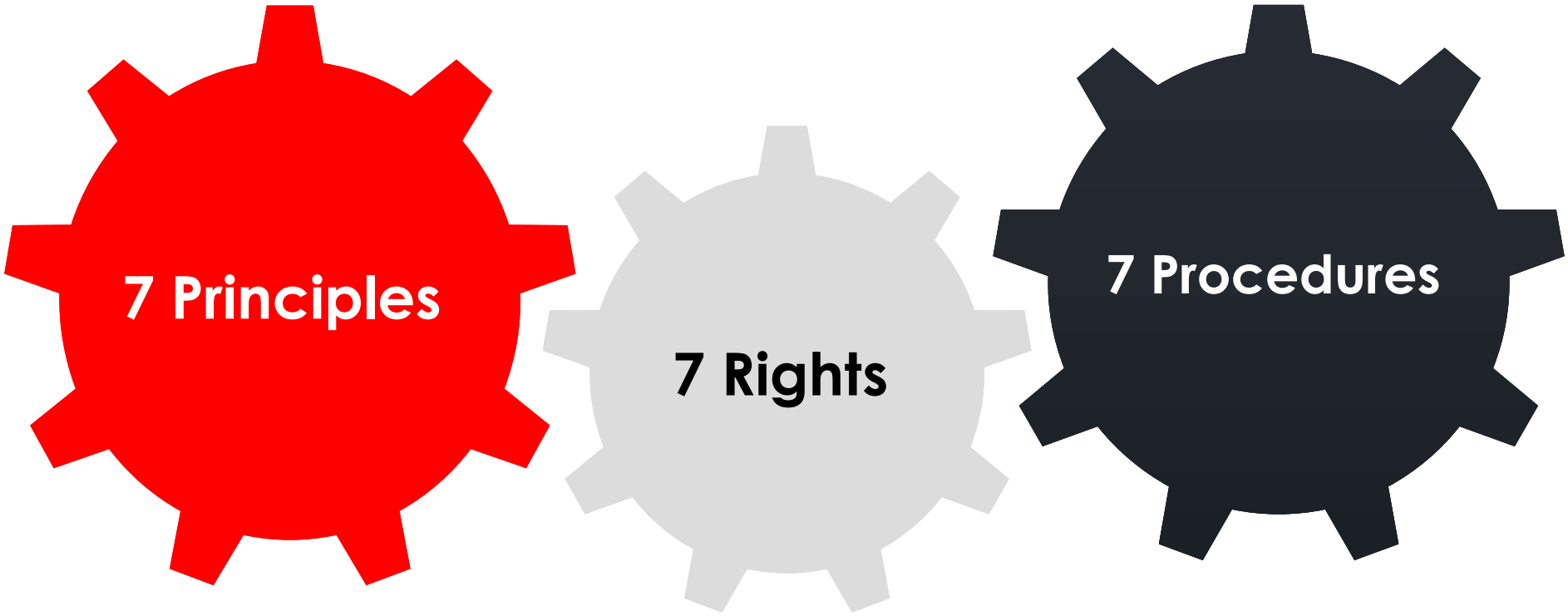
7 STEPS TO IMPLEMENT GDPR SUCCESSFULLY

MyData-TRUST
When GDPR meets Life Sciences

NOVEMBER 14, 2017
9:15-9:40 PM

XAVIER GOBERT
EXECUTIVE DIRECTOR
X.C.GOBERT@MYDATA-TRUST.COM

GDPR Overview



Controllers & Processors must demonstrate how they comply with this regulation.

Legal obligation to give effect to the rights of data subjects.

10M€/20M€ or 2%/4% of Global TO

GDPR Overview

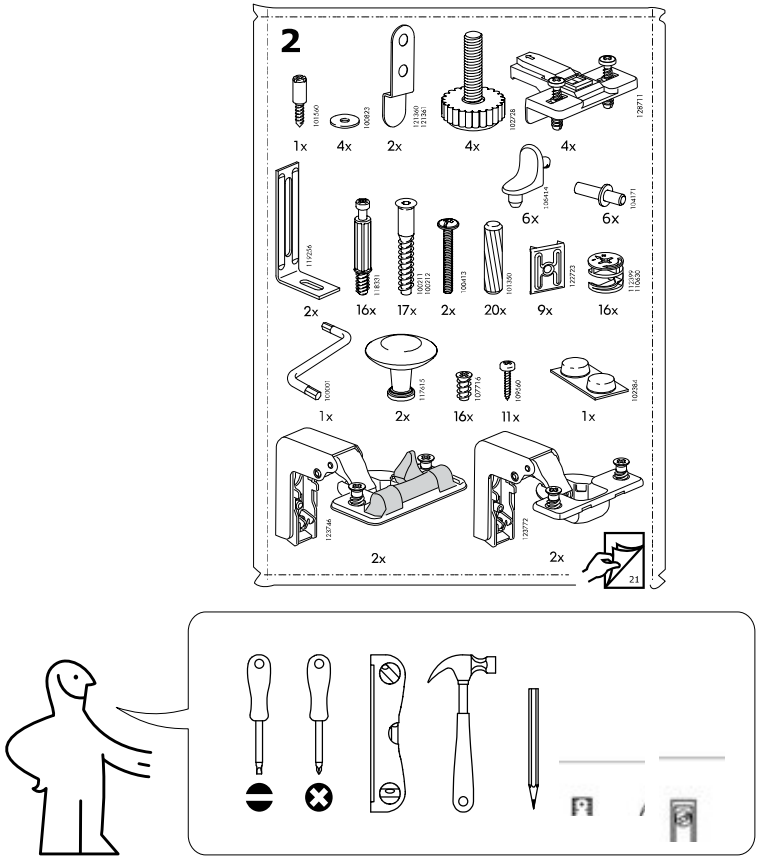
Principles	Rights	Procedures
1. Lawfulness 2. Fairness & Transparency 3. Legitimate Purpose 4. Minimization 5. Accuracy 6. Retention 7. Cyber Security	1. Information 2. Access 3. Rectification 4. Erasure 5. Restriction of processing 6. Data portability 7. Object	1. Records of Processing, 2. DPIA, 3. DPO, 4. Privacy By Design and By Default, 5. Data Transfers, 6. One-stop-shop, 7. Data Breach

Accountability

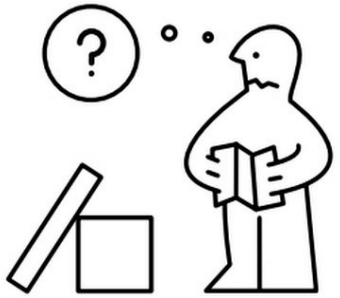
Complex system with multiple entries / Huge workload transversal impact / Short timeframe

GDPR Implementation Guidelines

For all organizations, implementing GDPR is a challenge. There is a vision with requirements and penalties but no implementation guide

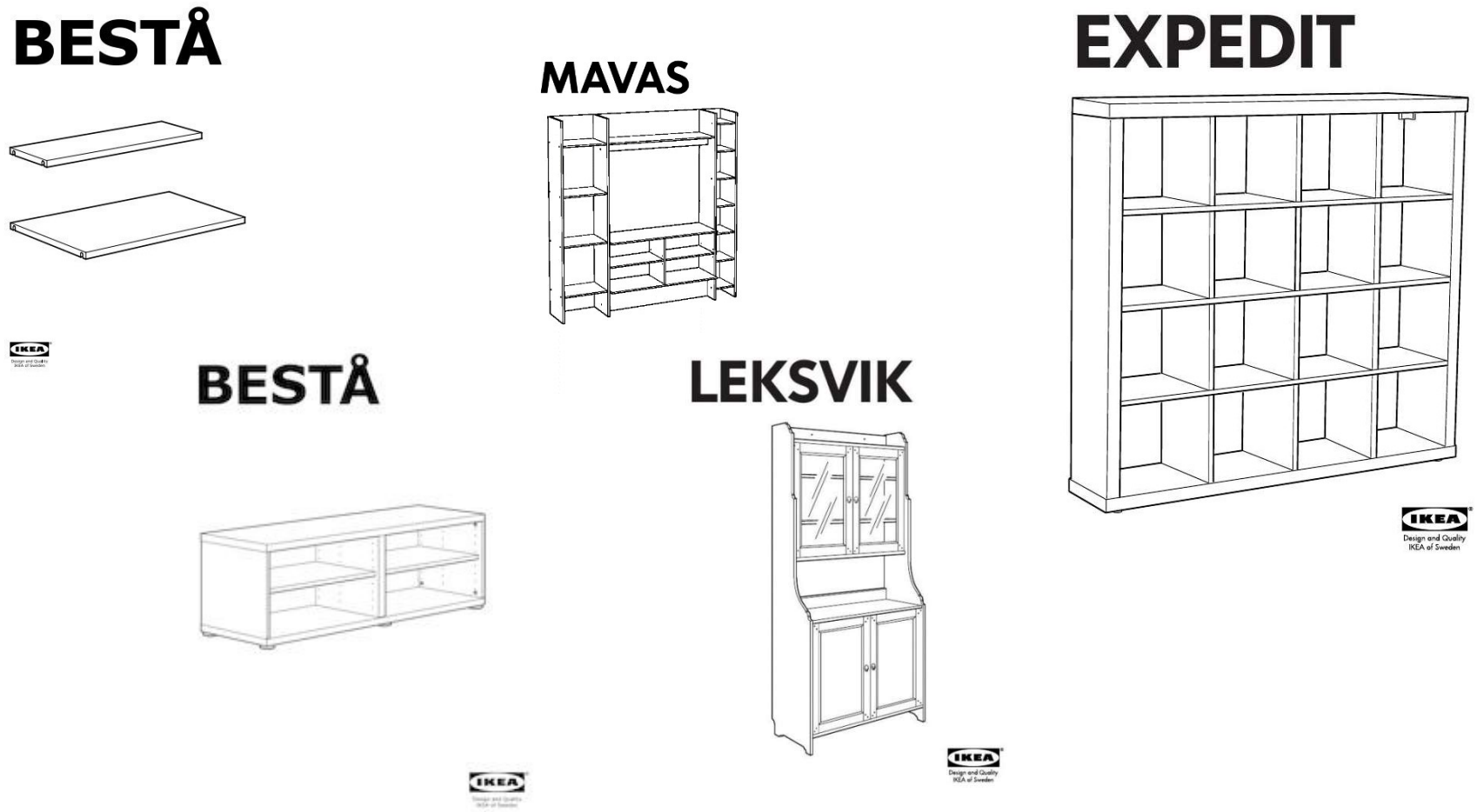


With no assembly instructions



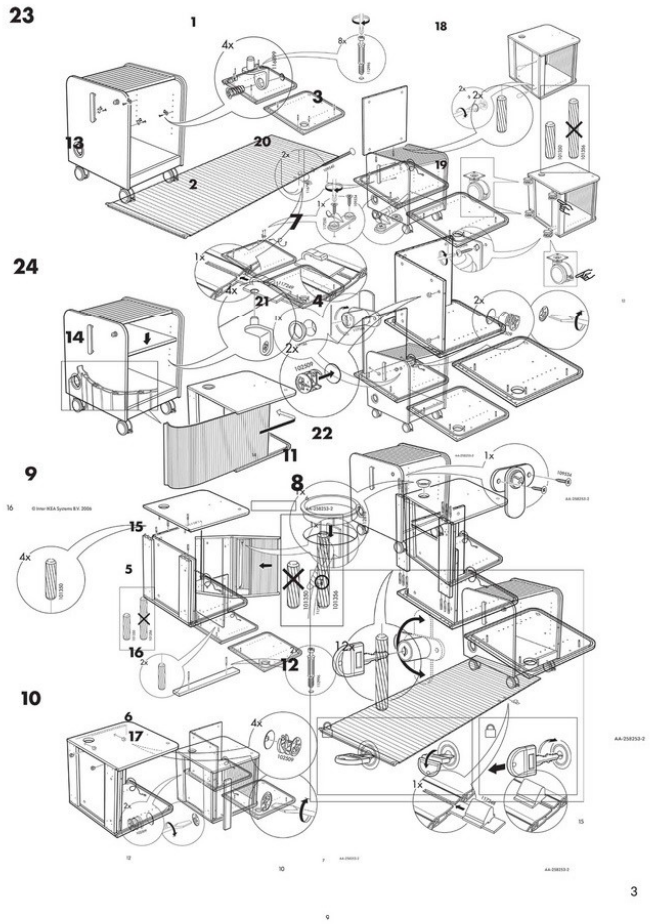
GDPR Implementation Guidelines

GDPR is yours and implementation must be aligned with your business specificities.



GDPR Implementation Guidelines

Keep simple and make it efficient ! Best practices recommend to use a risk based approach. Don't build a labyrinthine system.



- Work with people who know your business
- GDPR must bring benefits for your business !
- GDPR will mandate that companies practice good data analytics hygiene

1 Raise the sponsorship of your top management

GDPR is a real challenge for organizations

- Covering people development, processes optimization and systems evolution,
- Transverse: HR, IT, R&D, Marketing, Sales, Procurement & Prod.

Cost is a key driver : total GDPR implementation budget from 0,01 to 1% of global turnover depending on the size of the company, business scope and risk level in terms of personal data exposure.

- ✓ The new regulation emphasises accountability of Directors and Officers if they fail to bring their organisation in line with the forthcoming GDPR rules
- ✓ Have in mind fines and penalties
- ✓ Don't underestimate impact of data breaches on reputation & share value

2 Assess and challenge your providers

Rec.85; Art.5(2) : The controller is responsible for, and must be able to demonstrate, compliance with the Data Protection Principles.

Rec.81; Art.28(1)-(3): A controller that wishes to appoint a processor must only use processors that guarantee compliance with the GDPR. The controller must appoint the processor in the form of a binding agreement in writing, which states that the processor must:

1. only act on the controller's documented instructions;
2. impose confidentiality obligations on all personnel who process the relevant data;
3. ensure the security of the personal data that it processes;
4. abide by the rules regarding appointment of sub-processors ;

2 Assess and challenge your providers

5. implement measures to assist the controller in complying with the rights of data subjects;
6. appoint a DPO; and
7. provide the controller with all information necessary to demonstrate compliance with the GDPR.

- Require GDPR compliance in RFP/RFQ
- Audit your providers in regards of the GDPR implementation
- Amend all existing agreements / contracts with a GDPR adherence clause

3 Perform a Data Protection Gap Analysis

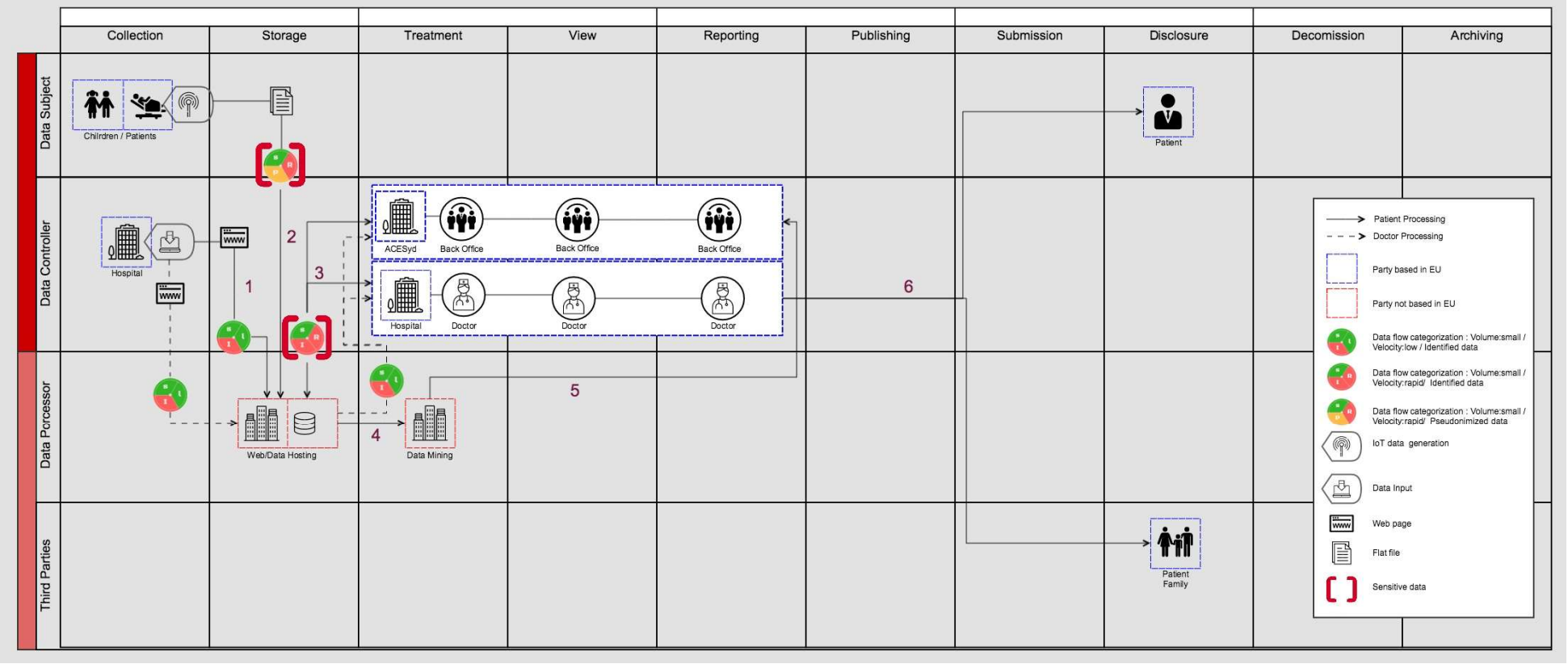
Prior to start the implementation, it's fundamental to have a clear view and a inter-departments understanding of the current data processing activities.

It helps organizations to understand and quantify the gaps that exist between the GDPR compliance required state and its present state for all processing activities

1. List all your on-going processing activities;
2. For all of them, map the dataflow, define parties involved in any data steps, describe the velocity, variety and volume of data transfers;
3. Identify R&R for all parties involved in the data process;
4. State the DP fundamentals: purpose, legal basis, data categories;
5. Identify cross-borders data transfers;

3 Perform a Data Protection Gap Analysis

6. Categorize data processing activities according to the risk; and
7. Prioritize implementation.



4 Maintain Records of Data Processing Activities

Rec.82, 89; Art.30

Organizations must keep records of their data processing activities and provide those records to (or is available on request by) Data Protection Authorities (DPAs).

There is no obligation to notify DPAs. Instead, each controller (and its representative, if any) must keep records of the controller's processing activities.

These include:

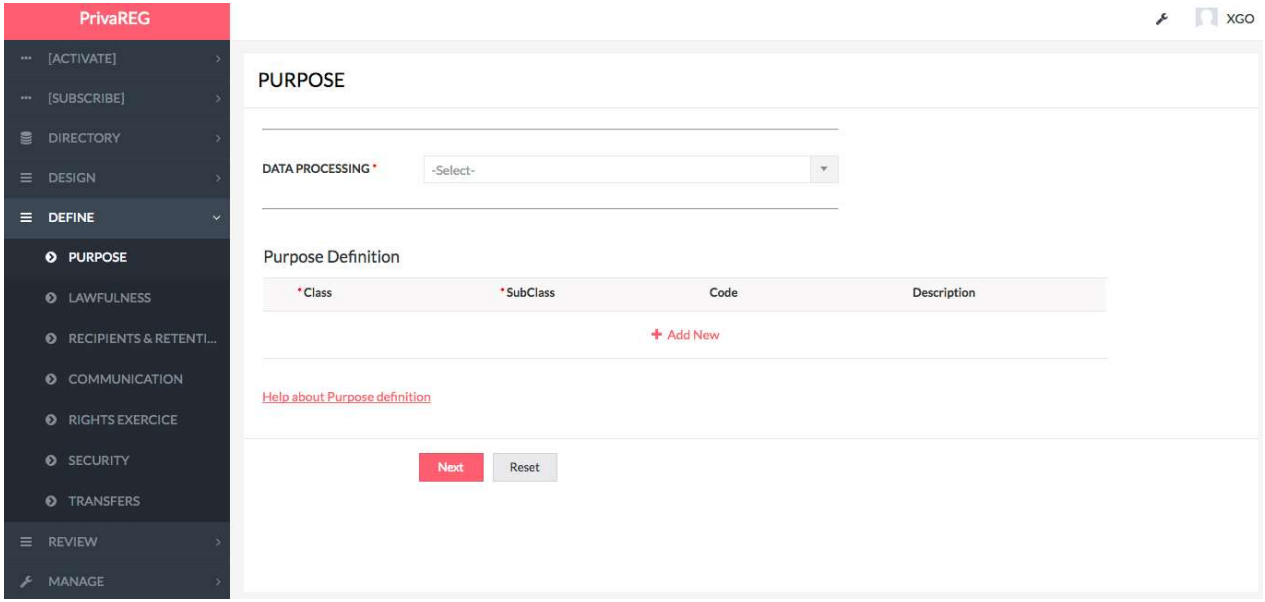
1. the contact details of the controller/representative/ DPO;
2. the purposes of the processing;
3. the categories of data subjects and personal data processed;
4. the categories of recipients with whom the data may be shared;
5. information regarding Cross-Border Data Transfers;

4 Maintain Records of Data Processing Activities

6. the applicable data retention periods;
7. and a description of the security measures implemented in respect of the processed data.
8. …

- Setup records of data processing activities.
- Monitor and control these records.

PrivaREG©



5 Assess Data Protection Impact

Rec.84, 90-94; Art.35; WP29 Impact Assessment Guidelines

Following the GAP Analysis, most critical data processing activities need to be addressed with a DPIA.

By conducting Impact Assessments, controllers identify and address risks that would otherwise not have been detected. This avoids breaches of the GDPR that might otherwise have occurred.

The WP29 has issued (WP 248) (the "Impact Assessments Guidelines") which provide further clarity on the requirements around Impact Assessments.

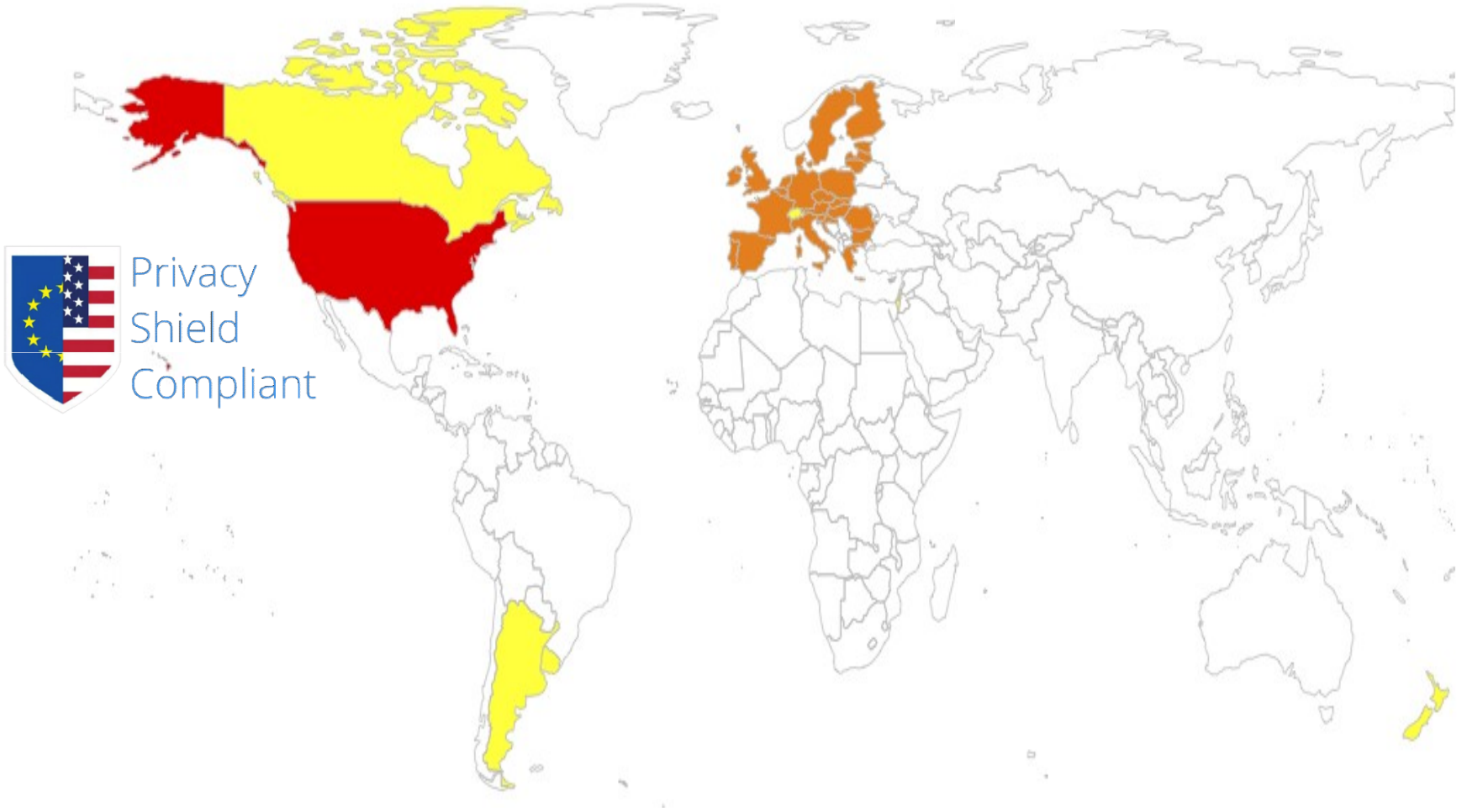
6 Review Data Transfers

It is increasingly important to be able to move data freely to wherever those data are needed.

However, the transfer of personal data to recipients outside the EEA is generally prohibited unless:

1. the jurisdiction in which the recipient is located is deemed to provide an adequate level of data protection;
   - ❖ Andorra, Argentina, Canada (where PIPEDA applies), Switzerland, Faero Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.
2. the data exporter puts in place appropriate safeguards;
   - ❖ OK for US if companies decided to comply the Privacy Shield (no more the Safe Harbor)

6 Review Data Transfers



7 Appoint a DPO

Rec.97; Art.37; Rec.97; Art.37(5)-(6); Art.38(1)-(2), (4)-(5); Art.38(3); Art.38(6), 39; WP29 DPO Guidelines (WP 243)

A Data Protection Offcier (DPO) is a person who provides the primary contact point for data protection issues within an organisation.

Organisations that do either of these things should appoint a DPO:

- regular and systematic monitoring of data subjects; and/or
- processing of Sensitive Personal Data.

A DPO can be an employee or an outside consultant. A DPO should have expert knowledge of data protection law and practice,

7 Appoint a DPO

The organisation can not instruct the DPO in the performance of his or her duties, and cannot terminate the DPO's employment .

His duties include:

1. informing and advising the relevant controller or processor (and any employees who process personal data) about their obligations under the GDPR;
2. monitor compliance with the GDPR by the controller or processor;
3. advise on Impact Assessments and prior consultation with DPAs; and
4. cooperate with DPAs
5. act as a point of contacts for data subjects and DPAs
6. Deal with data breaches

Conclusions

The 7 steps to success

7. Appoint a DPO
6. Review Data Transfers
5. Assess Data Protection Impact
4. Maintain Records of Data Processing Activities
3. Perform a Data Protection Gap Analysis
2. Assess and challenge your providers
1. Raise sponsorship of your top management

Conclusions

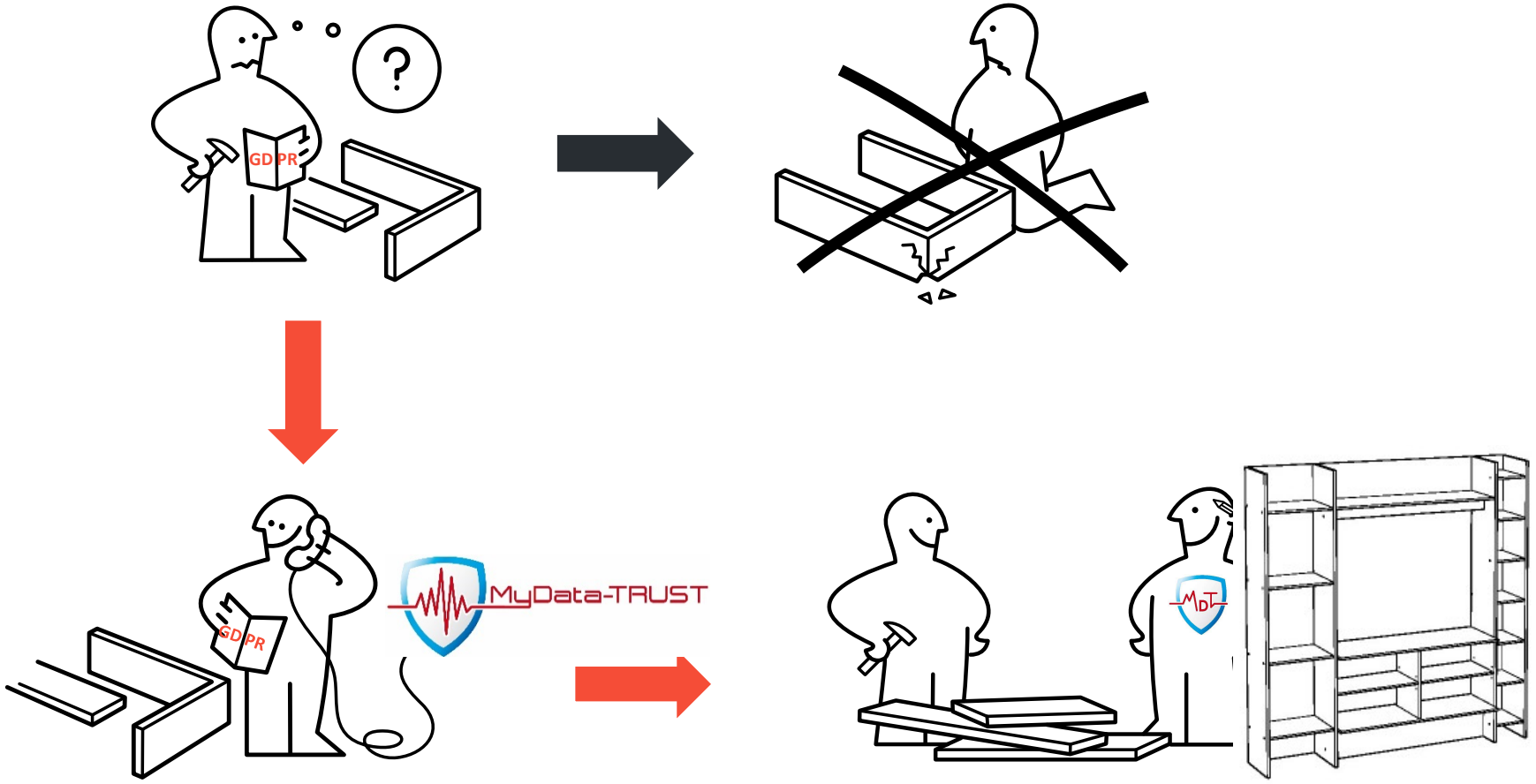
Start now ! Most important is to have a roadmap not to be totally GDPR compliant on the 25th of May 2018

Next steps: setup data breach process and look at the rights of subjects

Strive for a Privacy-Aware Culture : « Privacy awareness » is essential to the functioning of an organization.

- championed by executives,
- embedded in operational procedures,
- aligned to key business goals,
- measured regularly, and effectively communicated on a consistent basis to all employees

Conclusions



MyData-TRUST

When GDPR meets Life Sciences

CONTACT DETAILS

Gautier Sobczak - Development Director

Mobile : +32 493 09 97 04

g.c.sobczak@mydata-trust.com

MyData-TRUST SA.
Rue Descartes 2 / 37
7000 Mons – Belgium