VINCENT BIRLOUEZ

# THE GENERAL DATA PROTECTION REGULATION

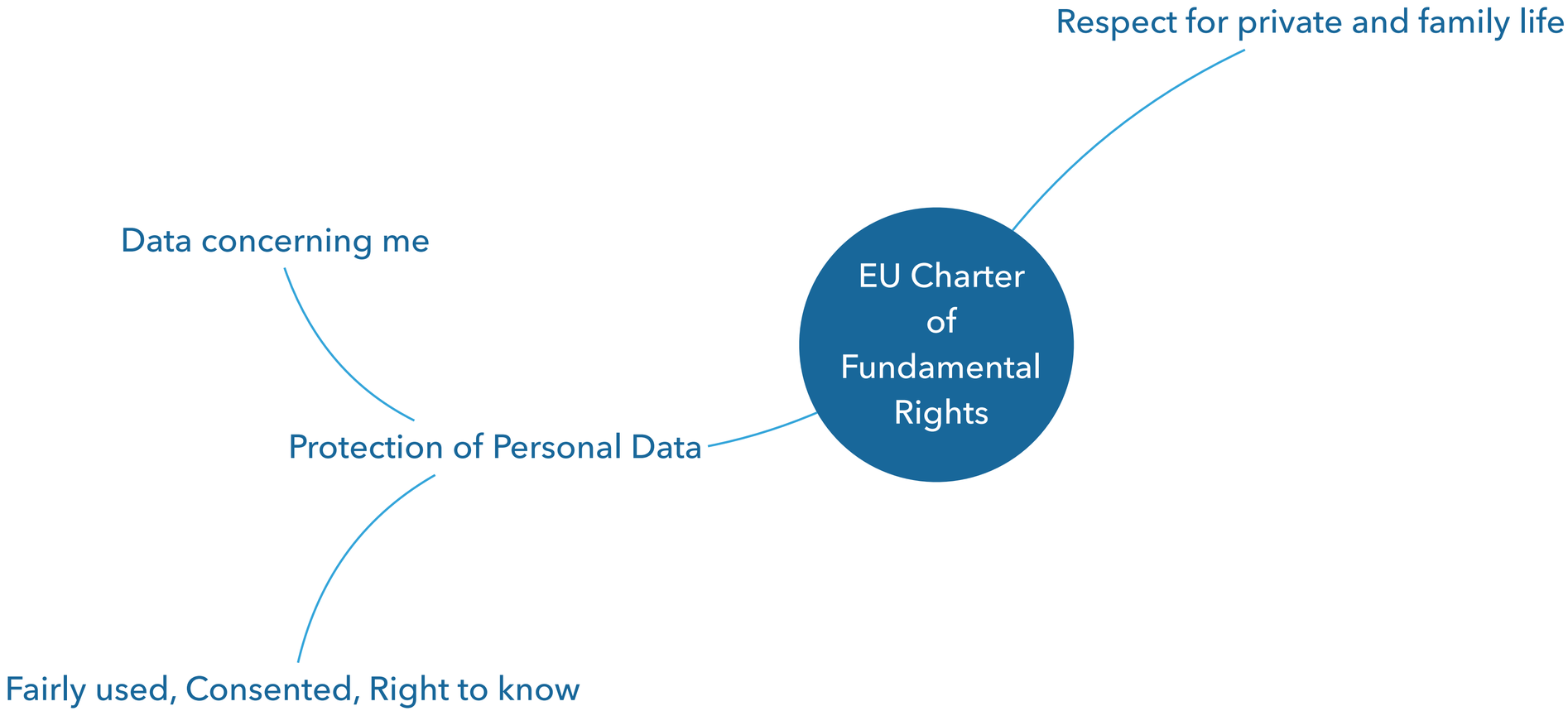
# TODAY'S OBJECTIVES

- Raise awareness of the data protection law
- Understand the type of actions you might need to take
- Answer any questions



# GDPR OVERVIEW

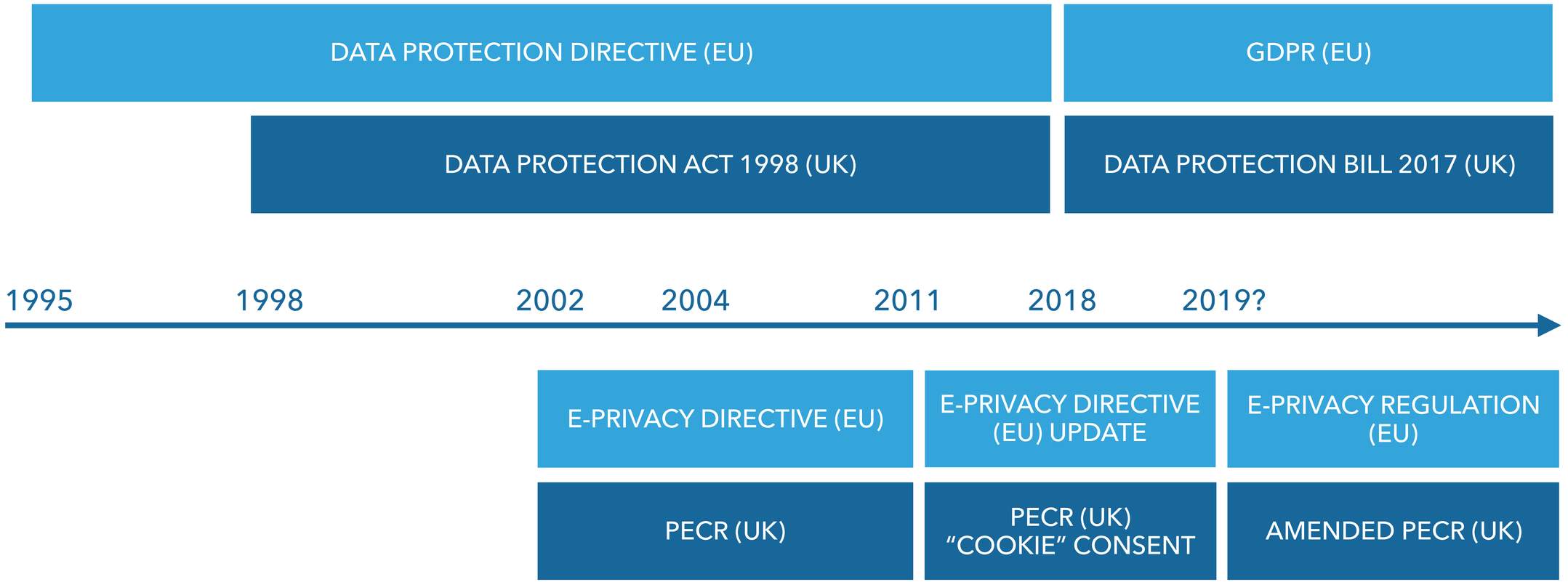
# WHAT IS DATA PROTECTION?



# OBJECTIVES OF THE GDPR

- Put citizens back in control of their own data
- Ensure strong enforcement of rules
- Set data protection standards worldwide

# EVOLUTION OF THE LAW



# THE GENERAL DATA PROTECTION REGULATION

(99 ARTICLES)

# WHAT IS PERSONAL DATA?

"Any information relating to an identified or identifiable natural person"

## SPOT THE DIFFERENCE





# ONE HAS PRINCIPLES

# PRINCIPLES (ART 5.)

**Responsible** for

Able to **demonstrate compliance** with

**"Accountability"**

**Personal data shall be:**

1. processed **lawfully**, **fairly** and in a **transparent** manner
2. collected for specified, explicit and legitimate purpose and not further processed in a manner incompatible with the purpose (**purpose limitation**)
3. adequate, relevant, and limited to what is **necessary** (**data minimisation**)
4. accurate and kept up-to-date, non-accurate data are erased or rectified (**accuracy**)
5. kept for no longer than what is necessary (**storage limitation**)
6. kept secured using appropriate **technical or organisation measures** (**integrity and confidentiality**)

New with GDPR



Apply those principles when dealing with personal data.
Make it part of your organisation's DNA.

# LAWFUL – WHAT IS THE JUSTIFICATION FOR COLLECTING THE DATA?

**CONSENT**

- Can be withdrawn (easily)
- Freely given: can't rely on consent if consent is required for the performance of a contract when consent not actually needed.
- A consent for each purpose.
- NOTE: if the current consent is not aligned to GDPR you need to re-consent before May 2018.

**PERFORMANCE OF A CONTRACT**

- You can't enter the contract without some personal data
- Does not mean you can use this to collect any data!

**LEGITIMATE INTEREST**

- Processing is necessary for the purpose of legitimate interest pursued by the controller
- EXCEPT when such interests are overridden by the interests OR fundamental rights and freedoms of the data subject
- Could require a balancing test: Legitimate Interest Assessment

**COMPLIANCE WITH LEGAL OBLIGATION**

- Processing is necessary for compliance with a legal obligation

**PUBLIC INTEREST / EXERCISE OF OFFICIAL AUTHORITY**

**PROTECT VITAL INTEREST OF NATURAL PERSON**



Know your data…document what you do with it and review the lawful basis for processing.

# DATA SUBJECTS RIGHTS

| Rights | What Is It? |
|---|---|
| Information | Inform the data subject when collection personal data: the purpose, the lawful basis, …<br>This is the "Privacy Notice" found on website. It must be concise, transparent, intelligible. |
| Rectification | The right to rectify inaccurate data. |
| Access | The right to know and get a copy of the personal data concerning the data subject |
| Erasure | Right to be forgotten. Delete me! |
| Data Portability | Right to get a copy of the information the data subject has provided |
| Restriction | Right to stop using my data…so just keep a copy of it and only use it when the data subject lift the restriction |
| Object | Right to object to processing (stop processing): marketing, profiling, … |



Create procedure to deal with those rights. Review your privacy policy and privacy notice.

# OBLIGATIONS

You process personal data → This creates a risk for rights and freedoms of the data subjects

You have to implement "**appropriate**" "**technical** and **organisational measures**" to be **compliant** and be able to **demonstrate** you are.

## Data Protection by Design (art. 25)

## Data Protection by Default (art. 25)

- Data minimisation
- Only personal data necessary
- Limit access to personal data
- Maximum privacy by default

## Security (art. 32)

- Encryption
- Ensure confidentiality, integrity availability and resilience
- Restore availability of services and access to personal data from incidents in a timely manner
- Regular testing, assessment and evaluation of effectiveness of security measures

## Processors (3rd parties)

- Ensure processors / 3rd parties have appropriate measures in place (contract)

## Data Breach Reporting

- Log incidents
- Report data breaches to ICO when there is a risk to data subjects
- Report data breaches to data subjects when it's a high risk

## Data Protection Officer

- Appoint a data protection officer in certain situation depending on the type of data processing

## DPIA

- Conduct DPIA before creating new processing activity that are likely to create high risks to data subjects



Review your security measures
Review your 3rd parties (suppliers)
Create a data breach reporting procedure
Check if you need a DPO and perform DPIA if needed

# PROCESSORS AND CONTROLLERS

Art 28

## CONTROLLER

Determine the purpose and mean of processing.
“Responsable du traitement”

## PROCESSOR

Process data on behalf of a controller.
“Sous-traitant”

Must be governed by a contract.



Controller - Processor Contract

Processor:

- Cannot engage another processor without authorisation of controller (possibility to object)
- Process data on documented instructions from controller
- Set-out: subject matter and duration of processing, nature and purpose, type of personal data, category of data subjects
- Implement security measures
- Support controller with data subjects requests (rights)
- Assist controller with data breach reporting and others
- Assist controller with compliance efforts (audits, …)
- Inform controller if - in his opinion - instructions infringes the regulation
- Establish contract with sub-processors with same obligations
- Can use Code of conducts or Certification to demonstrate compliance



Contracts standard clauses (ICO guidelines)

# RECORD OF PROCESSING ACTIVITIES

Art 30

A document you need to make available to the Supervisory Authority, on request.

## Controller

- Name and contact details of controller, the controller's representative and the DPO (where applicable)
- Purposes of processing
- Category of personal data and category of data subjects
- Category of recipients being disclosed with the personal data, and to which country if applicable
- Time limit for erasure of data
- Security measures (art. 32)

## Processor

- Name and contact details of processor(s) and of each controller, the controller's representative and the DPO (where applicable)
- Categories of processing
- Category of recipients being disclosed with the personal data, and to which country if applicable
- Security measures (art. 32)



ICO template

# ACTION PLAN



# ACTION PLAN

## Awareness
Ensure management is aware of the GDPR and understand the impact on the organisation.

## Know the information you hold
Document the information you have and who you share it with. Understand what lawful basis is most appropriate.

## Individual rights
Have procedures in place to deal with data subjects rights: access, delete, portability.

## Children
You need to seek parental consent to process data related to children

## Consent
You should be able to demonstrate that you have obtain a valid consent. You need to record every consent.

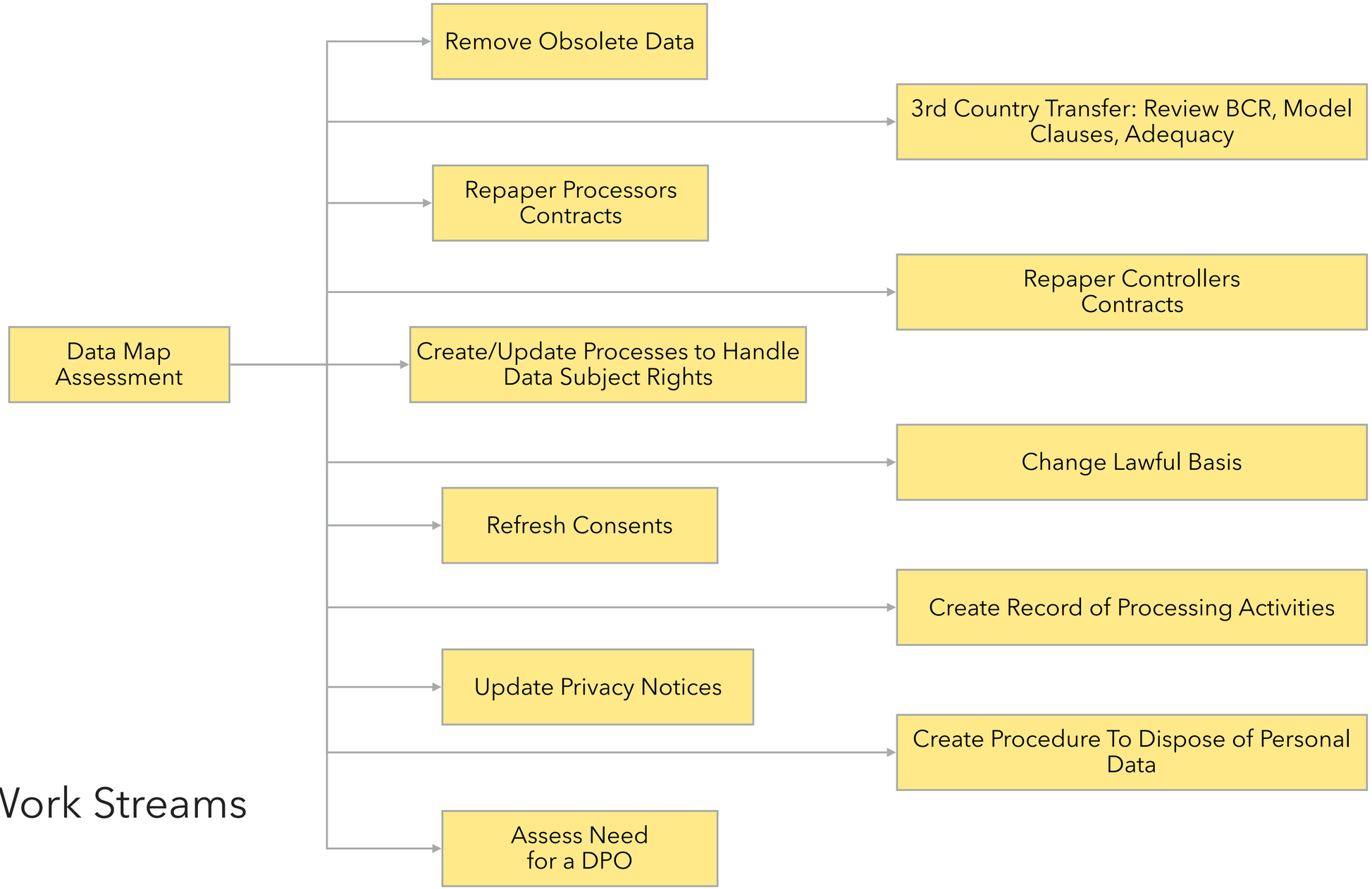
## Data Protection by Design, by Default, Security
You should review your IT Security practices and what data protection by design and by default could mean to you.

## Communicating privacy information
Review your privacy notice and update your data protection policies

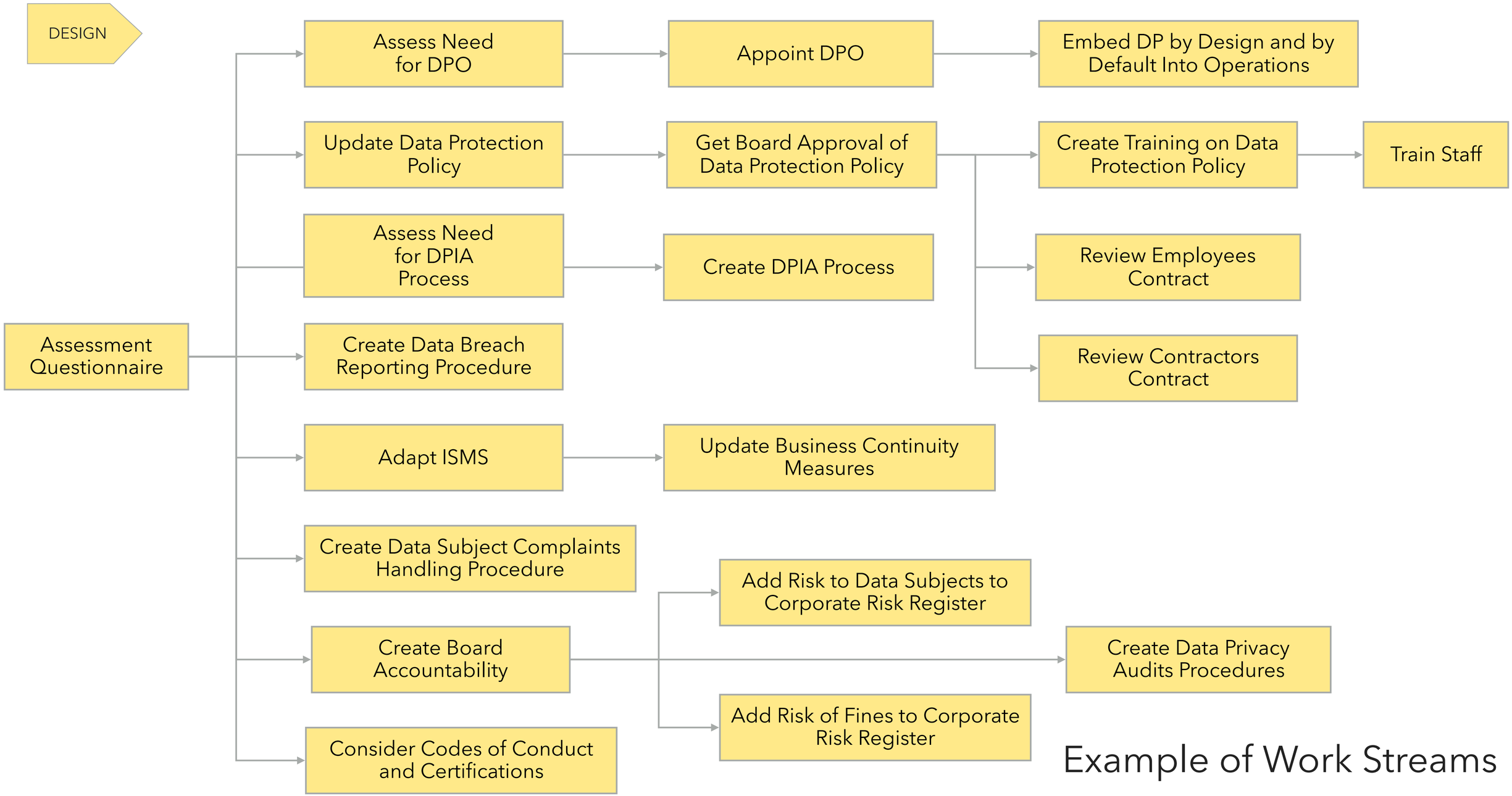
## Data Protection Officer
Somebody should be owning the data protection compliance.

## Data Breaches
You should have the right procedures in place to detect, report and investigate data breaches.

DESIGN




# Example of Work Streams




# Example of Work Streams

# Q&A