d'autres personnes …

→ **Est forcément une donnée <u>hyper-sensible</u> !!!**

Idée reçue n°7 :
salaires → données **sensibles** ???

→ Plutôt : au sens LPD, les salaires ne sont pas dans la liste “données sensibles” ;
les **salaires des employés sont “moins sensibles” que les certificats maladie**

projets → sécuriser les autres données personnelles des employés, comme les salaires.

Idée reçue n°8 : sécurité données → floue …

La LPD exige la sécurité des données personnelles, mais ne définit pas cette sécurité …

→ **Qui restera toujours imparfaite, le 100% sans risque n'est pas atteignable.**

Tous les experts du risque (informatique …) le disent.

Idée reçue n°8 : sécurité données → floue …

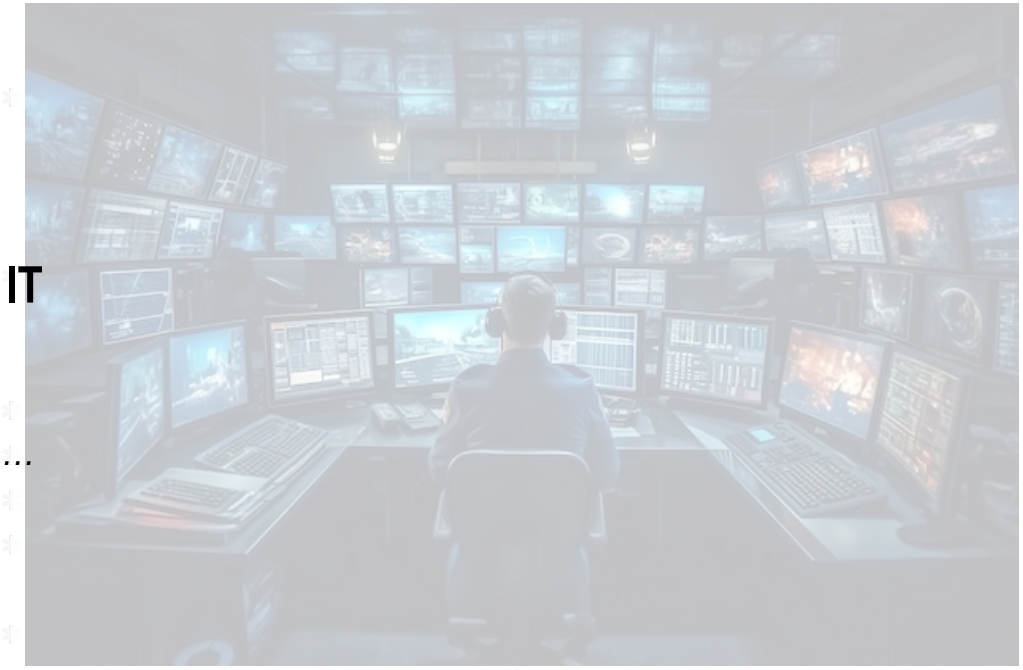
→ Plutôt : niveau minimal de sécurité (cf. état de l'art) défini dans **l'ordonnance OPDo** : **CIA + Traçabilité** (orientation ISO 27000)

projets → prendre en compte OPDo dès le début du projet. (et RGPD le cas échéant)

Idée reçue n°9 :
concerne vraies données → «production» IT

Seules les **vraies données** comptent ;
pas de problème hors les vrais systèmes de production IT.

→ **Pas besoin de sécuriser,**
ni traiter les données hors production IT
Possible de <u>sécuriser à la fin</u>.
Sytèmes de tests, d'UAT/intégration,
pour formation, d'archivage/sauvegarde (backup) …

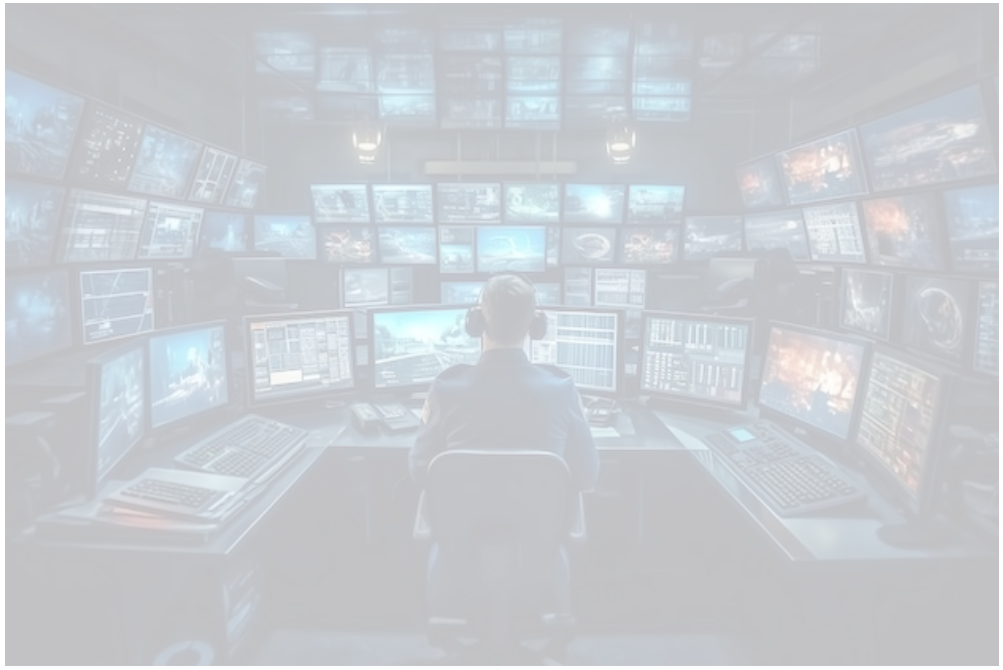


Idée reçue n°9 : concerne vraies données → «production» IT

academy-agile.ch

→ Plutôt : **toutes** les données personnelles de **tous les systèmes**, doivent être sécurisées (anonymisation ou pseudonymisation ?) et traitées conformément OPDo (et RGPD le cas échéant). Cf. exemple **Xplain**.

projets → prendre en compte conformité LPD dès le début du projet, un prototype ...



Idée reçue n°10 : consentement → justification idéale

Un traitement de données personnelles (LPD) doit avoir une justification :

→ **Consentement des sujets des données est une solution**
si pas de raisons légales.

Idée reçue n°10 : consentement → justification idéale

Un traitement de données personnelles (LPD) doit avoir une justification :

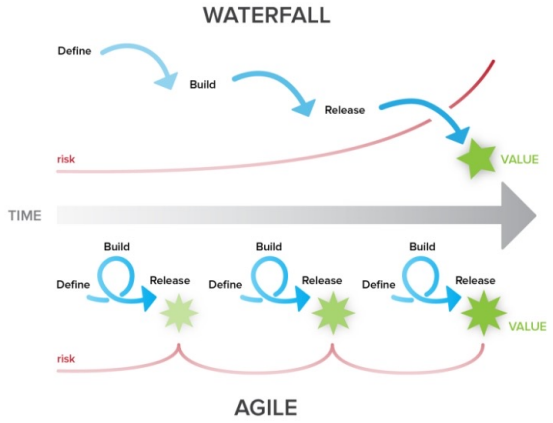
→ **Contrats** plutôt que consentement.
Cf. contre-exemples réseau cliniques, consentement employés …

projets → gérer légitimité traitement données dès le début du projet, un prototype ...

Idée reçue n°11 :
répondre efficacement à exigences → projet waterfall

Les exigences de la LPD et de son ordonnance OPDo sont clairement définies.
Les traitements sur les données aussi.
Une planification parfaite est possible.

→ **Un projet de mise en conformité LPD se mène mieux en waterfall.**

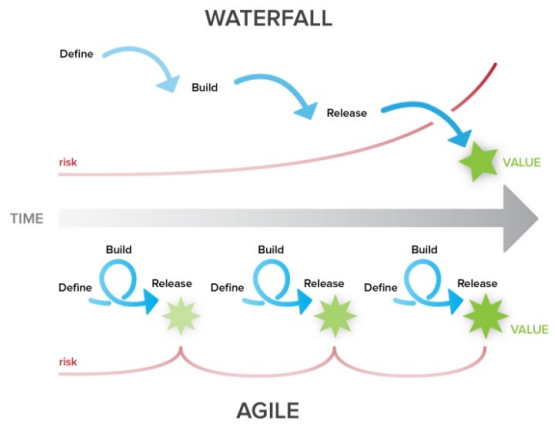


Idée reçue n°11 :
répondre efficacement à exigences → projet **waterfall**

academy-agile.ch

→ Plutôt AGILE : exigences (user stories) **prioritaires d'abord** ;
mieux vaut 80% des exigences que « rien » ;
Car grande variabilité :
- types et structures de données
- systèmes IT
- processus (traitements) données

projets → **gérer d'abord l'important (Pareto), mais le gérer vraiment.**



Eric Sinot
Guide de Montagnes Informatiques

academy-agile.ch

→ indépendant, avec expérience de :

→ **Cyber-conformité & Sécurité**
eric.sinot@lesmontagnesinvisibles.ch

→ Gestion de projet (academy-agile.ch)

À vous de déboulonner, debunker, maintenant !