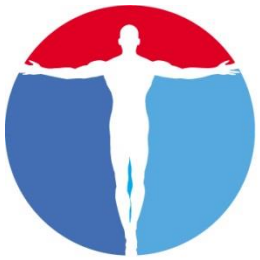


APDL

Association pour la Protection des Données au Luxembourg

GDPR | SANTE ET RECHERCHE

CLAIRE LEONELLI

DONNEES PERSONNELLES
DROITS DU PATIENT

DONNEES DE SANTE

↓

DONNEES PERSONNELLES

↓

LOI 2002
GDPR

↓

PATIENT

↓↑

PROFESSIONNEL DE SANTE

↓

LOI 2014 D&O DU PATIENT

↓

DROITS ET OBLIGATIONS SPECIFIQUES
(non applicables aux pers. décédées)

DROITS ET OBLIGATIONS SPECIFIQUES
(y compris pour patient décédé)

⇒DOMAINES D'APPLICATION DISTINCTS
⇒CERTAINS CHEVAUCHEMENTS

GDPR "IN A NUTSHELL"

- règlement UE = harmonisation
- objectif: faire de la protection des données un élément de la gouvernance des organisations
- la paperasserie infantilisante fait place à la responsabilité («*accountability*»)
- les organisations doivent prendre en compte la protection des données pour toute activité, tout projet
- face au risque, le personnel doit être formé aux règles
- droits renforcés/plus de droits pour les personnes
- haut niveau de conformité attendu
- sanctions énormes (jusqu'à EUR20mio/4% du CA mondial annuel)

L'AGE DE LA MATURITE

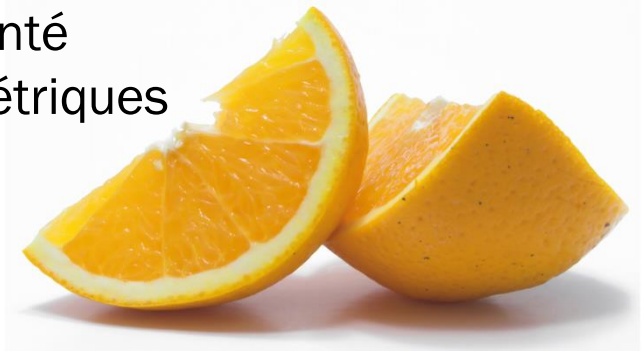
DEFINITIONS

RAPPEL DES NOTIONS CLES

DONNEE PERSONNELLE

Toute information de quelque nature qu'elle soit et indépendamment de son support concernant une personne DIRECTEMENT OU INDIRECTEMENT identifiée ou identifiable

- Nom, prénom, date de naissance, adresse
- Son, image
- Données électroniques
- Numéro d'identification
- Origine culturelle, sociale ou économique
- Données judiciaires
- Données de santé
- Données biométriques
- Etc.



GDPR: +référence aux identifiants en ligne et géolocalisation

TRAITEMENT

LOI ACTUELLE + GDPR

Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données, **telles que**:

- collecte
- organisation
- adaptation
- extraction
- utilisation
- rapprochement
- verrouillage
- communication par transmission
- toute autre forme de mise à disposition
- enregistrement
- conservation
- modification
- consultation
- diffusion
- interconnexion
- effacement
- destruction

DÉFINITION TRÈS VASTE COUVRE TOUT ACTE DE MANIPULATION OU D'EXPLOITATION DES DONNÉES (Y COMPRIS A DES FINS DE RECHERCHE)

DONNEES DE SANTE

Ensemble des données se rapportant à/révélant l'état de santé physique/mental passé, présent ou futur

- Données collectées lors de l'inscription en vue de soins de santé
- Numéros ou éléments spécifiques attribués pour identification unique à des fins de santé
- Informations obtenues lors de tests ou examens, y compris à partir de données génétiques et d'échantillons biologiques
- Toute information sur maladie, handicap, risque de maladie, antécédents médicaux, traitement clinique ou état physiologique ou biomédical, indépendamment de la source

DONNEES GENETIQUES | DONNEES BIOMETRIQUES

Données relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question (telle que analyse des chromosomes, analyse ADN ou ARN, etc.)

Données résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique,
qui permettent ou confirment son identification unique,
telles que des images faciales (dans certains cas) ou des données dactyloscopiques

Données génétiques = données de santé particulières
Données biométriques ≠ données de santé (en tant que telles)

PARTICULARITES DES DONNEES DE SANTE

DONNEES SENSIBLES

Traitement en principe interdit

SAUF CAS DE LÉGITIMITÉ SPÉCIFIQUES

SECRET PROFESSIONNEL

- obligation légale et déontologique à charge des professionnels de santé et organismes de sécurité sociale
- PAS à charge du patient qui peut librement partager les informations concernant sa santé et délier les professionnels de leur obligation au secret
- se poursuit au-delà du décès du patient
- évolution vers la multidisciplinarité / travail en équipe + DSP => vers un secret professionnel d'office partagé

ANONYMISATION

Loi 2002 + GDPR

PAS applicable

Empêche irréversiblement l'identification de la personne concernée

Réidentification impossible ou extrêmement compliquée

PSEUDONYMISATION

Loi 2002 + GDPR

applicable

Empêche **REVERSIBLEMENT** l'identification de la personne concernée

Réidentification reste possible au moyen d'autres informations conservées séparément et soumises à des garanties fortes

RESPONSABLE DU TRAITEMENT

Personne physique ou morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, **détermine les finalités et moyens** du traitement

Il est crucial de bien identifier le responsable

Pluralité de responsables du traitement possible

Parfois plusieurs scénarii possibles

SOUS-TRAITANT

Personne physique ou morale, autorité publique, service ou tout autre organisme qui traite des données **pour le compte du responsable** du traitement

NE PAS CONFONDRE
AVEC LE RESPONSABLE DU TRAITEMENT
(parfois plusieurs scénarii possibles)

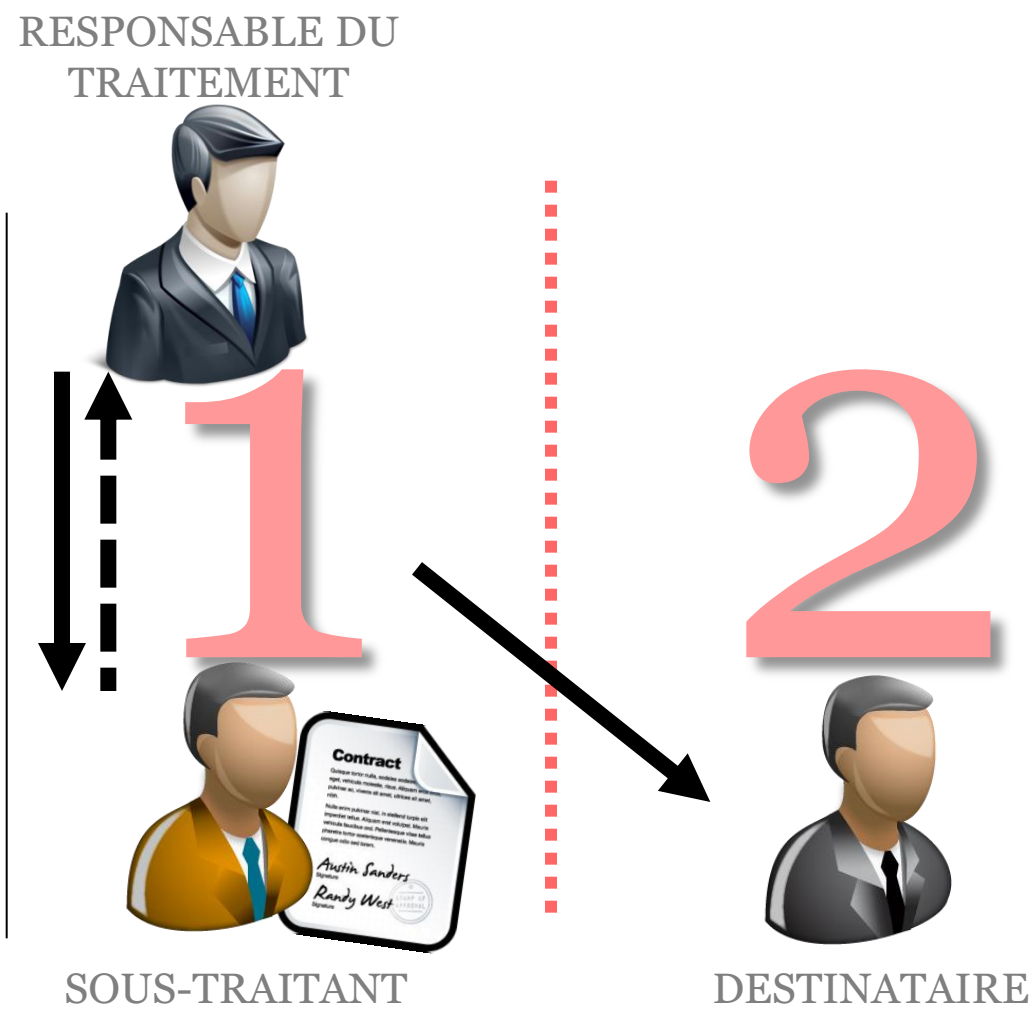
+

OBLIGATION D'AVOIR
UN **CONTRAT DE SOUS-TRAITANCE ÉCRIT**
contenant des clauses imposées par la loi

GDPR: +contenu du contrat: renforcement des obligations

DESTINATAIRE

Personne physique/morale, autorité publique, service ou tout autre organisme qui reçoit communication de données personnelles

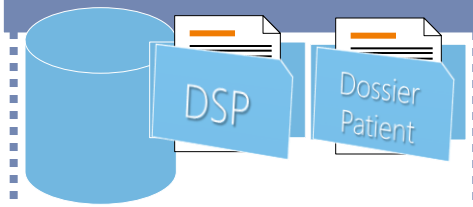


APPLICATION

Agence eSanté

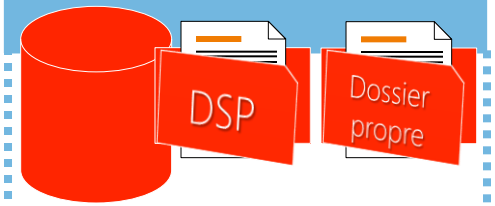
- Mise en place/structure
- Conformité exigences légales
- Gestion accès
- Accès et autres droits patients
- Sécurité

Etablissements hospitaliers
Médecins
Laboratoires
Autres PS / Chercheurs
Réseaux d'aides et sois



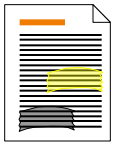
- Contenu (médical/autre)
- Conformité exigences légales
- Gestion accès (incl. Interne)
- Accès et autres droits patients
- Sécurité

CNS
CCSS



- Contenu administratif
- Conformité exigences légales
- Gestion accès (incl. internes)
- Accès et autres droits personnes concernées
- Sécurité

Patient



- Exercice des droits
- Pas de responsabilité quant au traitement

GRAND PRINCIPES

APPLICATION AUX DONNEES DE SANTE

LICEITE, LOYAUTE

LOI ACTUELLE +GDPR

Tout traitement doit être
en conformité avec la loi

Tout traitement doit être conforme
aux grands principes
et respecter les droits
des personnes concernées

QUALITE DES DONNÉES

LOI ACTUELLE +GDPR

Pertinence: données adéquates, pertinentes, non excessives /finalités

Exactitude: données exactes et si nécessaire mises à jour

Rétention proportionnée: uniquement tant que nécessaire pour les finalités

- ✓ Délais de conservation fixés par la loi
- ✓ Délai de prescription
- ✓ Quid quand la loi fixe des délais minimaux?
  Ex: dossier patient : au moins 10 ans après la fin de la prise en charge.

GDPR: +minimisation des données (+durée peut être plus longue si finalité = recherche

FINALITE DU TRAITEMENT

LOI ACTUELLE +GDPR

La finalité est le but recherché par le responsable du traitement et qui justifie le traitement

- les finalités doivent être déterminées à l'avance
- toutes les finalités doivent être divulguées (transparence)
- les finalités doivent être légitimes
- les données ne doivent pas être traitées ultérieurement pour des **finalités incompatibles**

PROPORTIONNALITE

LOI ACTUELLE +GDPR

Clé de voûte du système

- les moyens du traitement doivent être proportionnés à la finalité recherchée
- les actes de traitement doivent être nécessaires à atteindre la finalité recherchée

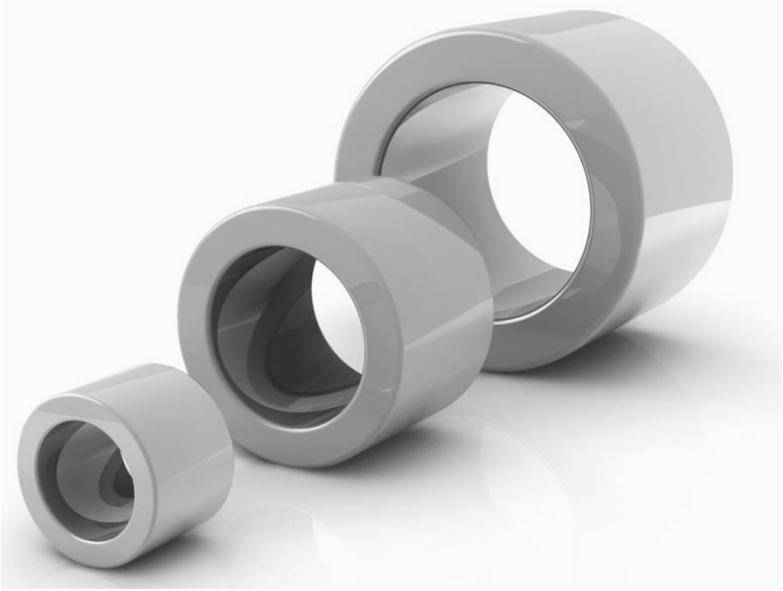
(GDPR) Data minimisation & privacy-by-design

- principe de minimisation: ne collecter que l'indispensable
- *privacy-by-design*: destruction/anonymisation/archivage/sécurisation systématique des données

LEGITIMITE

Un traitement est légitime s'il correspond à l'un des cas d'ouverture prévus par la Loi,qui dépendent du type de traitement…

TRAITEMENT «STANDARD»
DONNÉES SENSIBLES
SECTEUR DE LA SANTÉ
DONNÉES JUDICIAIRES
SURVEILLANCE (TIERS)
SURVEILLANCE (EMPLOYÉS)



LEGITIMITE - DONNEES SENSIBLES

LOI ACTUELLE + GDPR

Un traitement de «données sensibles» (y incluant les données de santé) est légitime si…

- Obligations du responsable (droit du travail/social)
- Mission d'intérêt public, recherche scientifique/historique/statistique (Loi actuelle)*
- Membres association politique, religieuse +consentement
- Exercice, défense d'un droit en justice
- Protection de l'intérêt vital de la personne/d'un tiers +consentement impossible
- Consentement
- Données manifestement rendues publiques par la personne
- Autorisation par RGD (Loi actuelle)

CONSENTEMENT N'EST PAS TOUJOURS OBLIGATOIRE POUR TRAITER DES DONNEES DE SANTE
MAIS PATIENT DOIT CONSENTIR AUX SOINS (SAUF EXCEPTIONS)

LEGITIMITE – INTERET PUBLIC

PRECISION GDPR (1/2)

Les traitements de données sensibles fondés sur l'intérêt public sont possibles pour autant que :

- il s'agisse d'un d'intérêt public important
- fondé sur le droit de l'Union OU
- fondé sur le 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.

LEGITIMITE – INTERET PUBLIC

PRECISION GDPR (2/2)

Les traitements de données sensibles fondés sur la santé publique sont possibles pour :

- des motifs d'intérêt public 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,

- fondé sur le droit de l'Union OU
- fondé sur le droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée (ex: secret professionnel)

LEGITIMITE
DONNEES DE SANTE | SERVICES DE SANTE

LOI ACTUELLE

Un traitement de données de santé et relatives à la vie sexuelle par les services de santé est légitime si…

GDPR

Un traitement de données de santé et de données génétiques par les services de santé est légitime si…

- pour la médecine préventive, les diagnostics médicaux, l' administration de soins et traitements
- pour la gestion des services de santé, sécurité sociale etc.
- pour la prise en charge sanitaire ou sociale,
- […]

+

⇒ par un professionnel de la santé soumis au secret professionnel ou sous sa responsabilité

⇒ par une autre personne soumise à une obligation de secret

CONSENTEMENT N'EST PAS OBLIGATOIRE DANS CES CAS
MAIS PATIENT DOIT CONSENTIR AUX SOINS (SAUF EXCEPTIONS)

LEGITIMITE - DONNEES GENETIQUES

LOI ACTUELLE

Un traitement de données génétiques est légitime si et seulement si…

- vérification d'un lien génétique(preuve en justice, identification d'une personne, prévention ou la répression d'une infraction pénale)
- protection de l'intérêt vital de la personne/d'un tiers +consentement impossible
- mission d'intérêt public notamment à des fins scientifiques/historiques/statistique
- par des instances médicales, pour la médecine préventive, les diagnostics médicaux, l' administration de soins et traitements

Pas de dispositions spécifiques pour les données génétiques

GDPR

LIBERTÉ DES ÉTATS MEMBRES DE MAINTENIR OU INTRODUIRE DES CONDITIONS SUPPLÉMENTAIRES, Y COMPRIS DES LIMITATIONS

LEGITIMITE – RECHERCHE MEDICALE | SCIENTIFIQUE

LOI ACTUELLE

sur données de santé si…

mise en œuvre par des instances médicales,
ou organismes de recherche,
ou personnes physiques ou morales dont le projet de recherche biomédicale a été approuvé

sur données génétiques si…

- consentement exprès (sauf disponibilité légale contraire ou indisponibilité du corps humain)
  OU
- consentement impossible
  + respect conditions fixées par RGD 1992 (données « dépersonnalisées »)

LEGITIMITE – RECHERCHE MEDICALE | SCIENTIFIQUE

GDPR

sur données de santé ou génétiques si...

- nécessaire à des fins de recherche scientifique ou historique ou à des fins statistiques

+

- sur la base du droit de l'Union OU
- 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.

LIBERTÉ DES ÉTATS MEMBRES DE MAINTENIR OU INTRODUIRE DES CONDITIONS SUPPLÉMENTAIRES, Y COMPRIS DES LIMITATIONS

LEGITIMITE ET TRAITEMENT SECONDAIRE

	LOI ACTUELLE	GDPR
PRINCIPES	▪ Licéité des traitements ultérieurs pour des finalités <u>compatibles</u> avec la finalité initiale (+GDPR: info des personnes concernées) compatible»: ce à quoi la personne concernée peut raisonnablement s'attendre au regard des finalités en cause, du contexte de la collecte des données, de la nature des données, des garanties (chiffrement, pseudonymisation) ▪ Interdiction des traitements ultérieurs pour des finalités <u>incompatibles</u> avec la finalité initiale	
EXCEPTION A L'INTERDICTION	consentement des personnes concernées +autorisation CNPD	consentement des personnes concernées

LE TRAITEMENT ULTÉRIEUR À DES FINS ARCHIVISTIQUES DANS L'INTÉRÊT PUBLIC, À DES FINS DE RECHERCHE SCIENTIFIQUE OU HISTORIQUE OU À DES FINS STATISTIQUES = OPÉRATION DE TRAITEMENT LICITE COMPATIBLE

CONSENTEMENT?

1 Libre

2 Spécifique

3 Informé

4 GDPR
+«non-équivoque»
+accord séparé
+sur base d'informations claires

Application au domaine de la recherche ?

Consentement doit pouvoir être donné pour certains domaines de recherche (« *dans le respect des normes éthiques reconnues en matière de recherche scientifique* ») ou pour certaines parties de projets de recherche

Qu'en est-il des mineurs ?

Principe: accord du titulaire de l'autorité parentale
Exception (GDPR): +16ans pour les services en ligne (liberté des EM jusqu'à 13 ans)

≠ Loi D&O du patient où mineur a droit (dans certains cas) d'exercer ses droits à l'égard de sa santé

DROITS DES PERSONNES

INTERACTION AVEC LES DROITS DU PATIENT

DROIT GENERAL A L'INFORMATION

PRINCIPES

Informations à communiquer

- identité du responsable
- finalités du traitement
- destinataires/catégories de destinataires
- caractère obligatoire/facultatif des questions, conséquences éventuelles défaut de réponse
- existence d'un droit d'accès/rectification

GDPR

+coordonnées DPO
+base juridique du traitement
+intérêt légitime poursuivi
+transfert vers pays tiers (niveau de protection local, mesures de sauvegarde)
+durée ou critères de rétention
+droit opposition
+droit effacement
+droit limitation
+droit retrait consentement
+droit réclamation/CNPD
+etc.

= OBLIGATION POUR TOUT RESPONSABLE DE TRAITEMENT QUE LES INFORMATIONS SOIENT OU NON DIRECTEMENT COLLECTEES AUPRES DE LA PERSONNE CONCERNEE

DROIT GENERAL A L'INFORMATION
EXCEPTIONS LIMITEES (GDPR)

- Personnes concernées disposent déjà des infos.
- +Si données non collectées directement auprès de la personne concernée:

✓ Si impossible ou au prix d'efforts disproportionnés (notamment pour la recherche) A CONDITION DE mettre en place des mesures appropriées (telles que rendre les informations publiquement disponibles)

✓ S'il existe des dispositions spécifiques européennes ou nationales relatives à l'obtention ou la communication de ces informations

✓ Si données restent confidentielles en vertu d'une obligation légale au secret professionnel

ATTENTION: NE PAS CONFONDRE AVEC LE DROIT A L'INFORMATION DU PATIENT

DROIT D'ACCES

LOI ACTUELLE +GDPR

DROIT INCONDITIONNEL DE LA PERSONNE CONCERNEE

- confirmation que données sont (ou non) traitées
- informations visées dans droit à l'information
- communication des données
- toute information disponible sur l'origine des données
- logique qui sous-tend tout traitement avec décisions automatisées
- Information relatives aux garanties mises en place en cas de transferts vers un pays tiers

- LOI ACTUELLE: Le responsable peut limiter le droit d'accès si les données sont exclusivement traitées à des fins de recherche scientifique
- GDPR: Liberté des EM de prévoir des exceptions en matière de santé publique, de recherche scientifique ou d'archives constituées dans l'intérêt publique

DROIT D'ACCES – DOSSIER PATIENT | DSP

LOI D&O DU PATIENT

DROIT INCONDITIONNEL DU PATIENT

- droit d'accès (sous 15jours ou - si urgence) au dossier patient et à l'ensemble des informations relatives à sa santé
- droit d'accès direct ou par l'intermédiaire d'un tiers non PS pourvu d'un pouvoir daté et signé par le patient
- droit de s'en faire expliquer le contenu
- droit de consultation et de copie
- droit de se faire assister par son accompagnateur du patient

EXCEPTION : CONSULTATION D'ANNONCE

DSP

- Droit d'accès prévu par l'article 60quater CSS
- Des précisions à attendre sur les modalités de cet accès (RDG à intervenir)

- LOI 2002 : « *L'accès aux données du patient détenus par un prestataire de soins de santé s'exerce conformément aux dispositions de la loi du 24 juillet 2014 relative aux droits et obligations du patient* »
- LOI D&O du patient : « *Sans préjudice des autres dispositions de la présente loi, l'accès du patient à son dossier de soins partagé s'exerce conformément à l'article 60quater du Code de la sécurité sociale* ».

DROIT DE RECTIFICATION

PRINCIPES GENERAUX

- correction d'erreurs ou mise à jour uniquement
- ne pas confondre avec droit d'opposition (qui est conditionnel)

GDPR

+information des destinataires sauf impossibilité ou efforts disproportionnés

+exception pour santé publique

DOSSIER PATIENT

- prestataire/patient, ne peuvent pendant cette durée retirer des éléments pertinents pour la tenue du dossier
- rectification possible sous la responsabilité du prestataire concerné
- toute rectification doit être réversible et documentée

- LOI ACTUELLE: Le responsable peut limiter le droit de rectification si les données sont exclusivement traitées à des fins de recherche scientifique
- GDPR: Liberté des EM de prévoir des exceptions en matière de santé publique, de recherche scientifique ou d'archives constituées dans l'intérêt publique

DROIT D'OPPOSITION

PRINCIPES GENERAUX

- conditionnel: pour des raisons prépondérantes et légitimes tenant à la situation particulière et SAUF traitement résultant d'une disposition légale
- Inconditionnel pour les traitement à des fins de prospection (+obligation d'informer de ce droit)

DOSSIER PATIENT

- Obligation légale pour les établissements hospitaliers et pour tous les PS (corrolaire du droit du patient à un dossier soigneusement tenu)

DSP

- Droit de s'opposer au partage de données au sein d'un dossier de soins partagé

- GDPR => EXCEPTION LIMITEE AU DROIT D'OPPOSITION: recherche nécessaire à une mission d'intérêt public
- GDPR => LIBERTE (RELATIVE) DES EM EN MATIERE DE DONNEES DE SANTE

DROIT A L'EFFACEMENT / DROIT A L'OUBLI

GDPR

PRINCIPES

Sur demande de la personne concernée si:

- données plus nécessaires pour leur finalité
- retrait du consentement sans autre base de légitimité
- droit d'opposition +pas de motif légitime impérieux contraire
- données ont fait l'objet d'un traitement illicite
- effacement requis par la loi

EXCEPTIONS

Si traitement nécessaire à:

- liberté d'expression et d'information
- constatation, exercice ou défense de droits en justice
- traitement prévu par la loi ou mission d'intérêt public
- motifs d'intérêt public/santé publique
- recherche scientifique / historique ou statistiques

OBLIGATIONS DU RESPONSABLE

APPLICATION AUX DONNEES DE SANTE

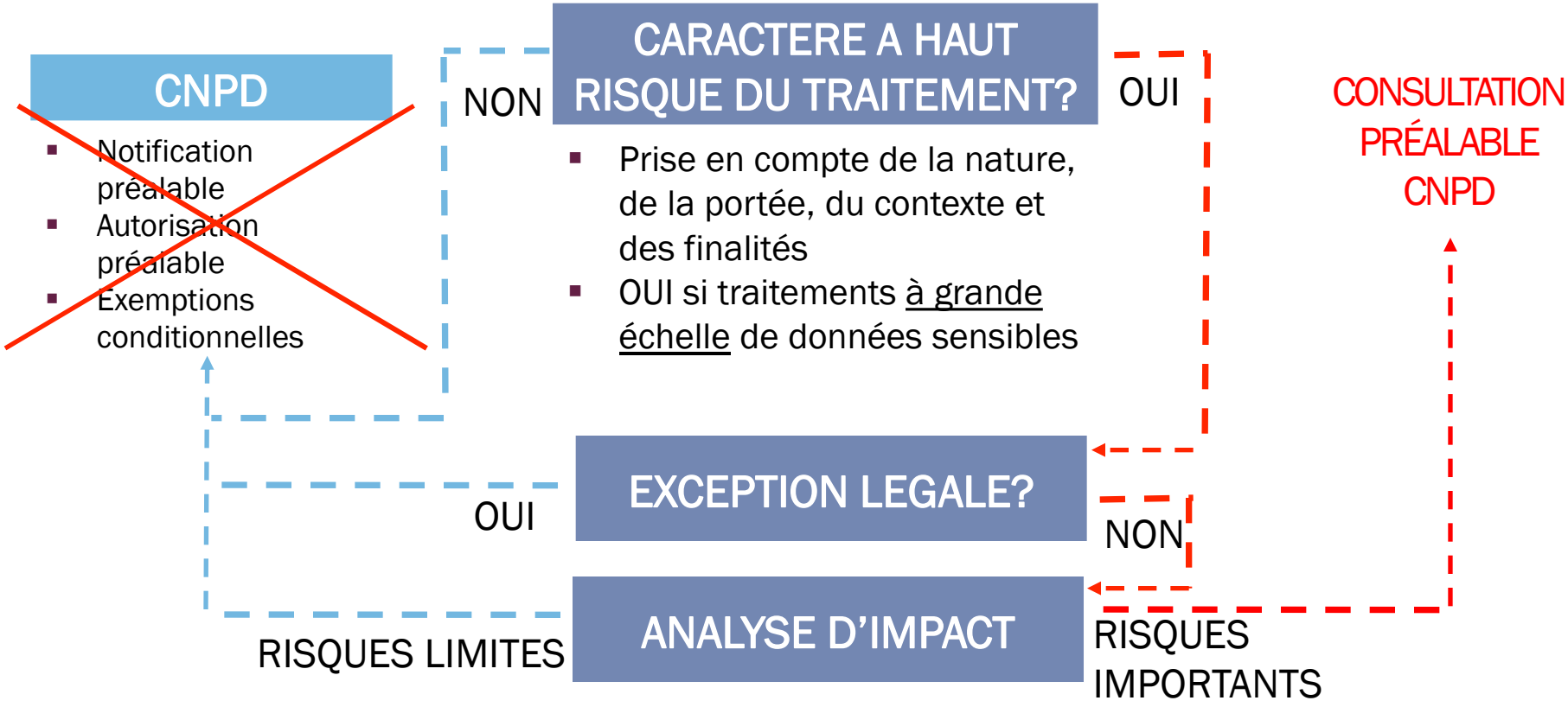
SECURITE

2NDE OBLIGATION PRIMAIRE DU RESPONSABLE:

= garantir un niveau de sécurité dépendant:

- de l'état des connaissances & coûts de mise en œuvre
- de la nature, portée, contexte et finalités du traitement
- risques (probabilité/gravité) pour droits et libertés des personnes

FORMALITÉS ADMINISTRATIVES
⇒ ANALYSE D'IMPACT



- CNPD devra arrêter une liste type des opérations nécessitant une analyse d'impact
- CNPD pourra arrêter une liste type des opérations ne nécessitant PAS une analyse d'impact
- Outil utile : guide CNIL sur PIA

FORMALITÉS ADMINISTRATIVES
⇒ REGISTRE DES ACTIVITES

CNPD

- Notification préalable
- Autorisation préalable
- Exemptions conditionnelles

Registre des activités

- Finalités
- Catégories de personnes concernées
- Catégories de données personnelles
- Catégories de destinataires
- Transferts hors UE + documents justifiant des garanties appropriées
- Délais d'effacement
- Mesures de sécurité

EXCEPTION pour les entreprises de -250 employés
JAMAIS pour les traitements à risque, récurrents ou de données sensibles

Obligation pèse sur responsable du traitement +sous-traitant

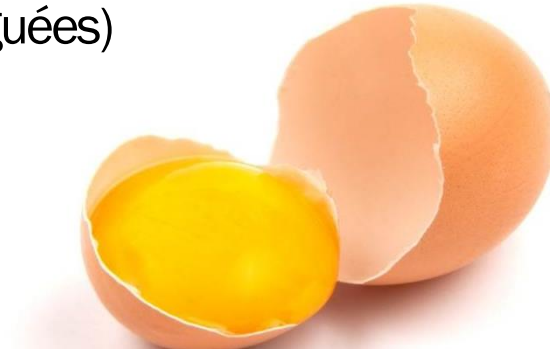
INCIDENTS DE SECURITE
DIVULGATION DE DONNÉES

- LOI ACTUELLE: sanctions pénales applicables mais notification non requise (!)
- GDPR:

✓ obligation d'informer:
- CNPD sous 72h (ou plus tard sur justification)
- personnes concernées dans délai, si leur vie privée est menacée

✓ exception si absence de risque pour les personnes concernées (ex. seules des données pseudonymisées ont été divulguées)

✓ incident doit être documenté (contexte factuel, effets, contre-mesures prises) pour permettre à la CNPD de vérifier la conformité



DELEGUE A LA PROTECTION DES DONNÉES
DPO

STATUT

- employé/externe
- Indépendant
- partage avec d'autres fonctions possible si pas de conflit (RSSI?)
- soumis au secret professionnel

MISSIONS

- associé à toutes les questions de données personnelles
- point de contact des personnes concernées et de la CNPD
- contrôle du respect du RGPD
- conseils sur analyse d'impact
- obligation d'information du responsable de traitement et de ses employés

=> Responsabilité finale reste sur le responsable de traitement / sous-traitant

OBLIGATOIRE pour le responsable/sous-traitant

- si traitement effectué par une autorité publique ou un organisme public
- si traitement exige un suivi régulier et systématique à grande échelle des personnes concernées
- si traitement à grande échelle de données sensibles ou judiciaires

GDPR ET [RÉ]ORGANISATIONS

QUE FAUT-IL FAIRE?

GDPR: QUEL IMPACT ORGANISATIONNEL?

- toute l'organisation est concernée, tout le personnel, toutes les opérations
- la protection des données n'est plus l'affaire des seuls juristes
- la sécurité de l'information n'est plus le domaine réservé des techniciens/IT
  => compétences croisées requises
- DPO doit être regardé comme coordinateur, centre de compétence et conseil
  => travail main dans la main avec RSSI
- importance de la formation du personnel (y compris/à commencer par la direction)
- mise en place d'une approche par les risques
- penser en termes d'auditabilité: tout doit être documenté, tracé et suivi
- éviter l'isolement (avis d'experts externes)

PRENDRE LE TEMPS DE LA RÉFLEXION (18 MOIS ...)
MAIS DÈS MAINTENANT (18 MOIS!)

Questions?

Claire LEONELLI
Avocat à la Cour
cl@claw.lu | (+352) 691 701 000
claw.lu