APDL

Association pour la Protection des Données au Luxembourg

GDPR | HEALTH & RESEARCH

CLAIRE LEONELLI

PERSONAL DATA
PATIENT RIGHTS DU PATIENT

HEALTH DATA

↓

PERSONAL DATA

↓

LAW OF 2002
GDPR

↓

PATIENT

↓↑

HEALTHCARE PROFESSIONAL

↓

LAW OF 2014
« Patient's rights and obligations »

↓

PARTICULAR
RIGHTS & OBLIGATIONS
(non applicable to deceased people)

PARTICULAR
RIGHTS & OBLIGATIONS
(including for deceased patients)

⇒DIFFERENT SCOPE OF APPLICATION
⇒SOME OVER LAPS

GDPR “in a nutshell”

- EU Regulation = stronger harmonisation within EU
- Purpose: make data protection a component of governance organisations
- Infantile paperwork replaced by «*accountability*»
- Organizations must take data protection into account for any activity, any project
- Considering risks, staff must be trained to new rules
- Reinforced rights and new rights for data subjects
- High level of compliance expected
- Huge sanctions (up to EUR20mio/4% of annual global turnover)

AGE OF MATURITY

DEFINITIONS

REMINDER OF KEY CONCEPTS

PERSONAL DATA

Any information of any kind relating DIRECTLY OR INDIRECTLY to an identified or identifiable natural person

- Name, birth date, address
- Voice, image
- Email address
- ID number
- Cultural, social or economic origin
- Police and judicial data
- Healh data
- Biometric data
- Etc.

GDPR: +online identifier and et geo-tracking

PROCESSING

CURRENT LAW + GDPR

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means,

such as:

- collection
- recording
- organisation
- structuring
- storage
- adaptation
- alteration
- retrieval
- consultation
- use
- disclosure by transmission
- alignment or combination
- dissemination or otherwise making available,
- Restriction
- erasure or destruction

VERY LARGE DEFINITION

COVER ANY ACTION OF HANDLING OR EXPLOITATION OF DATA (INCLUDING FOR RESEARCH PURPOSES)

HEALTH DATA

Personal data related to the past, current or future physical or mental health status of a natural person

- Data collected during registration for health care
- Specific numbers or elements assigned for unique identification for health purposes
- Information obtained from tests or examinations, including from genetic data and biological samples
- Any information about illness, disability, risk of illness, medical history, clinical treatment or physiological or biomedical state, regardless of source

GENETIC DATA

Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from

an analysis of a biological sample

chromosomal analyse

DNA or RBA analysis,

etc.

BIOMETRIC DATA

Personal data resulting from specific technical processing
relating to the physical, physiological or behavioural characteristics of a natural person,
which allow or confirm the unique identification of that natural person (such as facial images or dactyloscopic data)

Genetic data = particular health data
Biometric data ≠ health data (as such)

WHAT'S SPECIAL ABOUT HEALTH DATA

SENSITIVE DATA

PROCESSING PROHIBITED IN PRINCIPLE

EXCEPT SPECIFIC GROUNDS OF LEGITIMACY

PROFESSIONAL SECRET

- Legal and ethical obligation of health professionals and social security bodies
- NOT on the patient who can freely share information about his/her health and release medical professionals from their obligation to secrecy
- Continues beyond the death of the patient
- Evolution towards multidisciplinarity / teamwork + « DOSSIER DE SOINS PARTAGÉ » => towards a shared professional secret

ANONYMISATION

CURRENT LAW + GDPR

NOT applicable

IRREVERSIBLY prevents the identification of the data subject

Identification impossible or extremely complicated

PSEUDONYMISATION

CURRENT LAW + GDPR

applicable

REVERSIBLY prevent the identification of the data subject

Reidentification remains possible by means of other information kept separately and subject to strong safeguards

DATA CONTROLLER

Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

It is crucial to identify the data controller

Plurality of data controllers possible

Sometimes several possil scenarios

DATA PROCESSOR

Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

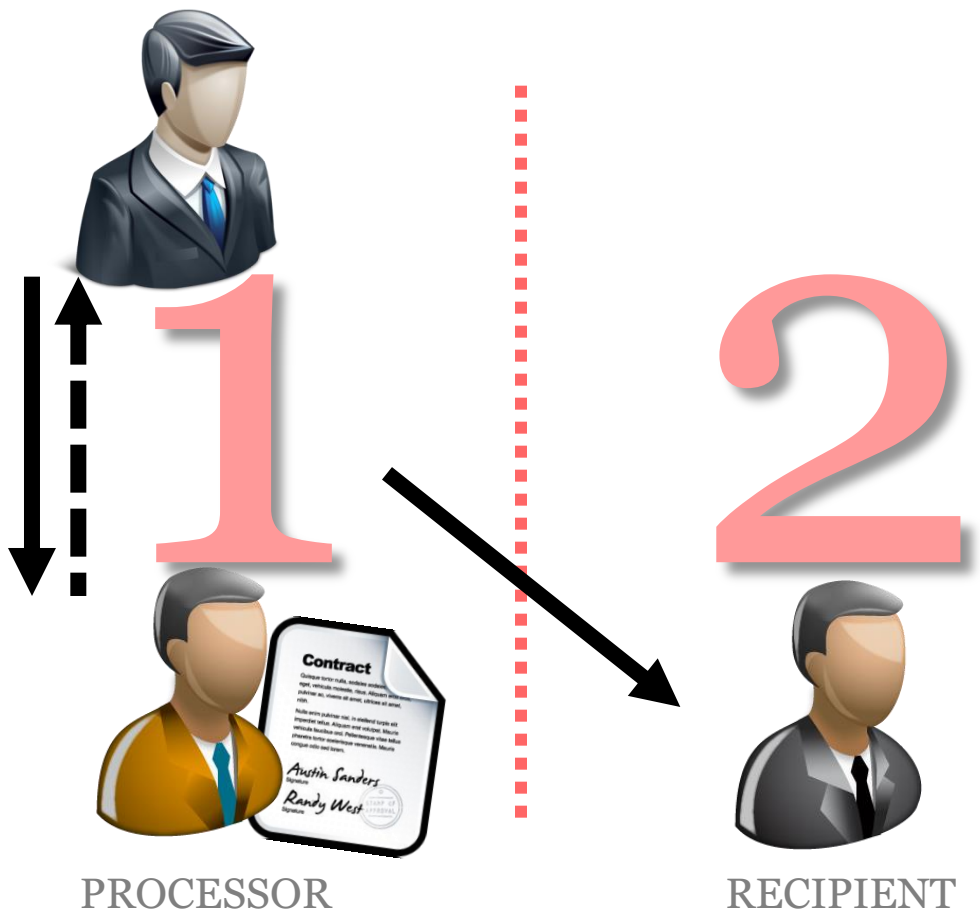
DO NOT CONFUSE
WITH DATA CONTROLLER
(sometimes several scenarios possible)

OBLIGATION TO HAVE
A WRITTEN SUBCONTRACT
containing clauses imposed by law

GDPR: +content of subcontract: reinforcement of processor's obligations

RECIPIENT

Natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

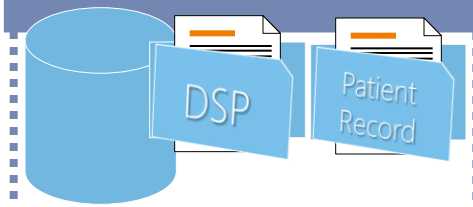


APPLICATION

Agence eSanté

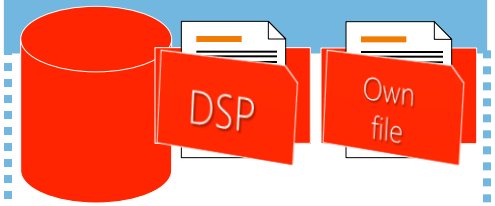
- Implementation / structure
- Compliance with the law (DSP)
- Access management
- Access and other patient rights
- Availability, security

Hospitals
Doctors
Laboratories
Other HCP
Aid & care networks



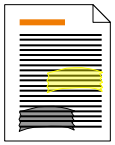
- Content (medical / other)
- Compliance with legal requirements applicable to providers
- Access and other patient rights
- security

CNS
CCSS



- Administrative contentC
- Compliance with legal requirements applicable to providers
- Access and other patient rights
- Security

Patient



- Exercise of rights
- Not accountable for processing

MAIN PRINCIPLES

APPLICATION to health data

LAWFULNESS, LOYALTY

CURRENT LAW +GDPR

Any processing must comply with the law

Any processing must comply with the the main principles and respect the rights of data subjects

DATA QUALITY

CURRENT LAW +GDPR

Relevance: adequate, relevant, non-excessive data / purposes

Accuracy: accurate data and if necessary updates

Proportionate retention: only as necessary for the purposes

- ✓ Storage periods stated by law
- ✓ Limitation periods for court actions
- ✓ When the law only states minimum period of storage?
  Ex: patient record: at least 10 years after the end of patient care.

GDPR: +data minimisation
+length of storage can be longer if data are used for research purposes

PROCESSING PURPOSES

CURRENT LAW +GDPR

The purpose is the aim sought by the data controller that justifies the processing

- The purposes must be determined in advance
- All purposes must be disclosed (transparency)
- The purposes must be legitimate
- The data must not be processed later for incompatible purposes

PROPORTIONALITY
CURRENT LAW +GDPR

Keystone of the system

- Processing means must be proportionate to the purpose sought
- Processing activities must be necessary to achieve the desired objective

(GDPR) Data minimization & privacy-by-design

- Principle of minimization: collecting only the indispensable
- Privacy-by-design: destruction / anonymization / archiving / systematic data security

LAWFULLNESS

A processing is lawful only if it meets one of the grounds stated by GDPR, which depend upon the type of processing…

«STANDARD» PROCESSING
SENSITIVE DATA
HEALTH DATA
JUDICIAL DATA
MONITORING (THIRD PARTIES)
MONITORING (EMPLOYEES)

LAWFULLNESS – SENSITIVE DATA

CURRENT LAW + GDPR

A processing of "sensitive data" (including health data) is lawful if…

- Obligations of data controller (employment and social law)
- Public interest mission, scientific / historical / statistical research*
- Members political association, religious + disclosure with consent
- Exercise, defense of a legal right
- Protection of the vital interest of the person / of a third party?
  + consent impossible
- Consent
- Data manifestly made public by the data subject
- Authorization by national regulation

CONSENT IS NOT ALWAYS REQUIRED TO PROCESS HEALTH DATA
BUT PATIENT MUST CONSENT TO CARE (UNLESS EXCEPTIONS)

LAWFULLNESS– PUBLIC INTEREST

CLARIFICATION GDPR (1/2)

Processing of sensitive data based on public interest are allowed provided:

- the public interest is substantial
- on the basis of Union law OR
- on the basis of a Member State law which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

LAWFULLNESS– PUBLIC INTEREST
CLARIFICATION GDPR (2/2)

Processing of sensitive data based on public health are allowed provided:

- Reasons of public interest such as protecting against serious cross-border threats to health OR
- ensuring high standards of quality and safety of health care and of medicinal products or medical devices,

- on the basis of Union law, OR
- On the law of a Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

LAWFULLNESS
HEALTH DATA| HEALTH SERVICES

CURRENT LAW

Processing of health data and data concerning sexual life are allowed for…

- for preventive medicine, medical diagnosis, care and treatment
- for the management of health services, social security, etc.
- for health and social care,
- […]

GDPR

Processing of health data and genetic data are allowed for…

+

⇒ By a health professional bound to professional secrecy or under his / her responsibility

⇒ By another person bound to an obligation of secrecy

CONSENT OF THE PATIENT IS NOT REQUIRED TO PROCESS HIS/HER DATA IN THESE CASES
BUT PATIENT MUST CONSENT TO CARE (EXCEPT SPECIFIC CASES)

LAWFULLNESS – GENETIC DATA

CURRENT LAW

Processing of genetic data is lawful if...

- Verification of a genetic link (legal evidence, identification of a person, prevention or repression of a criminal offense)
- Protection of the vital interest of the person / of a third party
  + consent impossible
- Public interest mission, scientific / historical / statistical research
- By medical authorities, for preventive medicine, medical diagnosis, care and treatment

No special provisions for genetic data

GDPR

FREEDOM OF MEMBER STATES TO MAINTAIN OR INTRODUCE ADDITIONAL CONDITIONS, INCLUDING LIMITATIONS

LAWFULNESS– MEDICAL| SCIENTIFIC RESEARCH

CURRENT LAW

ON HEALTH DATA IF…

Implemented by medical bodies, or research organizations, or natural or legal persons whose biomedical research project has been approved

ON GENETIC DATA IF…

- Express consent (unless contrary legal availability or unavailability of the human body), OR
- Consent not possible + compliance conditions set by Grand-Ducal Regulation

LAWFULNESS– MEDICAL| SCIENTIFIC RESEARCH
GDPR

on health or genetic data if…

- necessary for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes

+

- on the basis of Union law OR
- On the law of a Member State that must be proportionate to the objective pursued, must respect the essence of the right to data protection and provide for appropriate and specific measures to safeguard the fundamental rights and interests of the data subjects

FREEDOM OF MEMBER STATES TO MAINTAIN OR INTRODUCE ADDITIONAL CONDITIONS, INCLUDING LIMITATIONS

LAWFULNESS – FURTHER PROCESSING

	CURRENT LAW	GDPR
PRINCIPLES	▪ Legality of subsequent processing for purposes compatible with the original purpose (+ GDPR: info of the data subjects) Compatible ": what the data subject can reasonably expect with regard to the purposes in question, the context of the data collection, the nature of the data, the guarantees (encryption, pseudonymisation) ▪ Prohibition of subsequent processing for purposes incompatible with the original purpose	
EXCEPTION TO PROHIBITION	consent of data subjects +autorisation CNPD	consent of data subjects

SUBSEQUENT PROCESSING FOR ARCHIVAL PURPOSES IN THE PUBLIC INTEREST FOR SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR FOR STATISTICAL PURPOSES = COMPATIBLE PROCESSING OPERATION

CONSENT?

1 Free

2 Specific

3 Informed

4 GDPR
+«unambiguous»
+separate agreement
+on the basis of clear agreement

Application to the research field?

Consent should be granted to certain areas of scientific research ("*when in keeping with recognised ethical standards for scientific research*") or parts of research projects

What about minors?

Principle: agreement of the holder of parental authority
Exception (GDPR): + 16 years for online services (freedom of EM up to 13 years)

≠ Law on Patient's rights & obligations where minors are (in certain cases) entitled to exercice their rights related to their health

DATA SUBJECTS' RIGHTS

INTERACTION WITH PATIENTS' RIGHTS

GENERAL RIGHT TO BE INFORMED

PRINCIPLES

Information to provide

- Identity of the controller
- Processing's purposes
- Recipients /categories of receipients
- Compulsory / optional nature of questions, possible consequences lack of response
- Existence of a right of access / rectification

GDPR

+DPO details
+Legal basis of processins
+ Legitimate interest pursued
+ Transfer to third countries (level of local protection, safeguard measures)
+ Duration or retention criteria
+ Right of opposition
+ Right of erasure
+ Rights limitation
+ Right of consent withdrawal
+ Right to claim / CNPD
+ Etc.

= OBLIGATION FOR ANY CONTROLLER REGARDLESS DATA ARE OR NOT DIRECTLY COLLECTED BEFORE THE DATA SUBJECT

GENERAL RIGHT TO BE INFORMED
FEW EXCEPTIONS (GDPR)

- Data subject already have the information
- If data not collected directly from the data subject if:

✓ impossible or through disproportionate efforts (especially for research) PROVIDED to put in place appropriate measures (such as making information publicly available)

✓ obtaining or communicating such information is laid down by specific European or national provisions

✓ data remain confidential under a legal obligation of professional secrecy

WARNING: DO NOT CONFUSE WITH THE PATIENT'S RIGHT OF INFORMATION

RIGHT OF ACCESS

CURRENT LAW +GDPR

UNCONDITIONAL ACCESS OF DATA SUBJECTS

- Confirmation that data are (or are not) processed
- Access to data
- Any information covered by the right of information (purposes, categories of personal data, recipients, etc.)
- Any information available on their origin
- Logic that underlies any processing with automated decisions
- Appropriate safeguards in place when data are transferred to a third country

- CURRENT LAW: Controller may limit the right of access if the data are exclusively processed for the purpose of scientific research
- GDPR: Freedom of Member State to provide for exceptions in public health, scientific research or archives constituted in the public interest

RIGHT OF ACCESS– PATIENT RECORD | DSP

PATIENT R&O LAW

PATIENT UNCONDITIONNAL RIGHT

- Right of access to the patient record and all health information held by a healthcare provider or other medical authority in any capacity whatsoever
- Right of direct access or via a non-healthcare professional with a power dated and signed by the patient
- Right to have the record's content explained
- Right of consultation and copying
- Right to be assisted by his / her "patient attendant" ("accompagnateur")

EXCEPTION : 'ANNOUCEMENT VISIT '

DSP

- Right of access set forth by Article 60quater CSS
- Clarifications to be expected (upcoming RDG)

- 2002 LAW : « *Access to patient data held by a healthcare provider is exercised in accordance with the provisions of the Law of 24 July 2014 on the rights and obligations of the patient*»
- PATIENT R&O LAW: « *Without prejudice to the other provisions of this law, access to the patient's* (DSP) *is exercised in accordance with Article 60quater of the Social Security Code ».*

RIGHT TO RECTIFICATION

GENERAL PRINCIPLES

- Only error correction or update only
- Not to be confused with right to object (which is conditional)

PATIENT RECORD

- Provider / patient cannot withdraw material relevant to the record
- Rectification under the responsibility of the service provider concerned
- Any rectification must be reversible and documented

- CURRENT LAW: Controller may limit the right of access if the data are exclusively processed for the purpose of scientific research
- GDPR: Freedom of Member State to provide for exceptions in public health, scientific research or archives constituted in the public interest

RIGHT TO OBJECT

GENERAL PRINCIPAL

- conditional: for preponderant and legitimate reasons relating to the particular situation and EXCEPT processing resulting from a legal provision
- unconditional: processing for prospecting purposes (+ obligation to inform data subject of this right)
- unconditional: before first communication of data to third parties or use on behalf of third parties for prospecting purposesc

PATIENT RECORD

- Legal obligation for hospitals and for all HCP (corollary of the right of the patient to a record carefully kept)

DSP

- Right to object to data sharing within a shared care record

- GDPR => LIMITED EXCEPTION TO THE RIGHT TO OBJECT: Research required for a mission of public interest
- GDPR => FREEDOM OF MEMBER STATE FOR HEALTH DATA

RIGHT TO ERASURE /'RIGHT TO BE FORGOTTEN'

GDPR

PRINCIPLES

At the request of the data subject if:

- Data are no longer needed for their purpose
- Withdrawal of consent without any other basis of legitimacy
- Right to object
  + no compelling legitimate reason to the contrary
- Data ave been unlawfully processed treatment
- Deletion required by law

EXCEPTIONS

If processing is justified by/for:

- freedom of expression and information
- public interest or legal provisions
- reasons of public interest / public health
- scientific / historical research or statistics
- recognition, exercise or defense of legal rights

+ If the data were made public inform other controllers that the data subject has requested the deletion of the data, copies and links,
unless impossibility / disproportionate efforts and according to available technologies and implementation costsBy reasonable measures

DATA CONTROLER'S OBLIGATIONS

APPLICATION TO HEALTH DATA

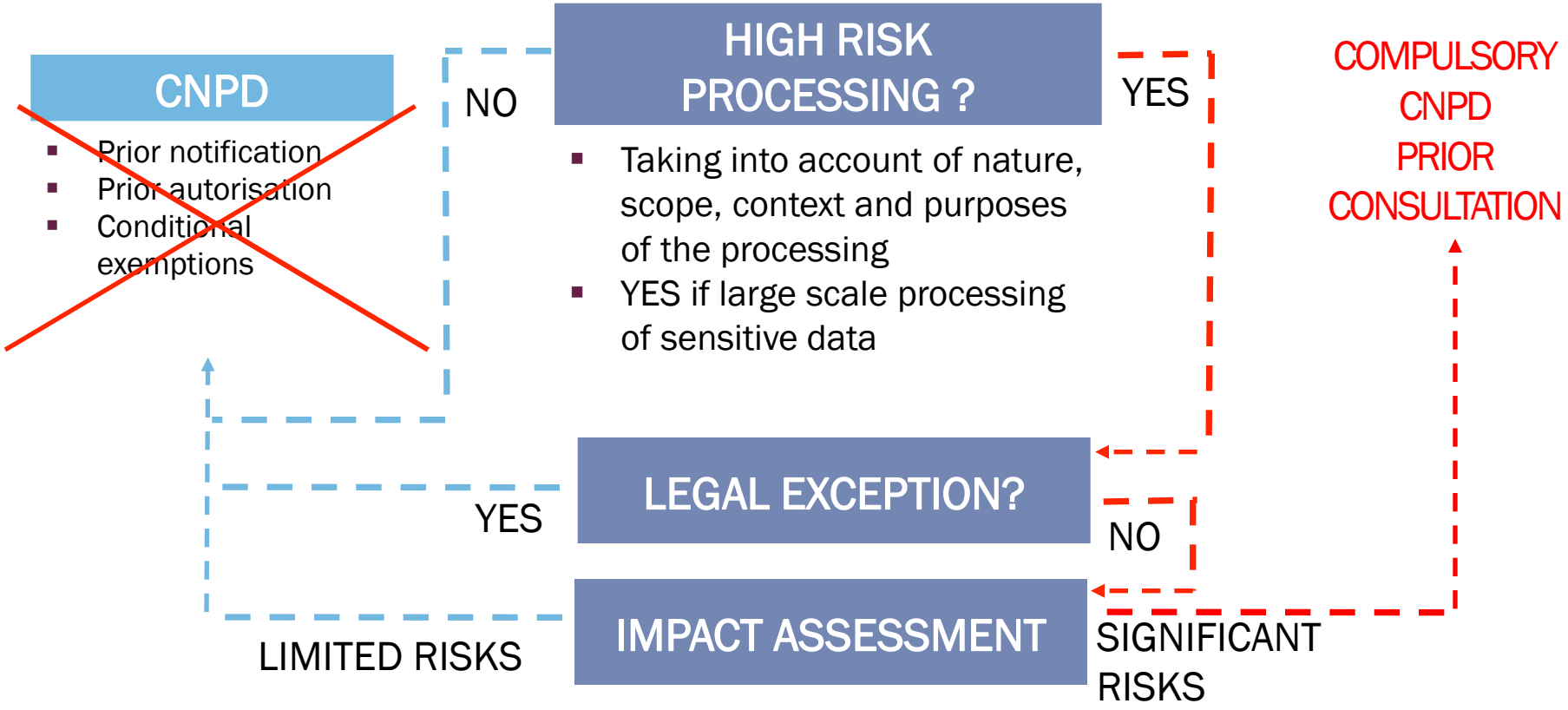
SECURITY

2ND PRIMARY OBLIGATION OF CONTROLLER:

= guarantee a level of security which depends upon:

- the state of knowledge & implementation costs
- nature, scope, context and purpose of processing
- risks (probability / severity) for human rights and freedoms

ADMINISTRATIVE FORMALITIES ⇒ IMPACT ASSESSMENT



- CNPD shall draw up a standard list of operations requiring an impact assessment
- CNPD may establish a standard list of operations NOT requiring an impact assessment
- Useful tool: CNIL guide on PIA

ADMINISTRATIVE FORMALITIES
⇒ RECORDS OF PROCESSING ACTIVITIES

CNPD

- Prior notification
- Prior autorisation
- Conditional exemptions

RECORD OF PROCESSING ACTIVITIES

- Purposes
- Categories of data subjects
- Categories ofpersonal data
- Categories of recipients
- Transfers to third countries + documents justifying appropriate guarantees
- Time limits for erasure
- Security measures

EXCEPTION organisation of - 250 employees
NEVER for risky processing, not occassional processing or processing of sensitive data

Obligation lies on
Data contoller
+ processor

SECURITY INCIDENTS
DATA BREACH

- CURRENT LAW: applicable penal sanctions but notification not required (!)
- GDPR:

✓ Obligation of inform:
- CNPD within72h (or later on justification)
- data subjects without delay, if their privacy is threathened

✓ Exception if there is no risk for data subjects (i.e. disclosure of pseudonysed data)

✓ Incident must be documented
(factual context, effects, counter-measures taken)

DATA PROTECTION OFFICER

DPO

STATUS

- Employee/external
- Independent
- Sharing with other functions possible if no conflict (RSIS?)
- Bound to professional secrecy

MISSIONS

- Associated to all personal data issues
- Point of contact of the data subjects and the CNPD
- Compliance with the GDPR
- Advice on impact assessment
- Obligation to inform the controller and its employees

⇒ Final liability remains on data controller / processor

COMPULSORY for controller/processor
si traitement effectué par une autorité publique ou un organisme public

- If processing by a public authority or a public body
- If treatment requires regular and systematic monitoring on a large scale of data subjects
- If large-scale processing of sensitive data or judicial data

GDPR & [RE]ORGANISATION

WHAT SHOULD BE DONE?

GDPR: WHAT ORGANIZATIONAL IMPACT?

- The whole organization is concerned, all staff, all operations
- Data protection is no longer a matter only for lawyers
- Security of information is no longer the reserved domain of technicians / IT
  => Required cross competencies
- DPO should be looked at as coordinator, center of competence and advisor
  => Work hand in hand with RSIS
- Importance of staff training (including / to begin with management)
- Implementation of a risk-based approach
- Think in terms of auditability: everything must be documented, traced and monitored
- Avoid isolation (advice from external experts)

TAKE TIME TO THINK ABOUT IT (2 years)....
... BUT NOW (2 YEARS)

Questions?

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