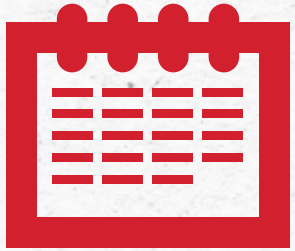
QUADATA

“INDEPENDENT ADVICE & EXECUTION”

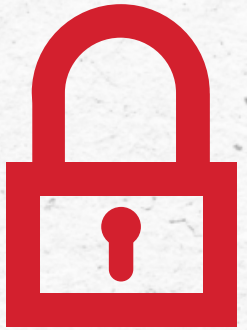
PROGRAMS

DATA QUALITY

MASTER DATA MANAGEMENT



DATA GOVERNANCE



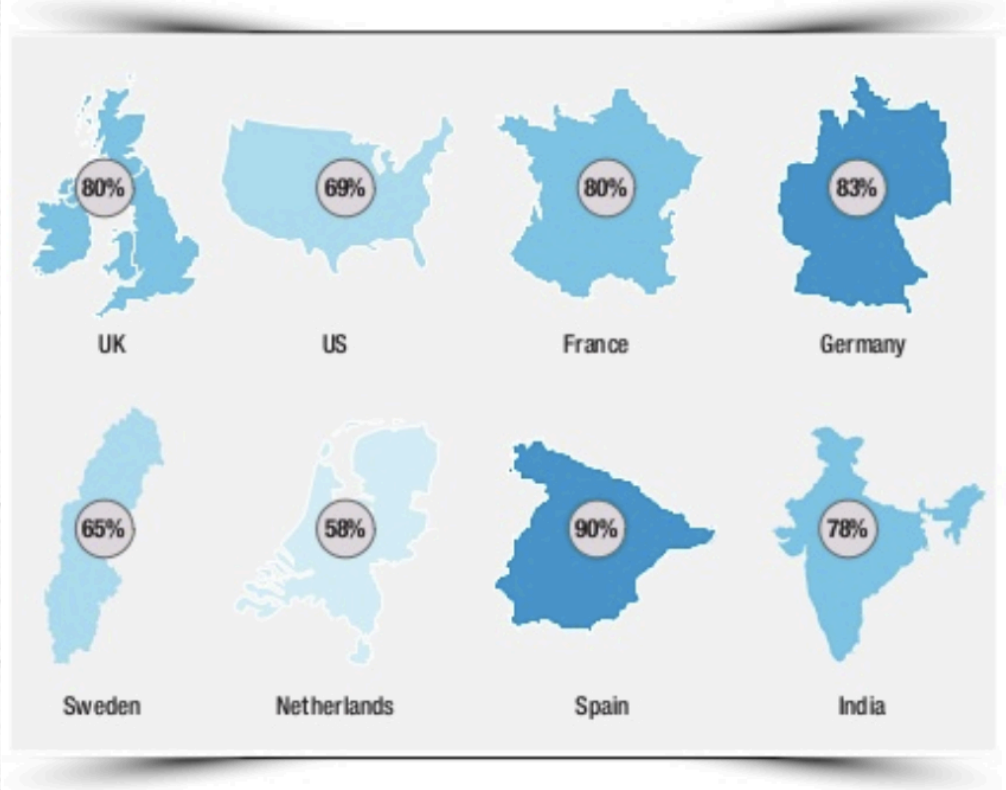
PRIVACY & DATA PROTECTION

81 %

of European citizens think they have
no control
over what companies do with their
personal data

74 %

of consumers would change bank in case of a data breach



Source: Capgemini


TRUSTED
Trusted Brand
TRUSTED


Scrn
Scroll Lock
Pause
privacy
?
Insert
Home

UNIVERSAL DECLARATION OF HUMAN RIGHTS

ARTICLE 12

=

PRIVACY

UNIVERSAL DECLARATION OF HUMAN RIGHTS

1948

United Nations


PASSPORT

PRIVACY AND DATA PROTECTION LAWS

UNIVERSAL AND EUROPEAN HUMAN RIGHTS

EUROPEAN CONVENTION ON PERSONAL DATA

SHENGEN AGREEMENT PROTECTION OF PERSONAL DATA

EU DATA PROTECTION **DIRECTIVE**

DATA PROTECTION DIRECTIVE TRANSLATED IN LOCAL LAWS

EU DATA PROTECTION **REGULATION**

E-PRIVACY **REGULATION**

WHY GDPR?

1 law in the entire EU

Better protection of citizens

Easier to comply for international companies

Better control and enforcement

CONTROL AND ENFORCEMENT

Controlled by local Data Protection Authority
(in BE = Privacy Commission
in NL = Autoriteit Persoonsgegevens)

Fines !
10 mio € or 2% of worldwide turnover
20 mio € or 4% of worldwide turnover

DON'T FORGET THERE IS MORE THAN GDPR

Local legislation stays if more strict than GDPR:

- Do-not-call-me list
- National Register Number
- E-commerce laws
- ….

Definitions

DATA SUBJECT

An individual who is the **subject of personal data**,
or in other words any individual consumer.

A company is not a data subject.

PERSONAL DATA

Personal information = any information that can be linked to an individual person or make identification of an individual person possible (with internal or external help, now or in the future)

GDPR is **applicable to all personal information** except your own personal contact information at home.

DATA CATEGORIES

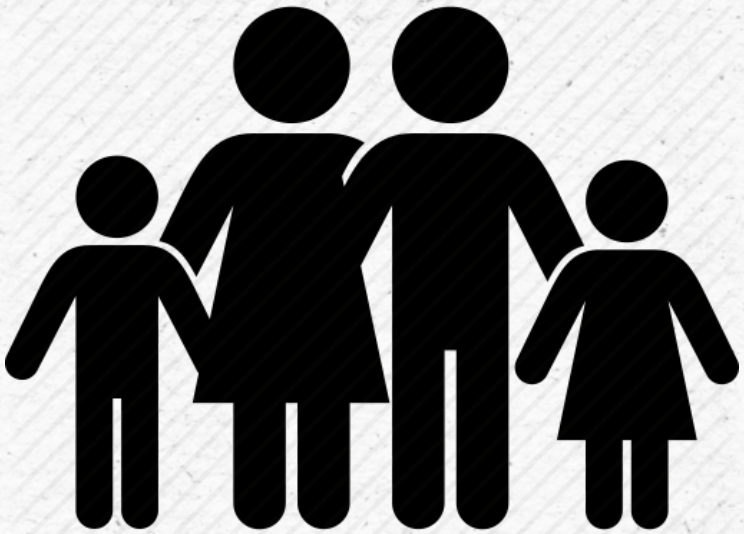
- Personal data
- Sensitive data
  - racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs
  - trade-union membership
  - data concerning health or sex life and sexual orientation
  - genetic data or biometric data
- (Pseudonymous data)
- (Encrypted data)

Pseudonymous data are still treated as personal data because they enable the identification of individuals (via a key).
However, if the "key" that enables re-identification of is kept separate and secure, the risks associated with pseudonymous data is lower, and the levels of protection required data are likely to be lower.

DATA ABOUT CHILDREN

Collecting data about children (-16 / -13) is prohibited without consent of one of the parents &

the data controller must be able to prove the parent's consent



DATA PROCESSING

- obtaining, recording or holding personal data
- carrying out any operation or set of operations on personal data, including
  - organisation, adaptation or alteration of the data
  - retrieval, consultation or use of the data
  - disclosure of the data by transmission, dissemination or otherwise making available
  - alignment, combination, blocking, erasure or destruction of the data

TERRITORIAL SCOPE OF GDPR

Applicable for

- Every European company or organisation
- Every data processor for European companies or organisations
- Every company or organisation that is data controller of data about European Data Subjects

Roles

DATA CONTROLLER

The natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data

JOINT CONTROLLERS

Where two or more **controllers jointly determine the purposes and means of processing**, they shall be joint controllers. They shall in a **transparent** manner **determine their respective responsibilities** for compliance with the obligations under this Regulation.

DATA PROCESSOR

A natural or legal person which processes personal data on behalf of the controller

ACCOUNTABILITY

Article 24 requires that organisations implement ‘appropriate technical and organisational measures’ to be able to ‘**demonstrate**’ their compliance with the Regulation

- Documentation of your data flows
- Clear and written security policies
- Written contracts with processors
- Inventory of processing activities (not for companies < 250 employees)
- Inventory of data incidents

Rights of the Data Subject

Current rights

- Right to be informed
- Right to access
- Right to rectification
- Right to object

GDPR rights as of 2018

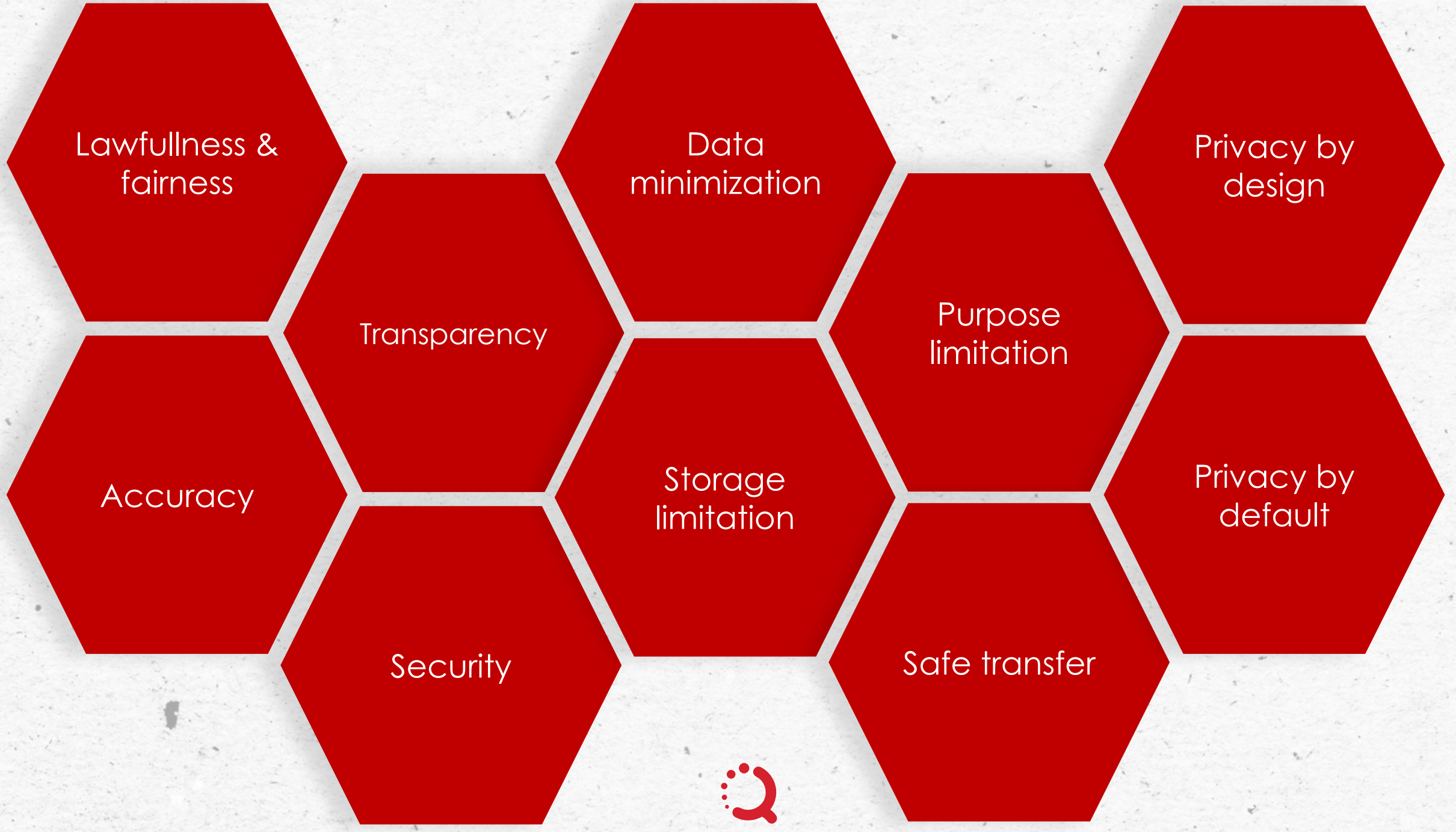
- Right to be informed
- Right to get access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object to direct marketing
- Right to object to profiling

DIRECT MARKETING

- Where personal data are processed for direct marketing purposes, the data subject shall **have the right to object at any time to processing of personal data concerning him or her for such marketing**, which includes profiling to the extent that it is related to such direct marketing.

- Where the data subject objects to processing for direct marketing purposes, **the personal data shall no longer be processed for such purposes**.

GDPR principles

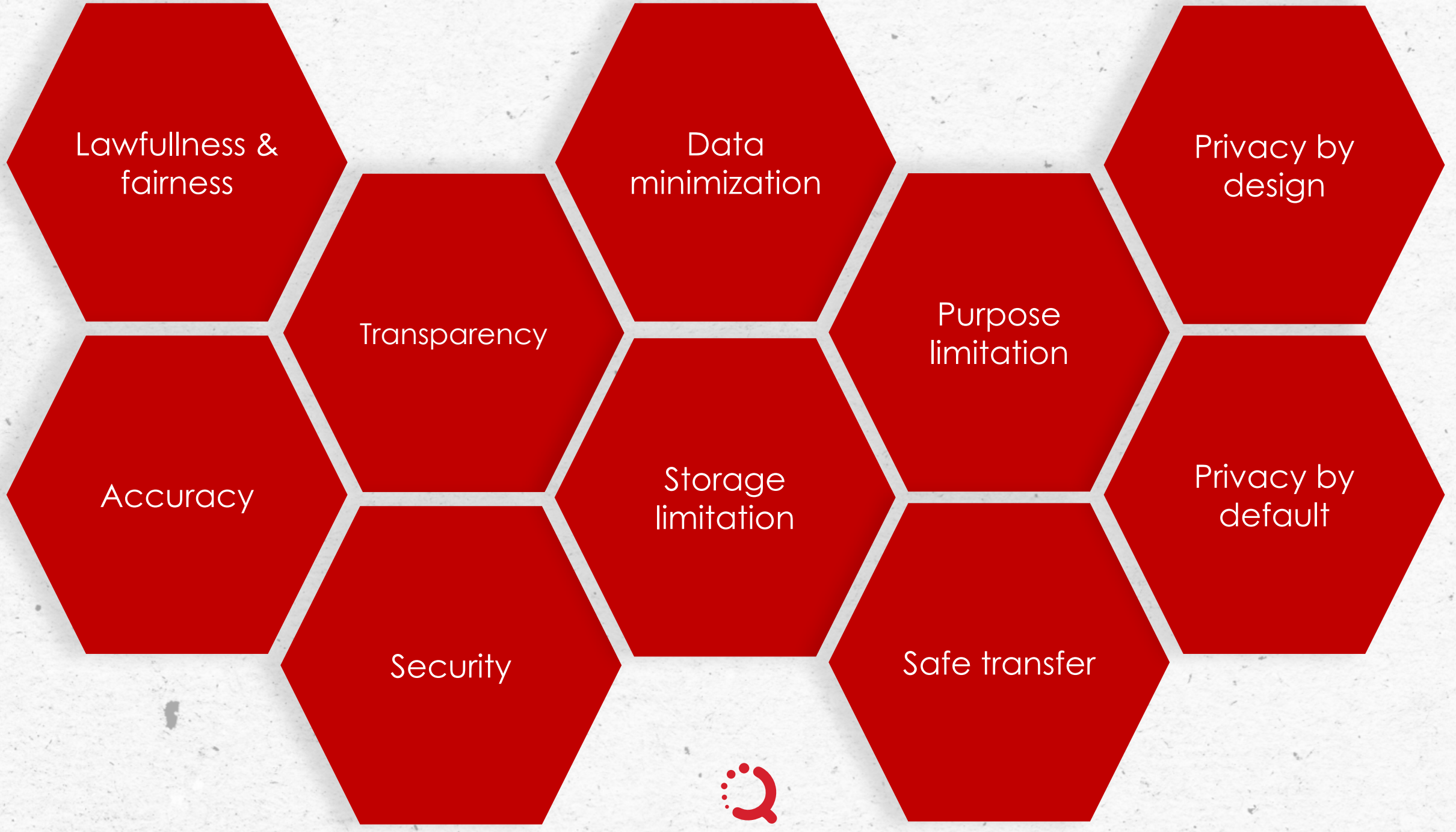

Lawfullness & fairness
Data minimization
Privacy by design
Transparency
Purpose limitation
Accuracy
Storage limitation
Privacy by default
Security
Safe transfer

LEGAL GROUNDS

- Consent
- Contract or data is needed to fulfill a contract
- Legitimate interest
- Legal basis
- Vital interest
- Common interest of public authority

CONSENT

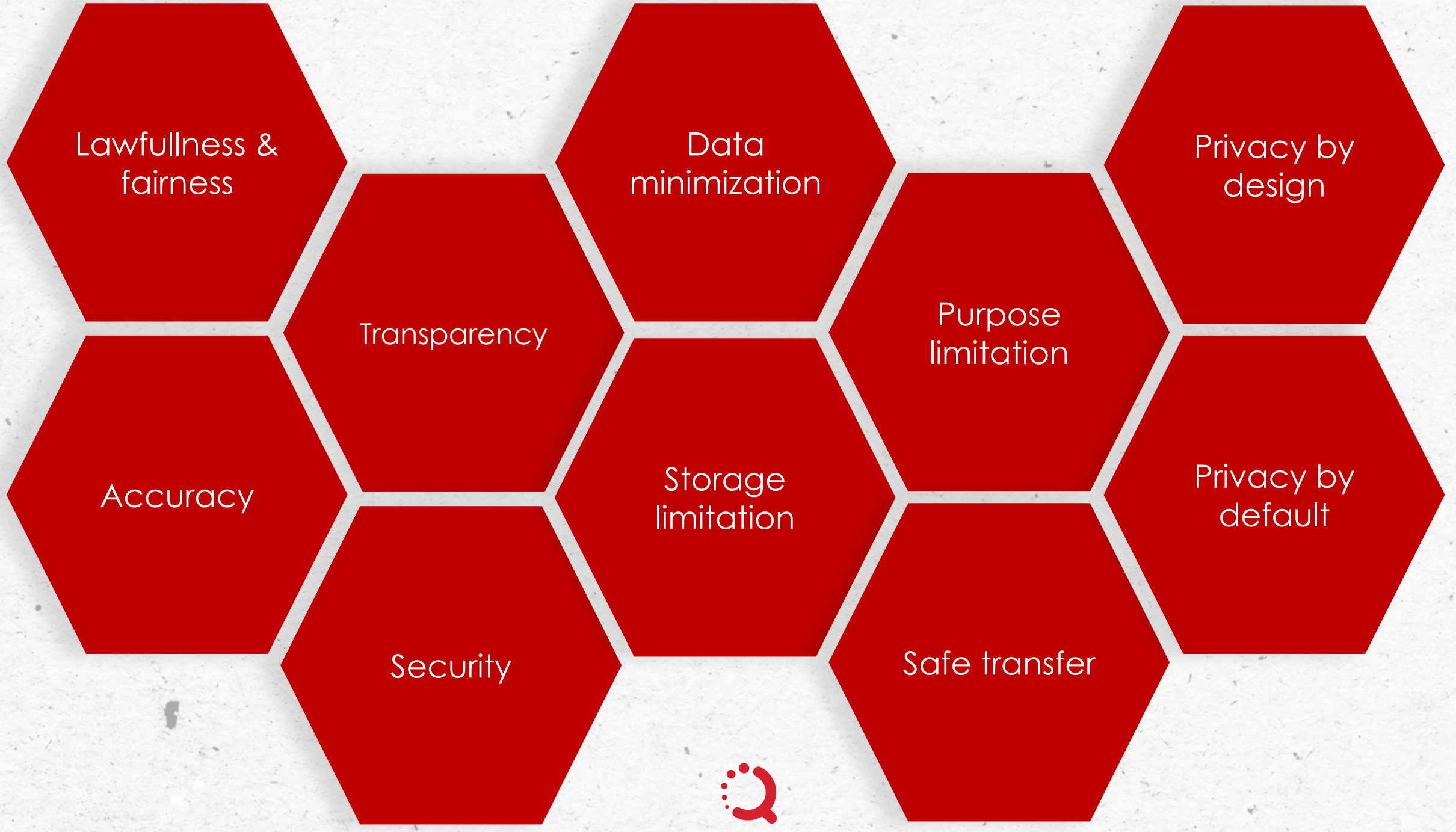
- For # types of processing
  - Communication (e-mail, phone, postal mail, social media, …)
  - Profiling
  - …
- Obligation to **prove** the consent was given
  - Place and time of the consent
  - Text the Data Subject agreed on


Lawfullness & fairness
Data minimization
Privacy by design
Transparency
Purpose limitation
Accuracy
Storage limitation
Privacy by default
Security
Safe transfer

ACCURACY / DATA QUALITY

Personal data needs to be **accurate** and, where necessary, **kept up to date**.

Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, **are erased or rectified without delay.**

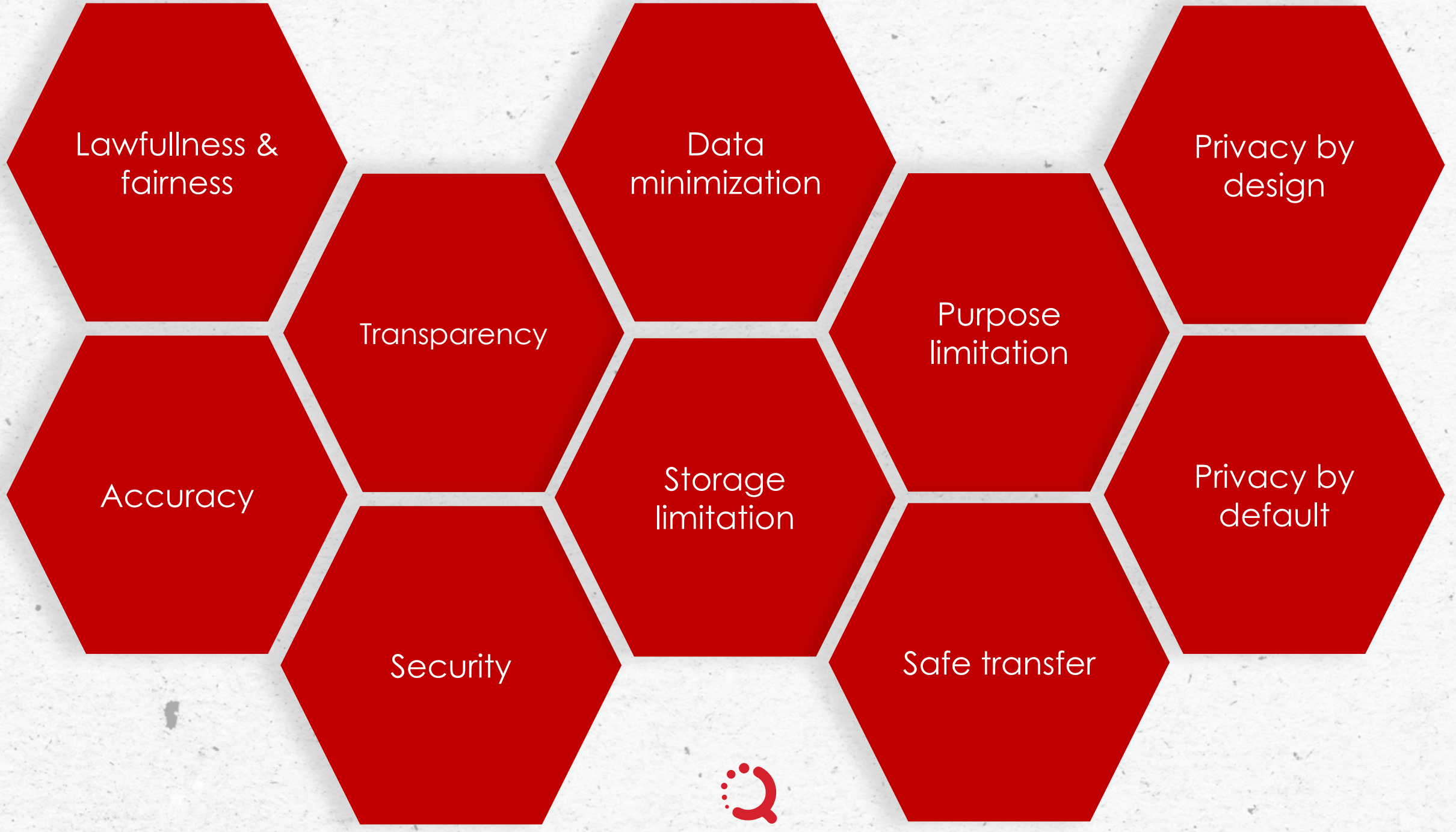

Lawfullness & fairness
Data minimization
Privacy by design
Transparency
Purpose limitation
Accuracy
Storage limitation
Privacy by default
Security
Safe transfer

TRANSPARENCY

The Data Subject has the right to be informed about:

- Why you collect his data
- What you are going to do with his data
- How long you will keep his data
- How he can withdraw his consent
- How he can use his rights

And you need to tell him in clear and understandable language


Lawfullness & fairness
Data minimization
Privacy by design
Transparency
Purpose limitation
Accuracy
Storage limitation
Privacy by default
Security
Safe transfer

BUSINESS DECISIONS TO BE TAKEN

Data minimization

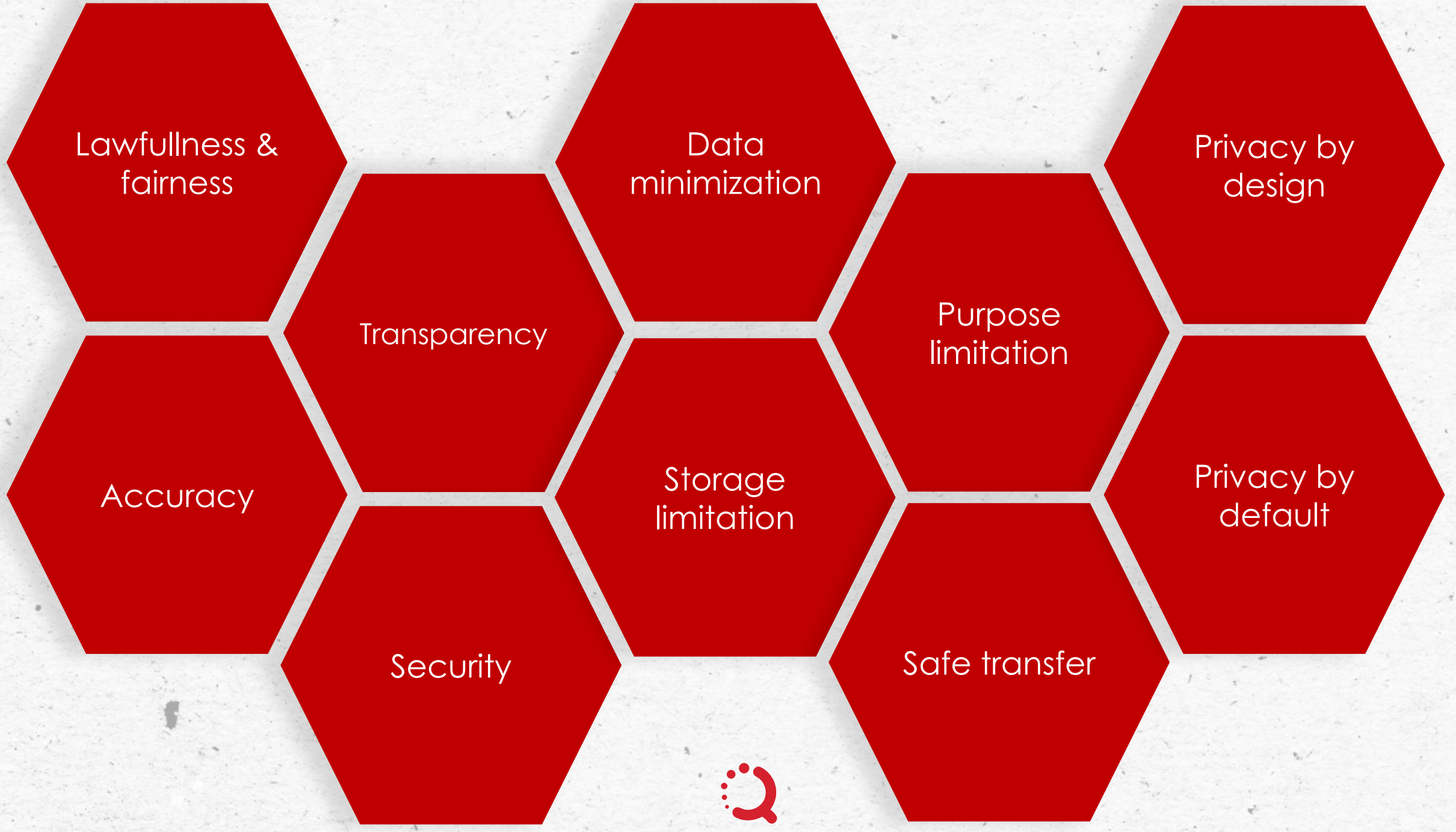
Determine the business goal you collect data for and decide what data you absolutely need to realize them

Purpose limitation

Don’t re-use data for other purposes

Storage limitation

Only keep data for as long as you need to realize your business goal


Lawfullness & fairness
Data minimization
Privacy by design
Transparency
Purpose limitation
Accuracy
Storage limitation
Privacy by default
Security
Safe transfer

PRIVACY BY DEFAULT

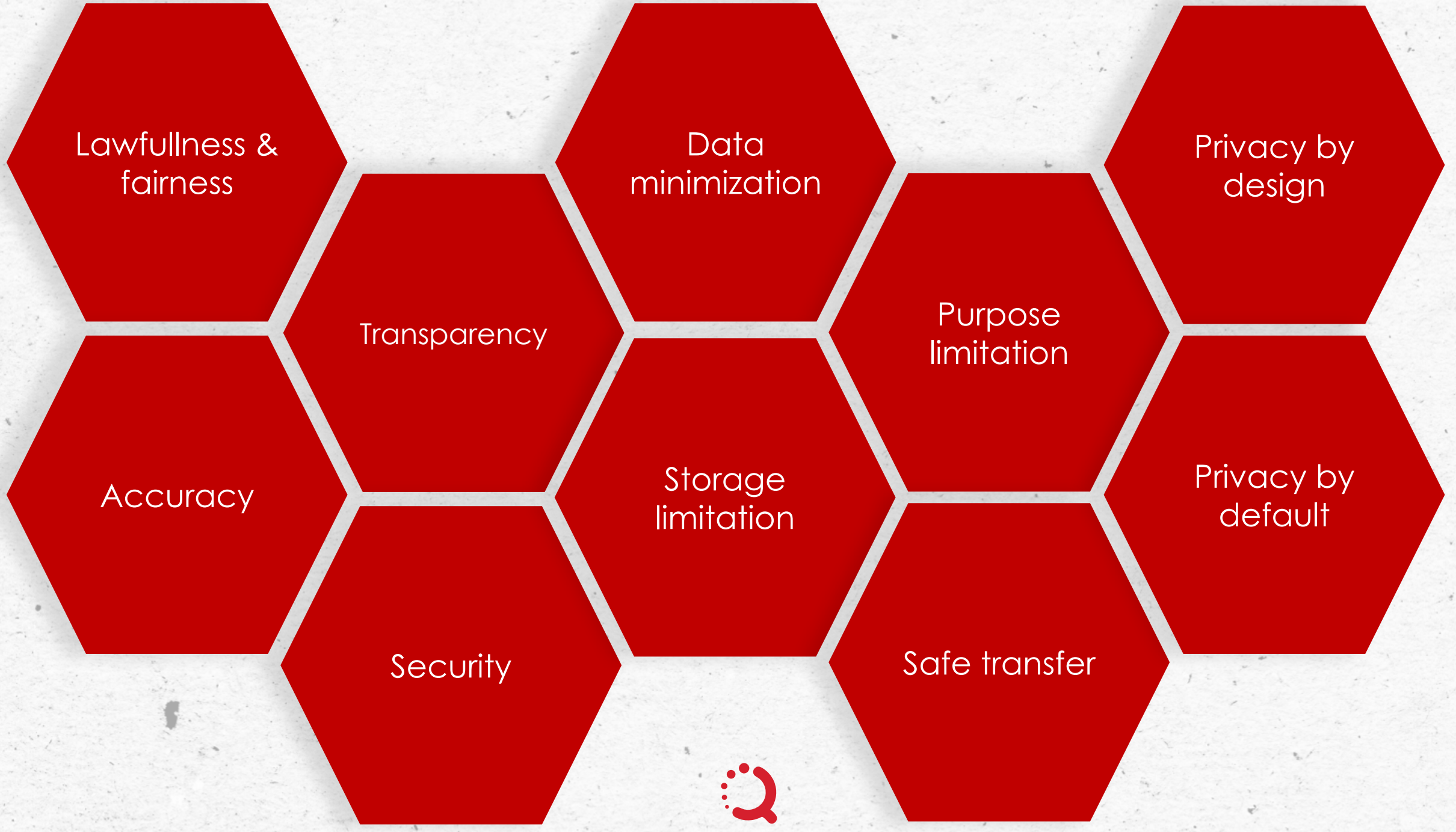
- only personal data that are **necessary for each specific purpose** are processed
- amount of data, the extent of their **processing, storage period and accessibility**

PRIVACY BY DESIGN

Privacy by Design is an internationally recognized privacy standard that has been endorsed globally by Data Protection Authorities and Privacy Commissioners, since 2010.

It means building privacy into the design, operation and management of IT systems, networks and business processes.

- implement technical and organizational measures
- at time of determination of the means of processing & at the time of processing itself


Lawfullness & fairness
Data minimization
Privacy by design
Transparency
Purpose limitation
Accuracy
Storage limitation
Privacy by default
Security
Safe transfer

ADEQUATE PROTECTION

- Pseudonymisation
- Encryption
- System integrity
- Security testing
- Secure data transfer
- Policies and procedures:

DATA BREACH

72 hour notification obligation:

- To the DPA if personal data involved
- To the Data Subjects if any risk for them
- Advice of the DPO

- Documentation of the breach
- Measures taken to stop the breach and restore normal situation
- Measures to be taken to avoid incidents in the future

DATA TRANSFER

- Security of the actual transfer
- Transfer outside of the EU:
  - US-EU privacy shield (https://www.privacyshield.gov)
  - Contracts with data processors (don't forget cloud providers!)
  - Avoid transfer to insecure countries

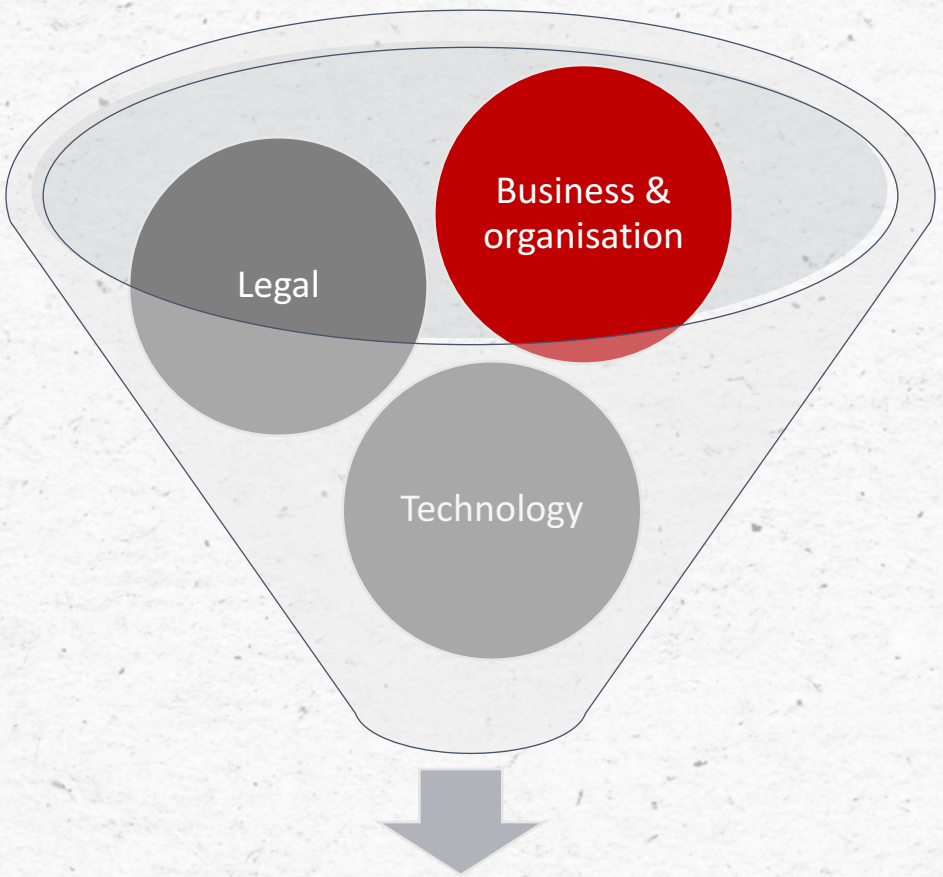
How to prepare for GDPR compliancy?

WHO SHOULD BE INVOLVED?

GDPR is **not only about legal** aspects of data protection

GDPR is **not only about technical** aspects of data protection

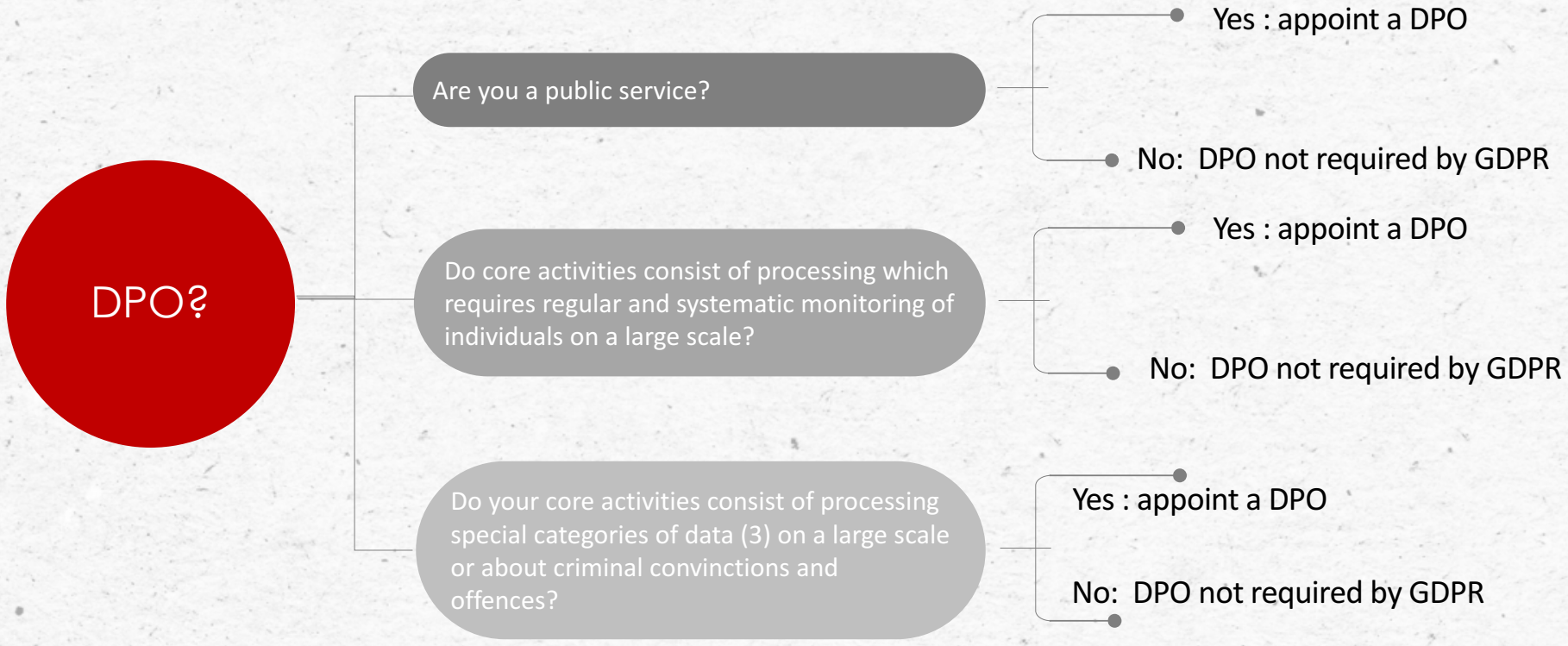
You will need to involve your entire **organisation**



CREATE AWARENESS

Make sure people who have **access to personal data** know about GDPR and develop **caution** when using Personal Information.

IF NEEDED, APPOINT A DPO



Even if not mandatory:
consider appointing a DPO or privacy manager if you collect (large volumes of) personal data

THE DATA PROTECTION OFFICER

- Has sufficient **knowledge** of privacy and data protection
- Is **advising** on privacy and data protection questions
- Is organising training and awareness building
- Is executing **DPIA**'s / PIA's
- Can be internal or external
- Must be able to work **independently**
- Is your organisations contact with the privacy commission

ORGANIZE

DATA GOVERNANCE

Policies, roles, responsibilities and organizational structures support the protection of individuals' privacy

DATA SUBJECTS RIGHTS

Data subjects get control over what data about them is processed and for what purpose

DATA SECURITY

Data subjects get control over what data about them is processed and for what purpose

DATA TRANSFERS

Legal controls are in place to ensure the adequate protection of personal data by 3th parties

DATA PROTECTION PRINCIPLES

Business and HR processes are organized in such way that the processing of personal data is lawful, purpose-limited and transparent to the data subject

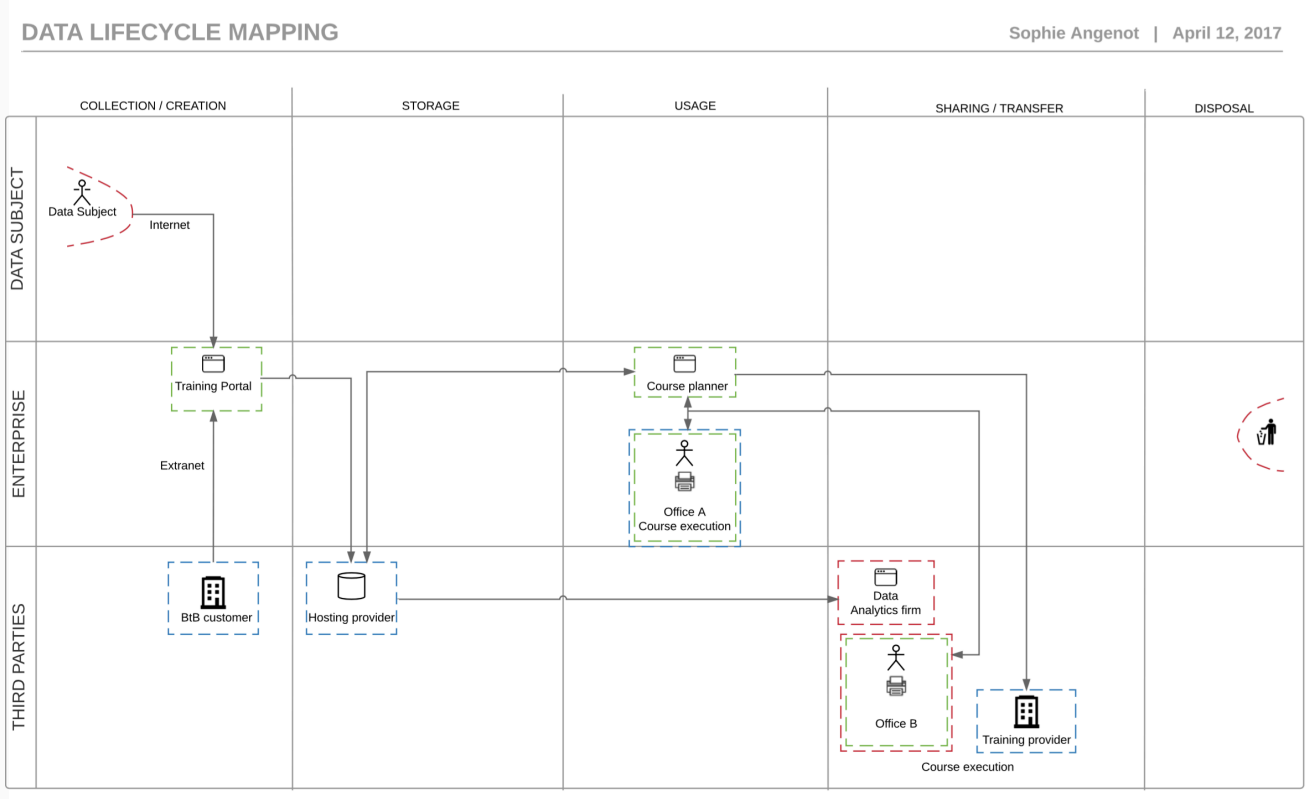
Central implementation

Per process

DOCUMENT THE CURRENT SITUATION

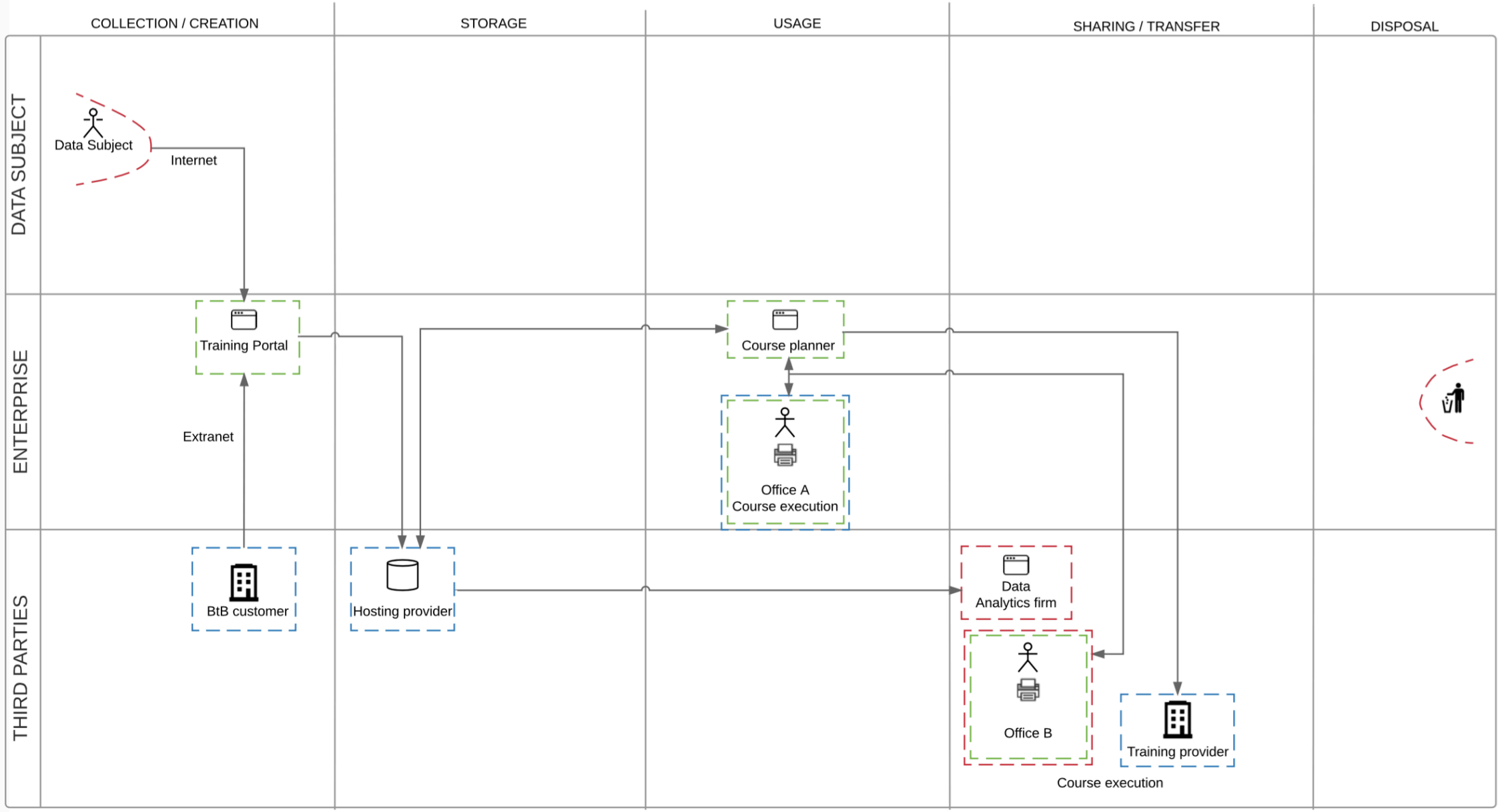
- What data is collected
- Where is it stored
- How is it used
- What the legal ground is
- Who has access

…..



DATA LIFECYCLE MAPPING

Sophie Angenot | April 12, 2017



FROM A CONSUMER POINT OF VIEW!

MAKE A PLAN

- Describe your vision on privacy and data protection
- Develop a strategy and explain the choices you make
- You won't be able to do it all in 1 year: plan your investments and show you're moving forward
- It's not only about technology, it's about people: awareness, training, ….
- Communicate!

DEVELOP PROCESSES AND MODELS

- Data subject rights processes and documents
- Data processing inventory
- Security policies (password, access rights, BYOD….)
- DPIA / PIA model
- Data breach processes and documents
- …

LEGAL ASSESSMENT

Contracts

- Employee contracts
- Data Provider contracts (as a data controller)
- Customer contracts (as a data processor)

- Privacy statement
- General conditions
- Cookie policy

ASSESS AND PLAN YOUR SECURITY

- Website https
- Mobile app security
- Password policy
- BYOD policy
- Personal data access / masking / …
- Data encryption
- System security
- Data transfer security
- …

YOUR ROLE AS MARKETER

- Help your company to develop an ethical, trustful vision on privacy
- Answering a customer question is a communication moment: use it!
- Privacy information should be easy to find and in clear, easy language.

SOME LAST ADVICE

- Don't underestimate how many systems contain personal data
- If you collect a certain volume of personal data, appoint a DPO, even if it's not mandatory, or at least make someone officially coordinating GDPR activities
- If you are a 100% BtB company: be pragmatic, but don't ignore GDPR.
- If you are present in more than 1 EU country: be aware that some DPA's intend to focus on the fines.

"Aan de uitspraak "ik heb niets te verbergen" ligt een aantal fundamentele aannames ten grondslag:

- De eerste aanname is dat diegene die dit zegt, weet *wat* het is dat hij niet te verbergen heeft.
- De tweede is dat hij weet *voor wie* hij dat niet verbergen heeft
- De derde is dat hij weet *waarom* hij dat niet te verbergen heeft

Uit de zoektocht in dit boek blijkt dat alle drie de aannames misvattingen zijn."

Make this the basis of your vision. We are all consumers, and as companies, we should really be more open about what personal data we collect, why we do so and what we use it for.

QUESTIONS?

Sophie Angenot
managing partner
sophie.angenot@quadata.eu
+ 32 474 84 24 78

www.quadata.eu

@QuaDataTweets