

GDPR Awareness

The Six GDPR Questions

1

What is **GDPR**?

2

Who is
Impacted?

3

What are the
Risks?

4

What are the Key
Requirements?

5

What **actions** are
to be taken?

6

How to be
Compliant?

What is GDPR?



Timing

The regulation entered **into force** in May 2016 and its direct application will **take effect** after two years, meaning **as from May 2018**

(...) the **protection of persons** with regards to **processing of personal data** (...)

'Data Processing' is any operation performed on personal data; i.e.

- creation,
- collection,
- storage,
- view,
- transport,
- use,
- modification,
- transfer,
- deletion,
- etc.

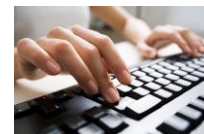


Information Commissioners Office
UK supervisory authority



Data Controller

Organisation which
determines the purpose &
means of data processing



Data Processor

Organisation who's sole
aim is to process the data
in-lieu of the controller



Data Subject

Individual who's data
you hold , natural
Citizen



Third party

Any person or organisation you
are sharing data with but not as
Data processor or Data Controller
i.e. Police etc



DPO – Data Protection Officer

Named individual responsible
for guidance and compliance



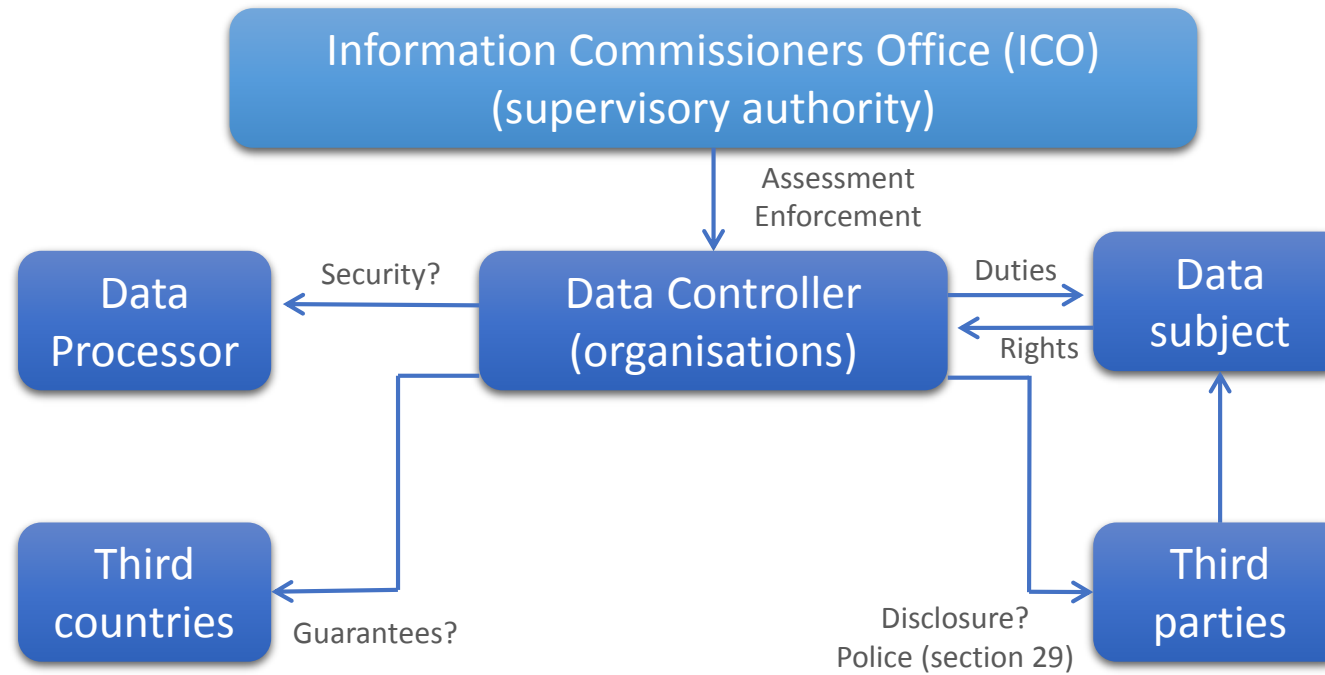
Information security management systems

Description of policies, procedures and
records of security measures used to
keep information secure.

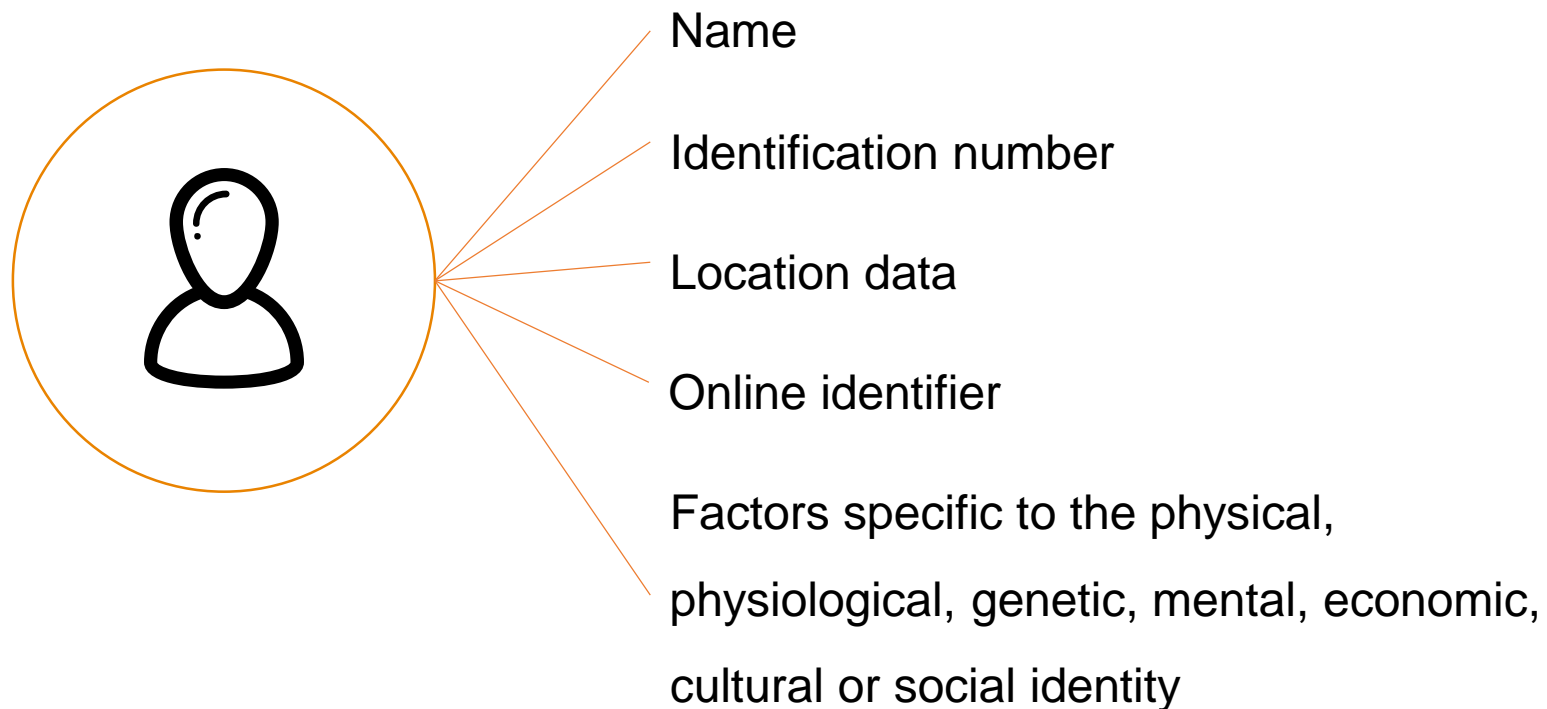


Risk

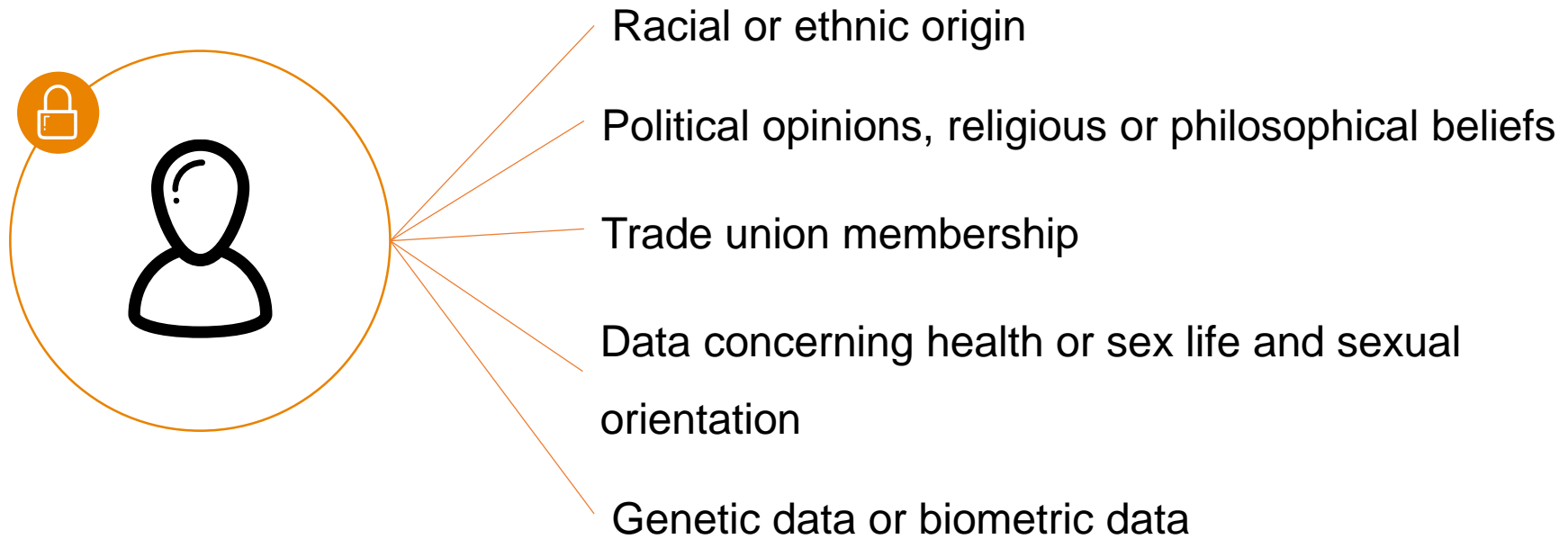
Probability of something
happening multiplied by its
impact



Any information relating to the identification, directly or indirectly, of natural persons



Personal data revealing:





Physical files

Printouts, correspondence etc.



Physical archived files

HR records, Pupil records etc.



Locally kept electronic files

Files, databases, spreadsheets, etc.



Internet based electronic files (Cloud)

Website, backups, emails, online storage etc.



Physical Backups

USB sticks, removeable drives, backup tapes etc.



Mobile devices

Laptops, mobile phones, tablets etc.

Who is Impacted?



Every **Public** or **Private Organization**, including sub-contractors, **processing personal data** in the context of the activities **establishment in EU**



Sub-contractors and/or **Companies Outside Europe** when the **processing** are **related to**:

- **Offering of goods or services** to persons in the European Union
- **Monitoring of behaviour** as far as behaviour takes place within the Union

Who is Impacted?



- Who is in charge of Data Privacy within the company?
- Who do you report to in the event of a breach?
- What exposure does your department have on Data Privacy risks?
- How material is that?
- Did you obtain the data legally?
- Do you know the key risks you want to address?
- Do you consider the 'right to be forgotten'?
- Do you have formal processes in place to consider the 'right to keep the data up to date'?
- Are you aware of how your third parties safeguard your data?
- As part of your role, do you share data outside of the EU?
- When obtaining information from clients/customers, do you let them know how you will use their information?
- What monitoring / profiling is legally permitted?
- What fines/penalties apply to Data processors and Data controllers?

WHAT ARE THE RISKS IF YOU ARE NOT COMPLIANT ?

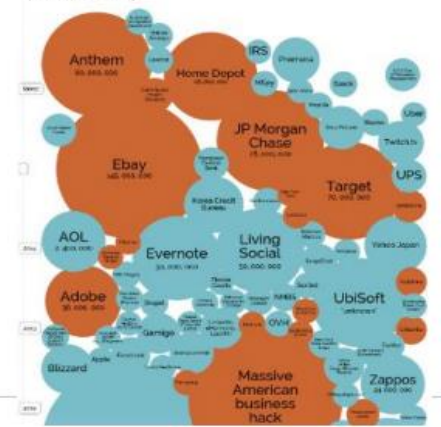


Fines up to €20 Million or 4% of the Worldwide Annual Turnover, whichever is the highest



World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 6th June 2015)



What are the key requirements?

Privacy by Design

- Ensure 'technical and organisational protection' measures (native, permanent and monitored protection of personal data against destruction, loss, dissemination, alteration or access)
- Evaluate obligation to appoint a Data Privacy Officer
- Put appropriate level of security according to the risk and consider protection means (encryptions, pseudonymisation,...)
- Minimise data transfers and arrange them contractually

Security by Default

- Minimize collected and retained personal data
- Limit Storage in time (no longer than is necessary for the purpose for which the personal data are processed)
- Balance between the controller's interest and the data subjects' interest (Have the fair, adequate, not excessive and lawfulness processing for purposes or storage)

Data Accountability

- Identify, document and justify any personal data processing, also when recourse to external partner
- Process data only for specified, explicit and legitimate Business purpose and recipient
- Ask explicit consent (i.e. « Opt-in » on a voluntary basis from the consumer rather than « Opt-out »)

Respect of Individual Rights

- Respect the data subjects rights :
 - ✓ "to be informed"
 - ✓ "to access"
 - ✓ "to rectify"
 - ✓ "to object"
 - ✓ "to be forgotten"
 - ✓ "to transfer"
- Stick to the specific and lawful purposes (i.e. for the normal contract performance)

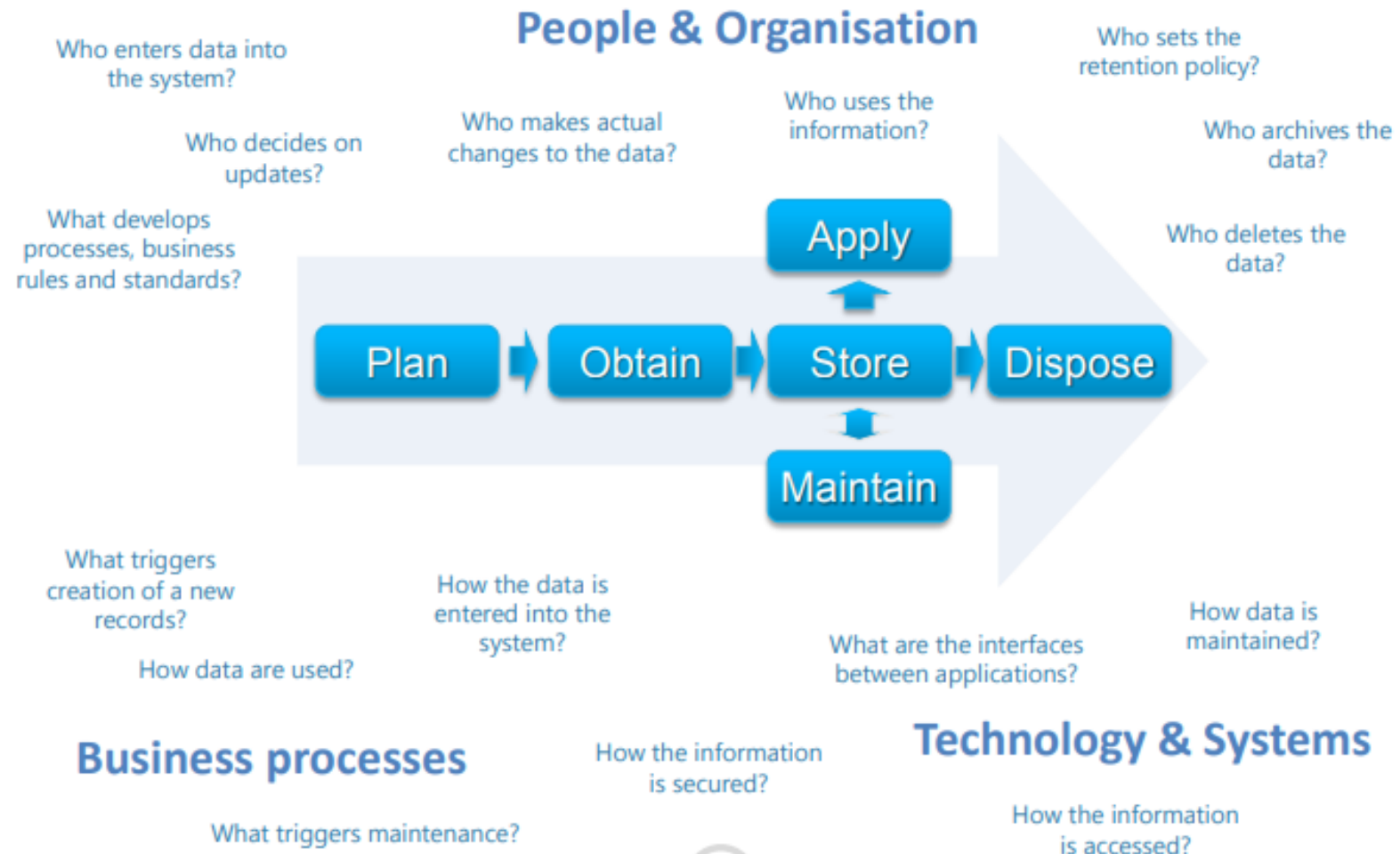
Breach Notification

- Embed Breach Management in the Information Security Incident Management
- Ensure clear communication streams with the data protection authorities and stakeholders

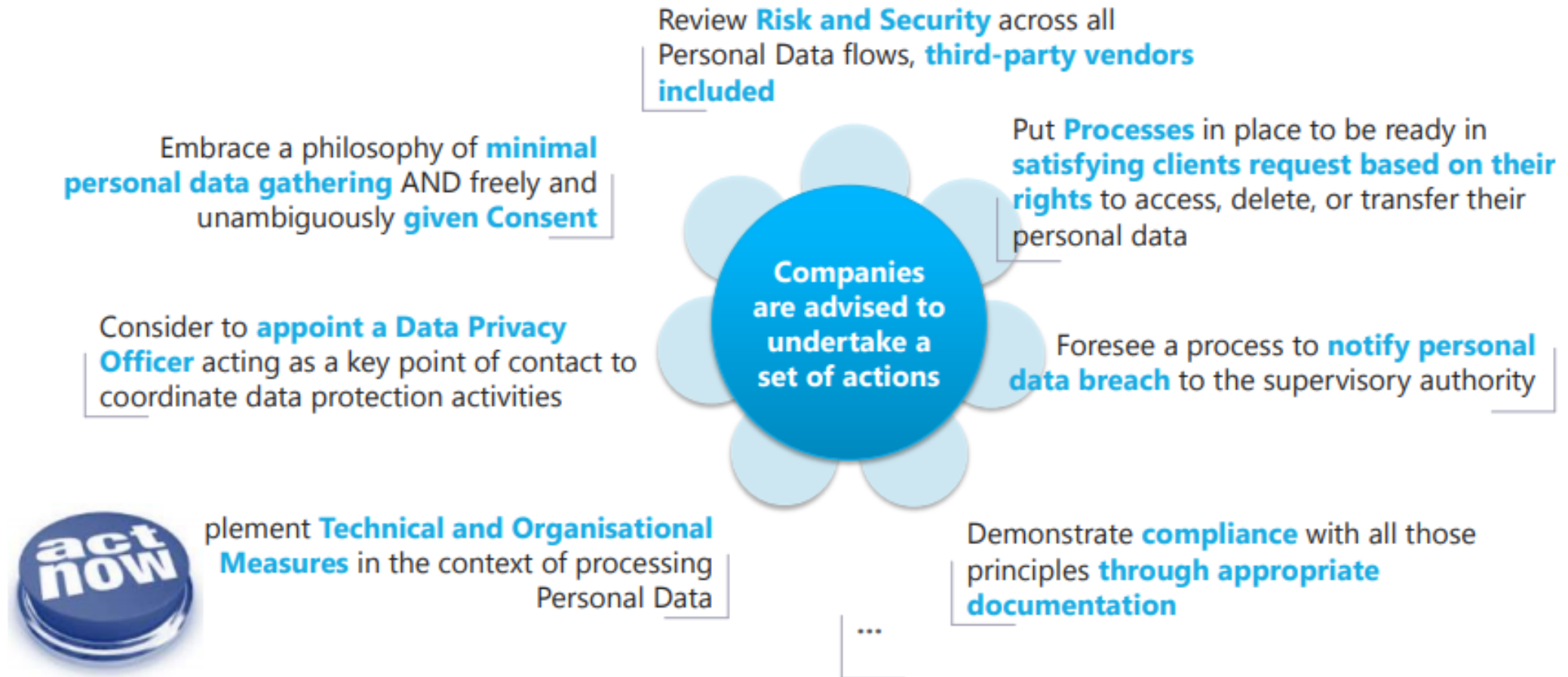
Data processing must comply with the **6 general GDPR principles**

- 1 Lawfulness, fairness and transparency**
- 2 Purpose limitation:** personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- 3 Retention:** personal data must be kept in an identifiable format no longer than necessary
- 4 Integrity and confidentiality:** personal data must be kept secure
- 5 Data minimization:** personal data must be adequate, relevant and limited to the purpose
- 6 Accuracy:** personal data must be accurate and up to date

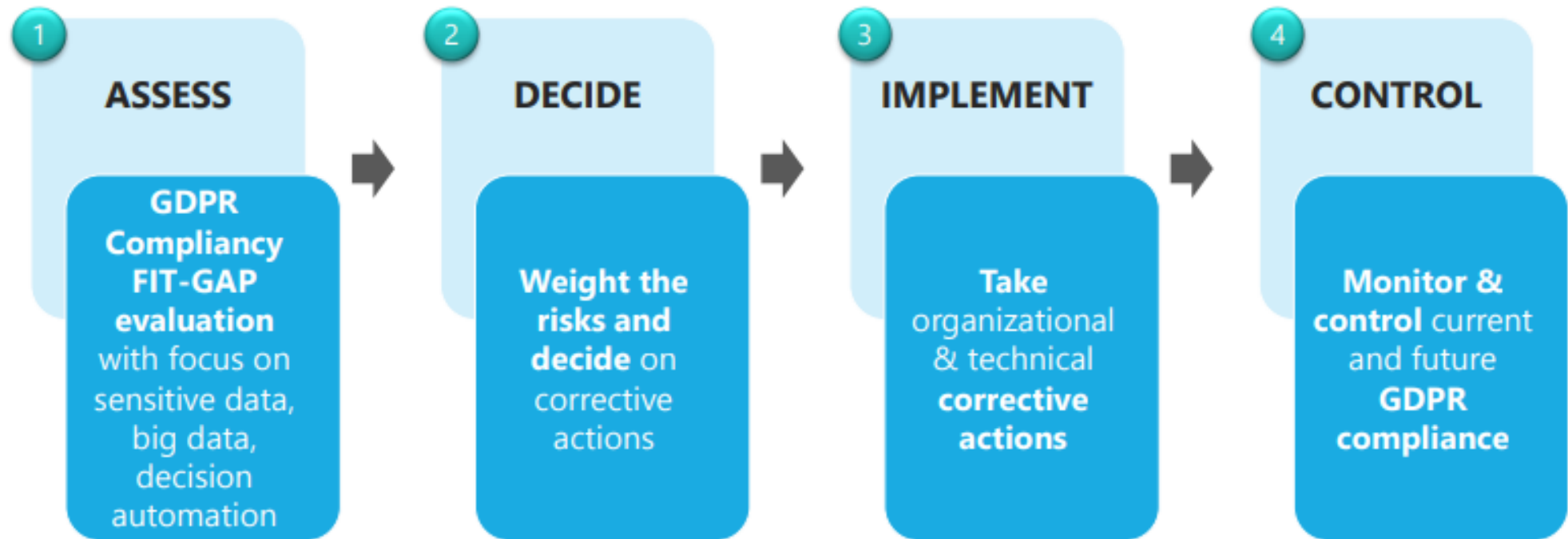
Data Life Cycle

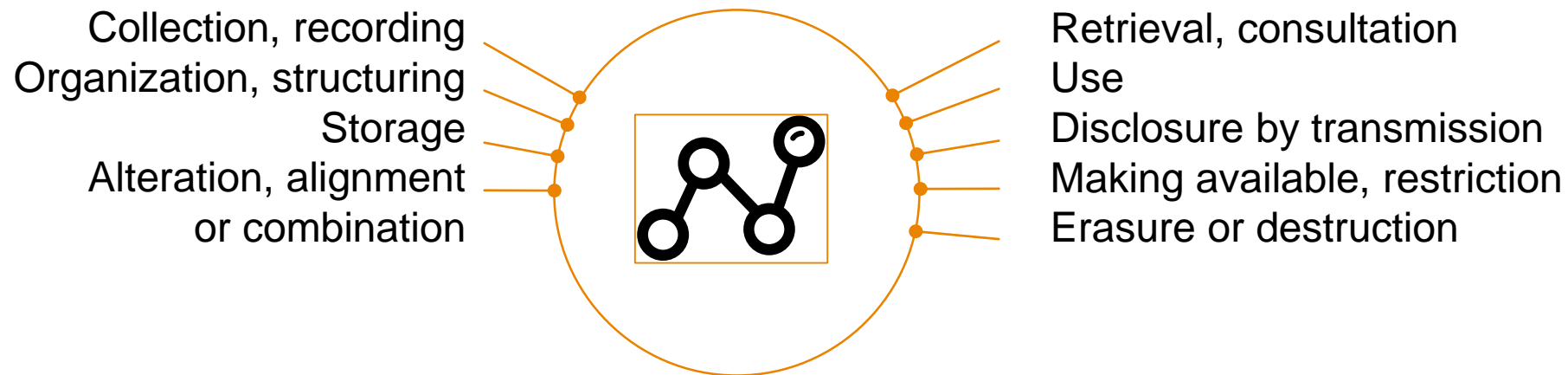



What is personal data?





What is personal data?








-  Awareness

Inform the stakeholders and policy makers about the upcoming changes. They have to estimate what the effects of the GDPR will be for the organization and are responsible for making the required changes.
-  Data Inventory

Identify what personal information you process, where the information comes from and with whom it is shared, why you perform the data processing, on which legal basis, ...
-  Communication

Evaluate your existing privacy notice, policy and plan any necessary changes aligned with the GDPR.
-  Data Subject Rights

Check if the current procedures in your organization provide all the rights that a concerned person can claim: right to rectify, right to be forgotten,...
-  Subject Access Request

Update your existing access procedures and consider how a request for access will now be covered by the new terms in the GDPR.
-  Lawfulness of Data Processing

Document the different types of data processing you perform and identify the legal basis for each of them.



Consent Strategy

Evaluate the manner in which you request, obtain and register permission and change where necessary.



Children

Develop systems that check the age of the person and the parent(s) or guardian(s) to request permission for the data processing of underage children.



Data Breaches

Provide adequate procedures in case of a data breaches to trace, report and investigate it. Personal data breaches have to be reported to the appropriate supervisory authority.



Privacy by Design

Familiarize yourself with the concepts “Privacy by Design” and “Data Protection Impact Assessment” and look how to implement these concepts into your organization.



International Data Transfers

Determine whether international transfers are authorized or not.



DPO

Indicate, if necessary, a Data Protection Officer, or someone who bears the responsibility for compliance with the GDPR.




Existing Contracts

Evaluate your existing contracts, mainly with processors and subcontractors , and make the necessary changes timely.



GDPR-ISO27K

Requirements




requirement

Design




design

Coding



coding

Testing




testing

Release

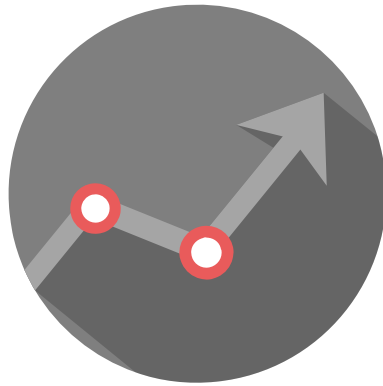


release

Maintenance

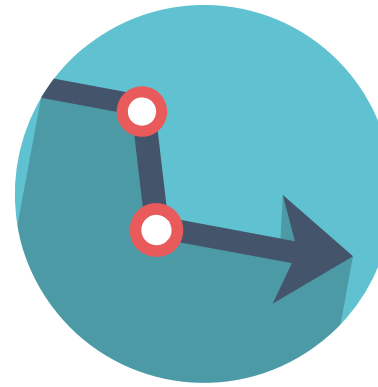


maintenance



As we increase:

- Awareness
- Training
- Security
- Use of formal Processes
- Use of contracts
- Accountability



Our risk of:

- Data breach
 - Severe penalties
 - Loss of reputation
- ...will decrease.