GDPR

General Data Protection Regulations

Presented by: Masoud Barati
November 2019

Agenda

GDPR principles

Available rights in GDPR

GDPR information life cycle

Translation of GDPR into codes

GDPR principles

What is GDPR?
What is personal data?
What is data processing?
What are elements/roles in GDPR?

What is GDPR

- The General Data Protection Regulations (GDPR) is new EU legislation that comes into effect on May 25th 2018

- It clearly sets out the ways in which the privacy rights of every EU citizen must be protected and the ways in which a person’s ‘Personal Data’ can or can’t be processed

- It enforces actors processing personal data to comply with the rule and to show compliance

- It carries significant penalties for non-compliance

Personal data

Name

Email-address

IP address

Phone

Bank details

Identification number

and So On ...

Sensitive data

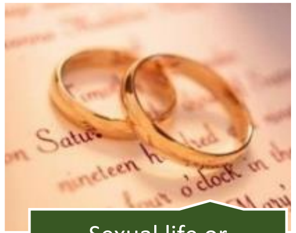
Race or ethnicity

Political opinions

Religious or philosophical beliefs

Trade union membership

Physical or mental health



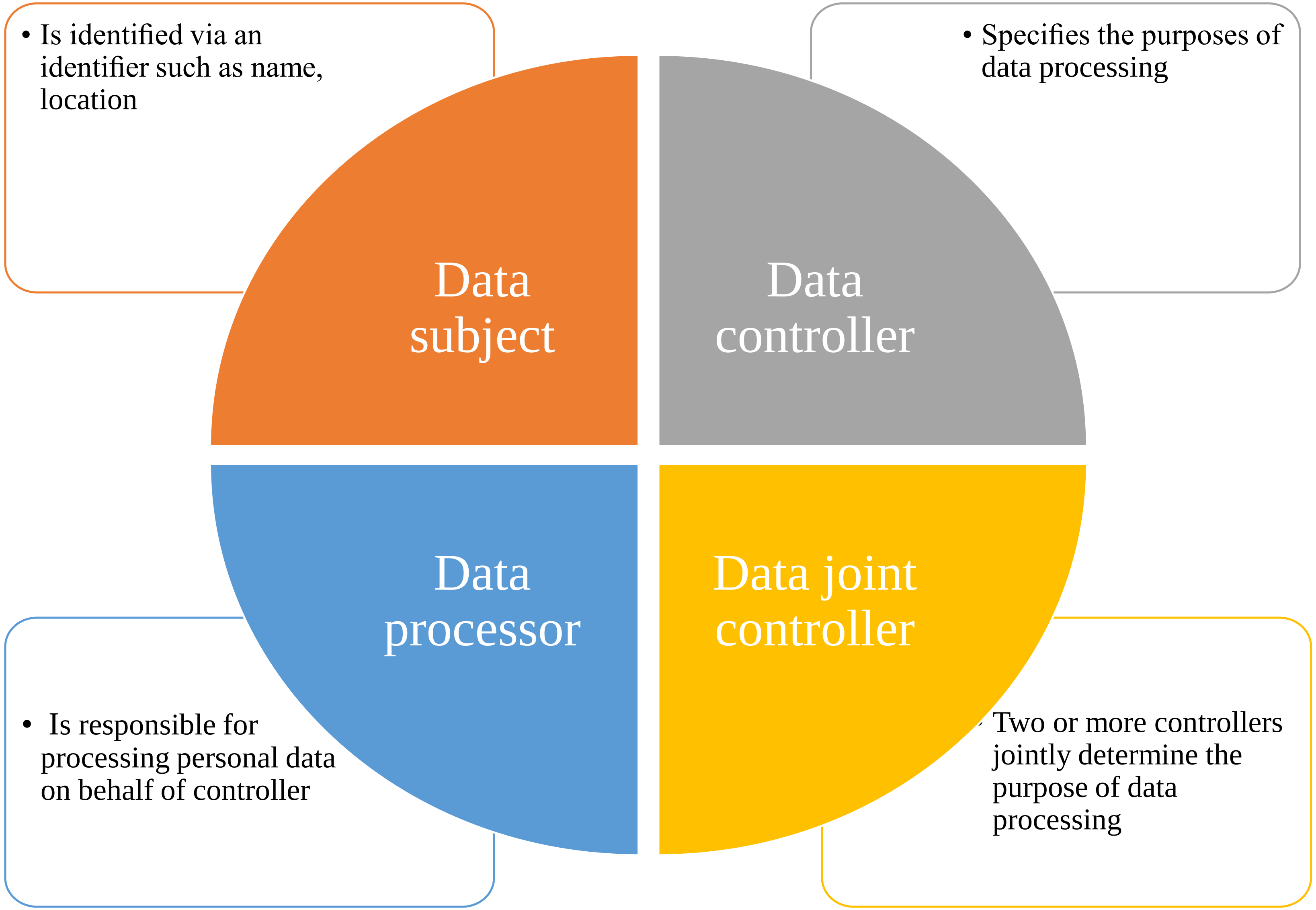
Sexual life or orientation

Genetic or biometric

Examples of data processing

- Staff management and payroll administration
- Access to/consultation of a contacts database containing personal data
- Sending promotional emails (ads)
- Posting/putting a photo of a person on a website
- Storing IP addresses or MAC addresses
- Video recording (CCTV)

Key elements of GDPR



- Is identified via an identifier such as name, location

- Specifies the purposes of data processing

- Is responsible for processing personal data on behalf of controller

- Two or more controllers jointly determine the purpose of data processing

Examples of controller, processor

- A network of town-centre CCTV cameras is operated by a **local council** jointly with the **police**. Both are involved in deciding how the CCTV system is run and what the images it captures are used for.
  - The **council** and the **police** are **joint controllers** in relation to personal data processed in operating the system

- **Your website** collects email addresses and other personal data provided by customers for sales and **marketing** purposes. If you provide the data and the instructions, then:
  - **you** are the **data controller** and **Marketing and Promotions Ltd** is the **data processor**

Rights and obligations in GDPR

Right to be informed

- Data subjects have the right to receive privacy information such as:
  - How their data will be processed
  - Who it will be shared with
  - What their rights are with respect to it

- The information supplied by controller or processor must be:
  - Concise, transparent, intelligible and easily accessible
  - Written in clear and plain language, particularly if addressed to a child
  - Provided free of charge

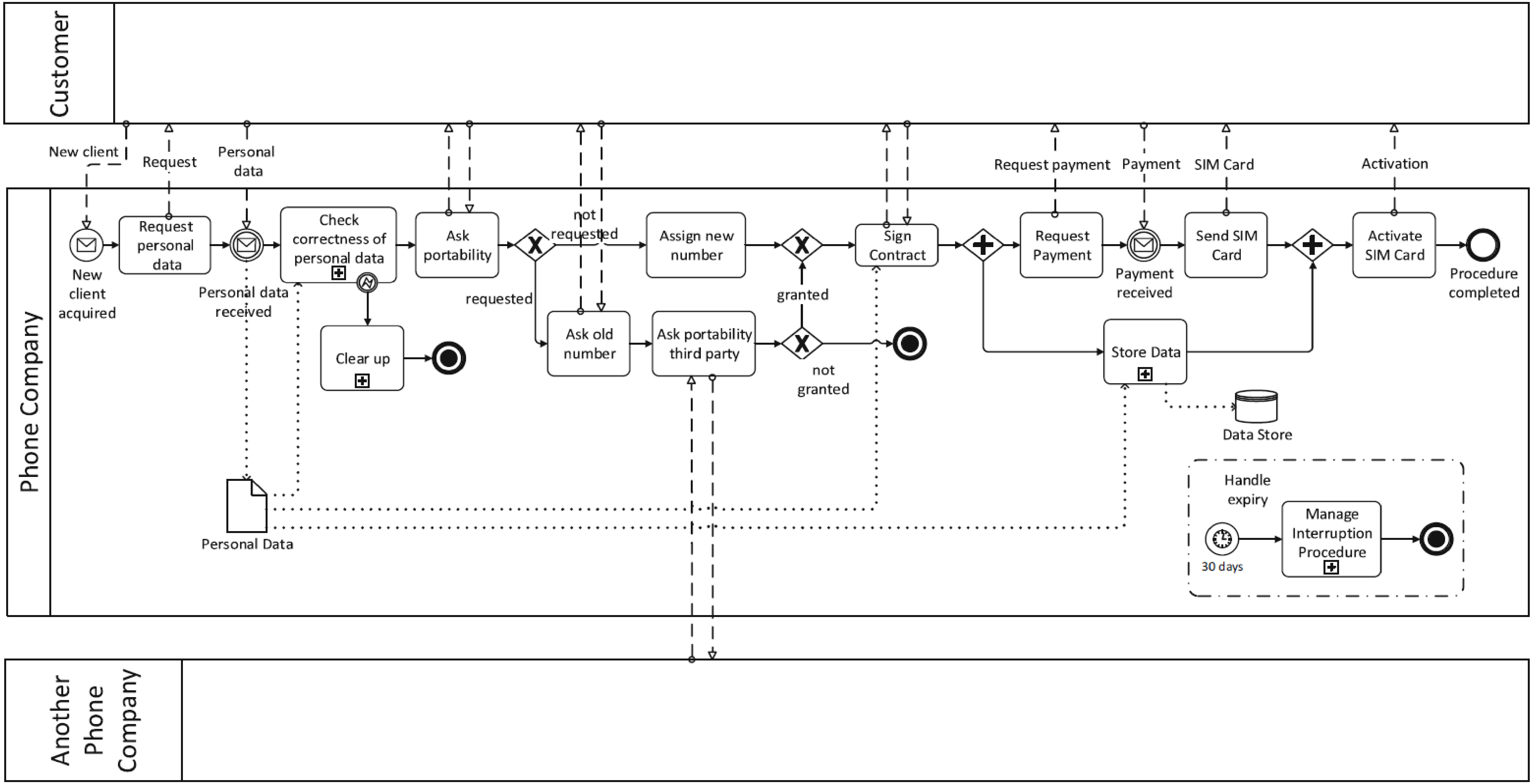
Right of access

- Data subjects have the right to:
  - Have confirmation that their data is being processed
  - Be aware of and verify the lawfulness of the processing
  - Request access to their personal data

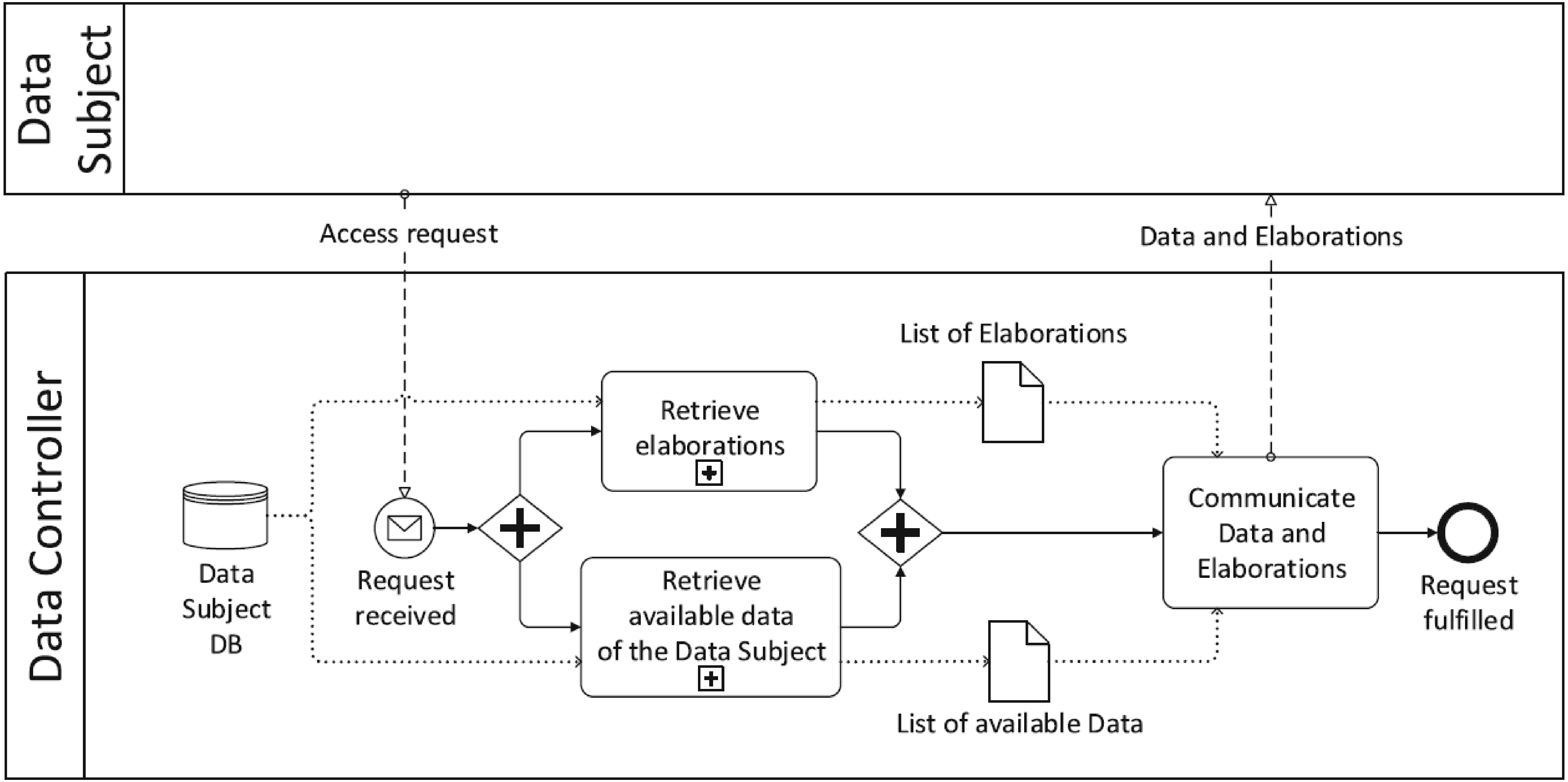
- The controller or processor must:
  - Take reasonable steps to verify the identity of the requestor
  - Provide requested information free of charge

For electronic format of requests, actors should provide information in a commonly used electronic format

Example—A phone company



Right of access in BPMN

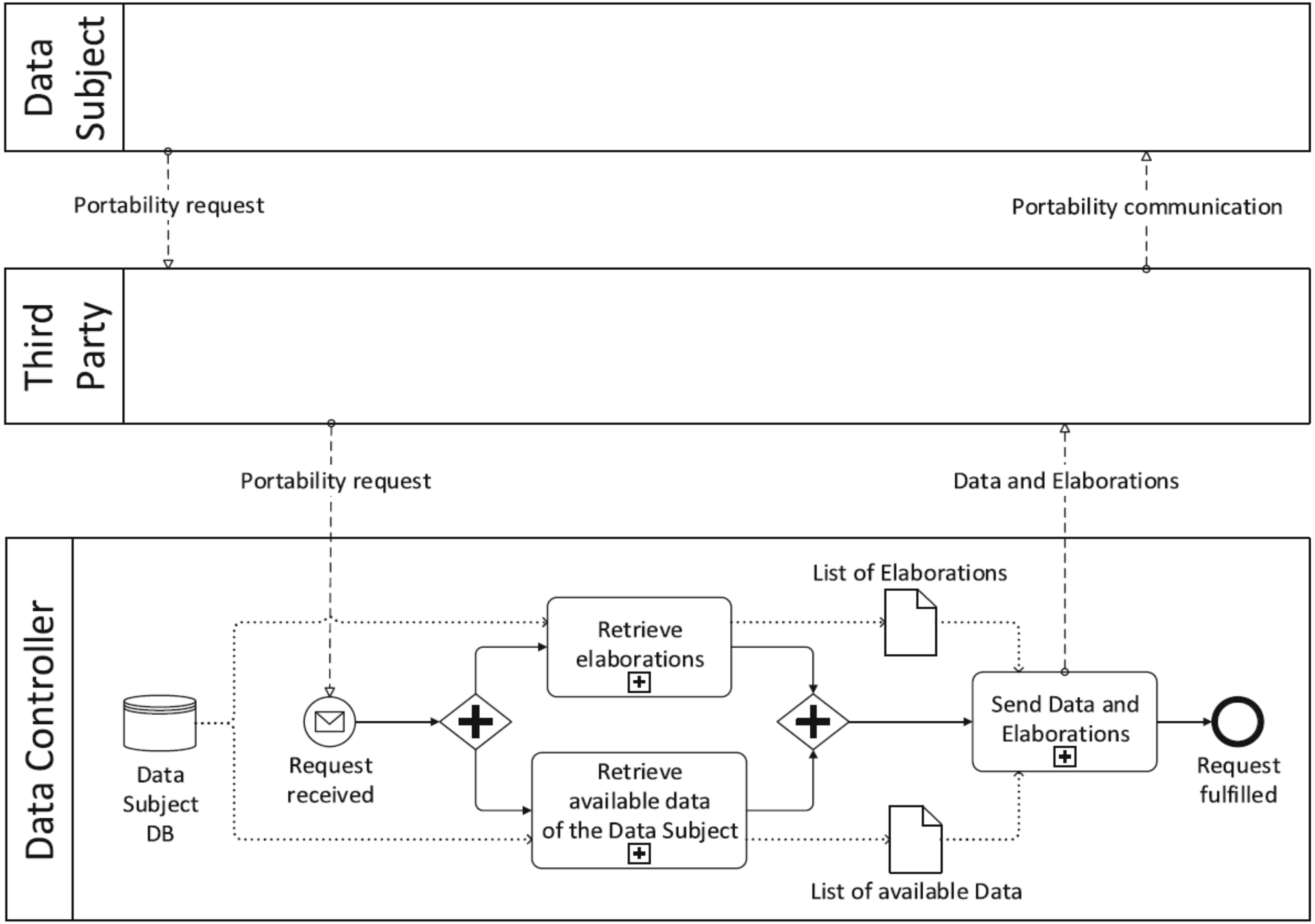


Right to data portability

- Data subjects have the right to:
  - Receive their personal data in a structured, commonly used and machine readable format
  - Transmit their data to another controller without any delay

- This right only applies if:
  - Data subject has provided you with their personal data
  - The data is processed by consent
  - Processing is carried out by automated means

Right to data portability in BPMN

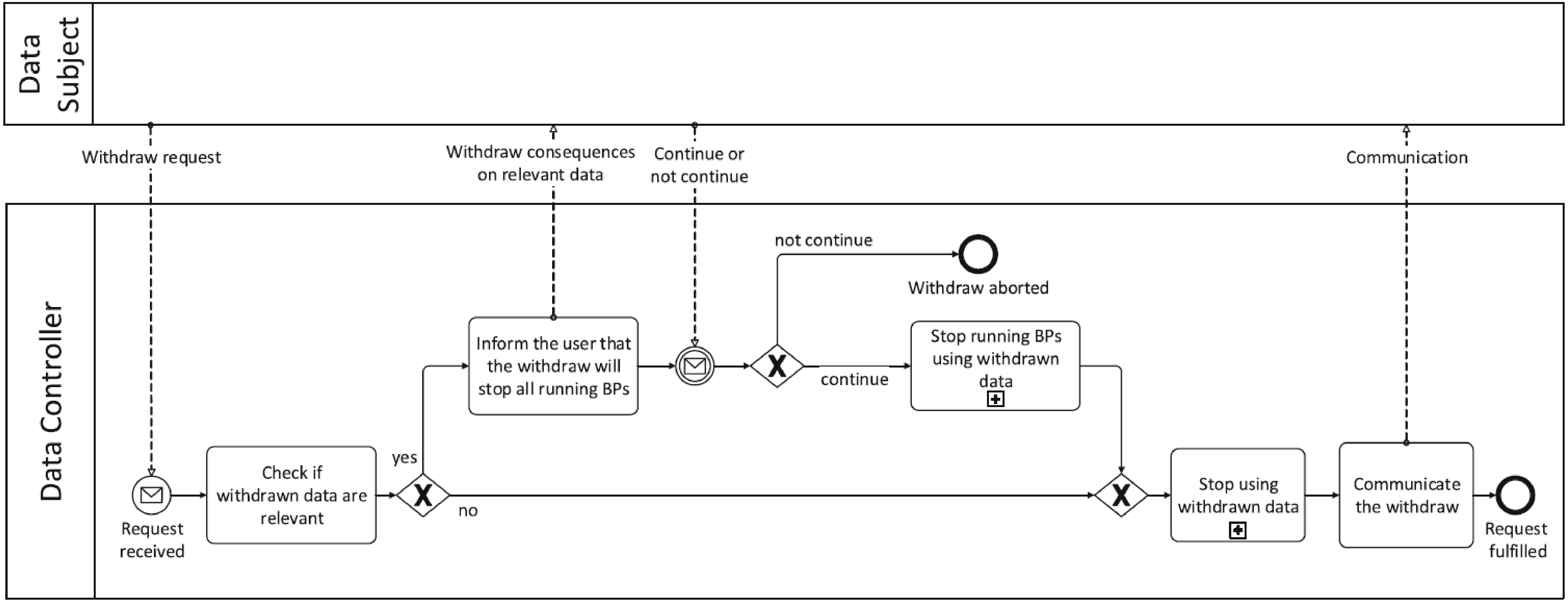


Right to be forgotten

- Data subjects have the right to erasure if:
  - Personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
  - Data subjects withdraw consent
  - Their data has been unlawfully processed

- The controllers/processors must:
  - Comply with the request unless they have a legal obligation to continue processing the data
  - Take steps to inform any other sub processors to erase personal data

Right to be forgotten in BPMN

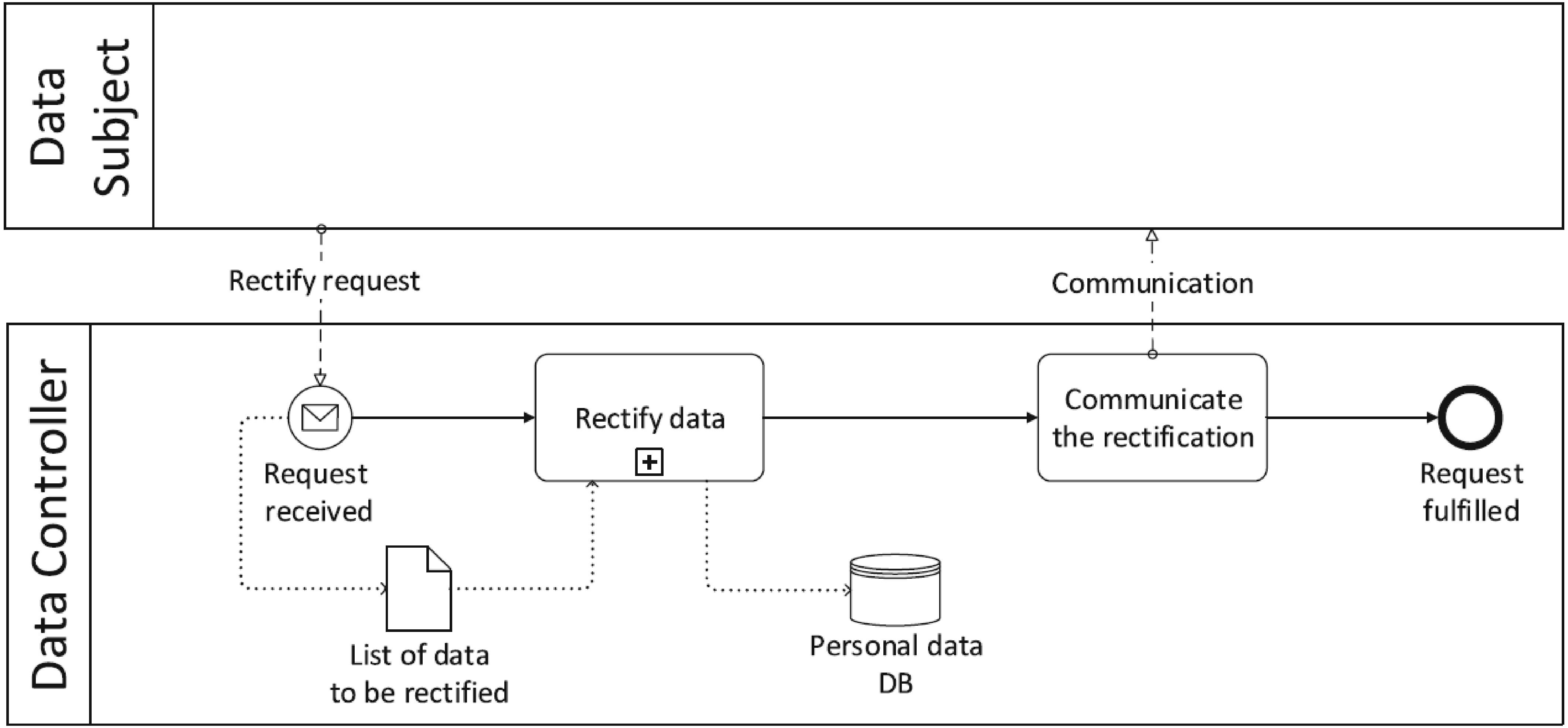

Data Subject
Data Controller
Withdraw request
Withdraw consequences on relevant data
Continue or not continue
Communication
Request received
Check if withdrawn data are relevant
yes
no
Inform the user that the withdraw will stop all running BPs
not continue
Withdraw aborted
continue
Stop running BPs using withdrawn data
Stop using withdrawn data
Communicate the withdraw
Request fulfilled

Right to rectification

- Data subjects have the right to:
    - Their personal data being accurate
    - Request inaccurate data be corrected and incomplete data completed

- The controllers/processors must:
    - Correct inaccurate matters of fact and confirm rectification
    - Inform recipients of incorrect data of the rectification
    - Inform the data subject if you are not amending the record and why

Right to rectification in BPMN



Some obligations:

User consent

Accountability

Breach notification

User consent

Methods for obtaining consent:

- Tick box
- Signing a declaration/form
- Sending an email
- Selecting Yes/No options
- Oral statement

Whichever method is used, GDPR requires us to keep evidence of consent (accountability)

Verifying User consent

Targeted marketing:

Sending advertisements to registered emails

Do I need consent? (Am I sending marketing emails?)

No → Send non-marketing email as usual

Yes ↓

Do I already have valid consent (specific, informed, opt-in)?

No → Draw up programme to collect valid consent + evidence

Yes ↓

Can I provide evidence of that consent?

No → Draw up programme to collect valid consent + evidence

Yes ↓

Send marketing email

Accountability under GDPR

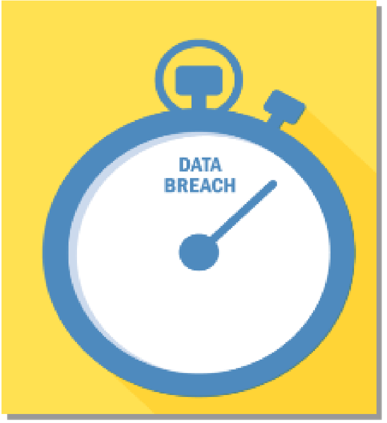
The GDPR’s accountability principle (Art. 5(2)) requires controller/processor to be able to demonstrate how you comply with the data protection principles

This can be demonstrated by having effective policies and procedures in place such as:

- Processing data in a transparent manner
- Maintaining records of processing

Breach notification

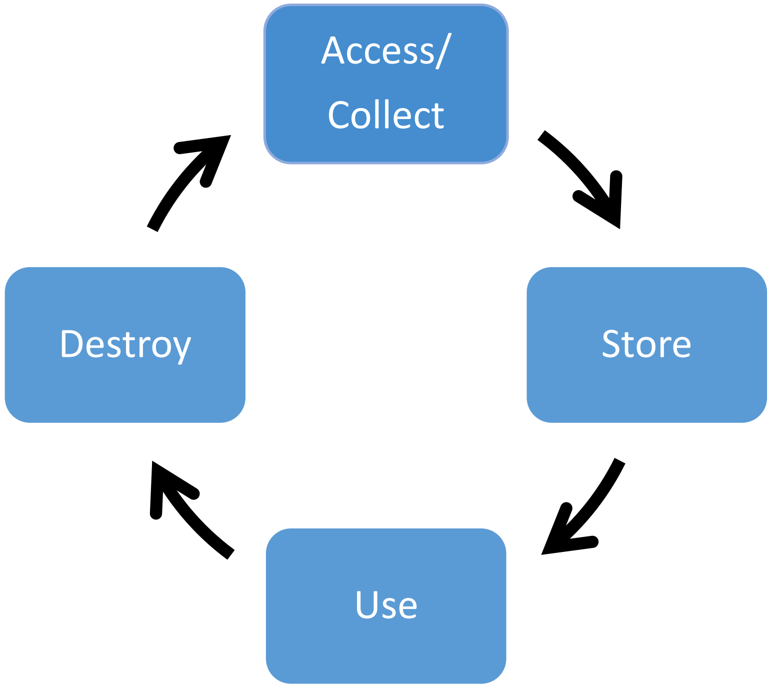
- Notify Information Commissioner’s office (ICO):
  - Not later than 72 hours (Can add detail later)
  - Where likely to result in a **risk** to rights and freedoms of individuals



- Notify data subject:
  - Without undue delay
  - Where likely to result in a **high risk** to rights and freedoms of individuals

GDPR life cycle

GDPR information life cycle



Access / collect

1. What you are allowed to collect
2. What you must tell the person in advance (purpose)
3. What you must get from them (their consent)

Store

1. How you must store it
2. Where it can be stored
3. What happens if you lose it

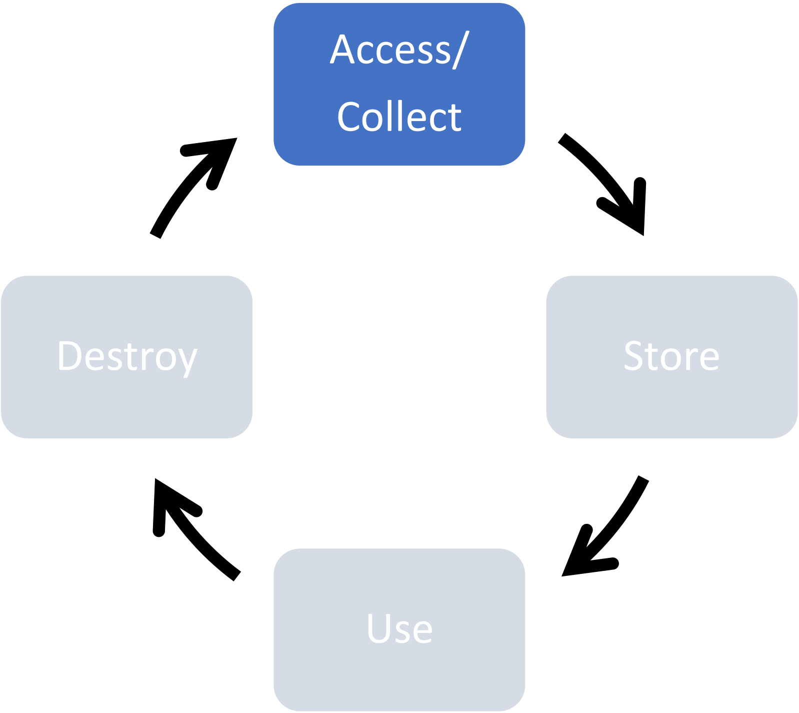
Use

1. What you can use it for
2. What you can't use it for

Destroy

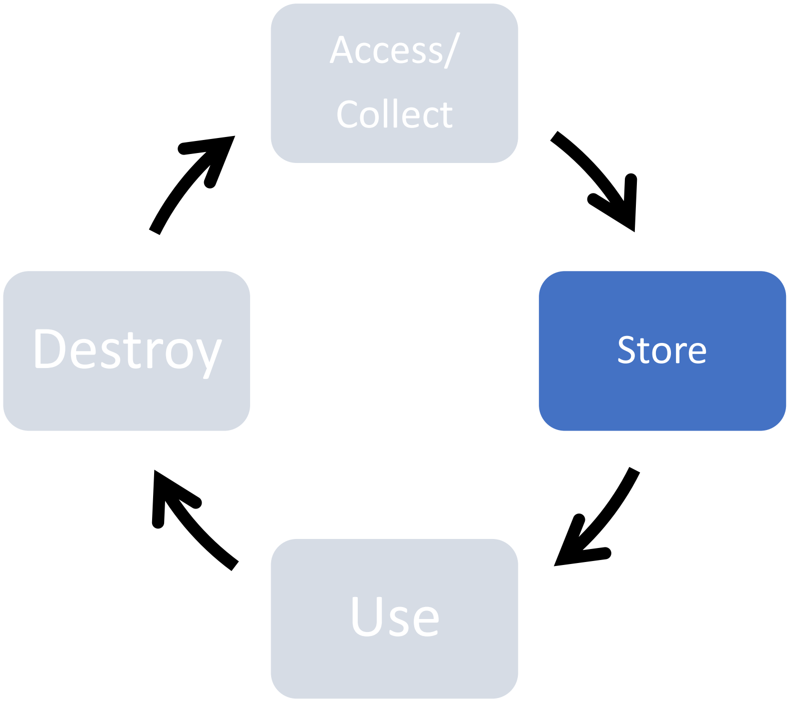
1. How long you can keep it for
2. When you must destroy information

GDPR information life cycle 2



1. **Data Minimisation** (Only ask for what is needed)
2. **Privacy Notices** (Clearly inform what, why, who and where)
3. **Data Subject Rights** (state the persons rights under the legislation)
4. **Obtain Consent** (consent must be freely given and explicit for the purpose or purposes)
5. **Ensure Protection** (encryption, secure login)

GDPR information life cycle 3



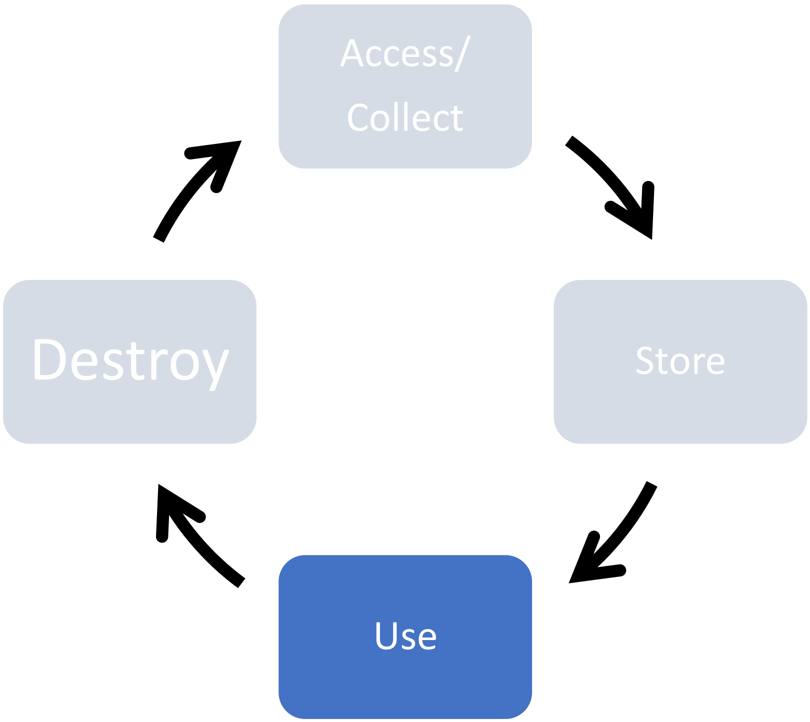
1. **Safe and Secure** (Information must be stored appropriately e.g. locked cabinets/password protected files)

2. **Restricted Access** (Only authorised persons should have access to it)

3. **Data Inventory** (Information captured should be recorded)

4. **Data Breaches** (Processes to detect, report and investigate Data Breaches must be in place)

GDPR information life cycle 4



1. **Appropriate use** (Must be for the purpose(s) originally stated)

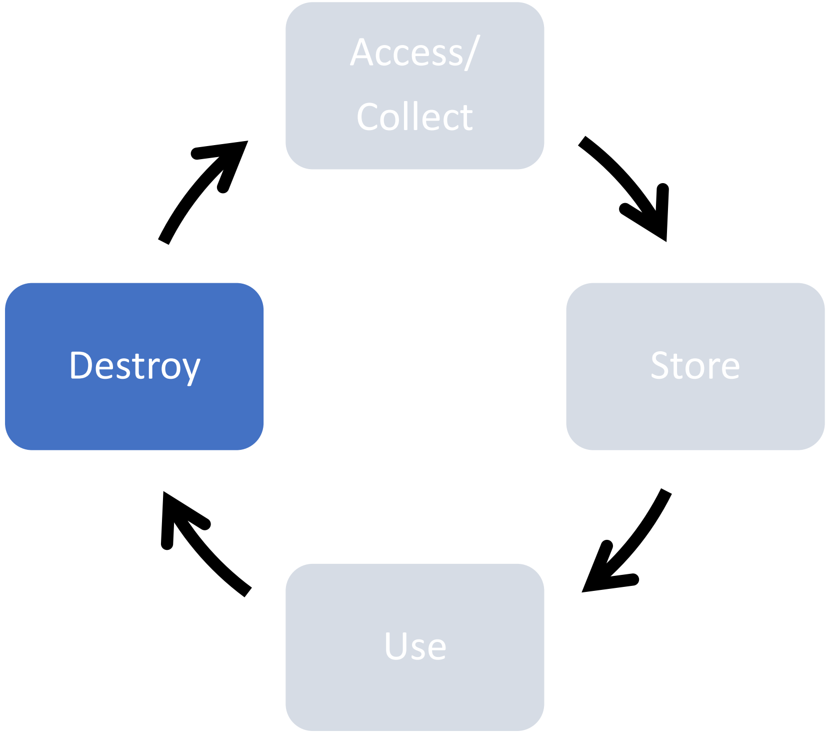
2. **Consent** (Must have person’s consent or a lawful basis for processing it)

3. **Manage Consent** (Individuals have the right to revoke consent for part or all of the processing, this must be managed)

4. **Restricted** (Profiling or automated decision making are restricted-underage person)

5. **International Transfers** (Any processing that occurs outside EU must have been communicated to person at time of data capture and must have additional safeguards in place)

GDPR information life cycle 5



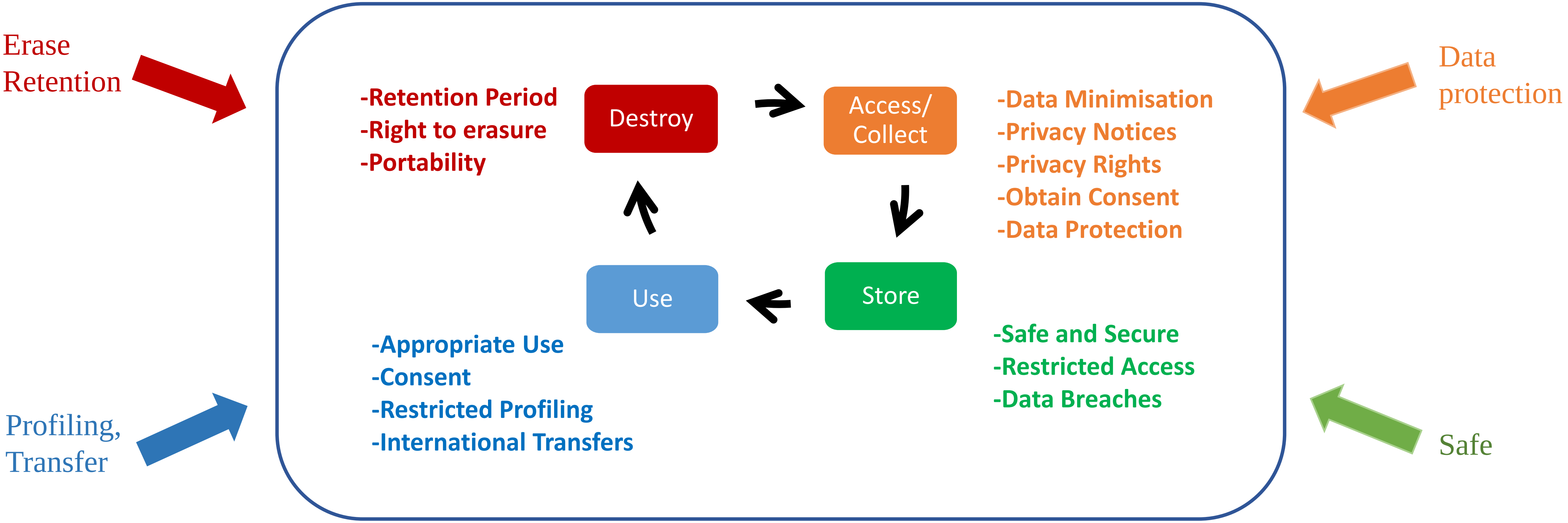
1. **Retention Period** (Retention periods must be documented and justified and data must be destroyed after its useful retention period has expired)

2. **Right to erasure** (Must be erased upon request from person)

3. **Portability** (Must be provided in standard format)

4. **Third Party Copies** (All copies of information must be deleted including those held by third parties)

GDPR life cycle summary



Erase
Retention

-Retention Period
-Right to erasure
-Portability

Destroy

Access/
Collect

Data
protection

-Data Minimisation
-Privacy Notices
-Privacy Rights
-Obtain Consent
-Data Protection

Store

Safe

-Safe and Secure
-Restricted Access
-Data Breaches

Use

Profiling,
Transfer

-Appropriate Use
-Consent
-Restricted Profiling
-International Transfers

Translation of GDPR into codes

GDPR legal questions

L1: Does your service deal with sensitive customer data?

L2: Does your service support encryption or authentication access for the customer data?

L3: Does your service give the choice of EU-based migration or local storage of personal data?

L4: Has your underlying connected provider (IaaS/PaaS) been certified for their Binding Corporate Rules (BCR) clauses by a EU DPA?

…

BCR is internal rules (e.g. code of conduct) adopted by a community of multinational companies that want to move customer data internationally across various jurisdictions

GDPR translation to codes

```
Program check of GDPR compliance
Legal_Compliance=True;

If (L1==Yes){
    If(L2==No){
       Legal_Compliance=False;
       Return Legal_Compliance;
   }
}

If (L3==No){
    If(L4==No) {
        Legal_Compliance=False;
        Return Legal_Compliance;
   }
}
```

PSEUDOCODE
SOLUTIONS

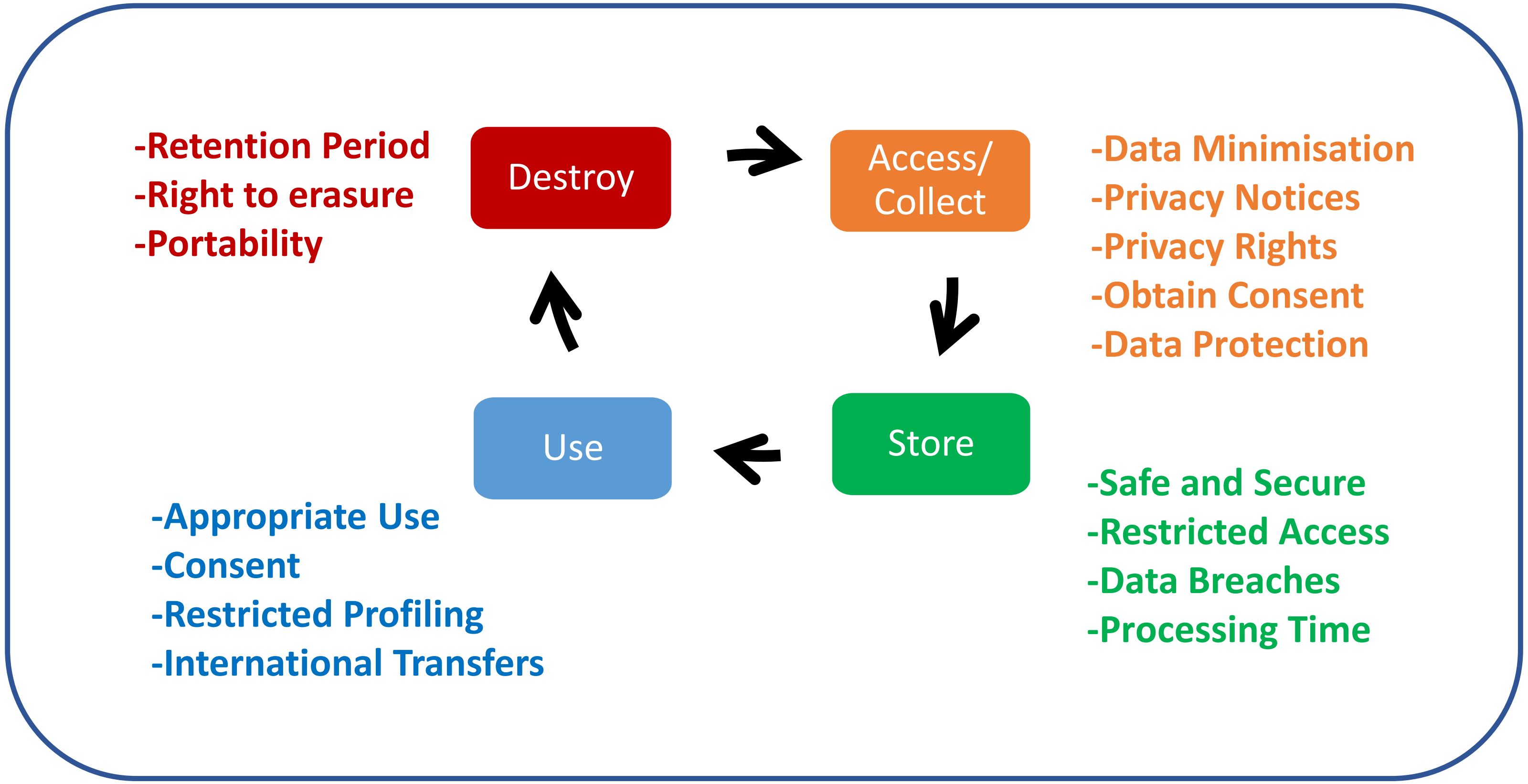
Intended operations and legal questions

Read

Write/Destroy

Profiling

Transfer



-Retention Period
-Right to erasure
-Portability

-Data Minimisation
-Privacy Notices
-Privacy Rights
-Obtain Consent
-Data Protection

-Safe and Secure
-Restricted Access
-Data Breaches
-Processing Time

-Appropriate Use
-Consent
-Restricted Profiling
-International Transfers

GDPR rules for operations 1

- **Read**: The Art. 32(1)(a) of GDPR requires actors who read or access sensitive personal data to have an **encryption** or authentication control mechanism for preventing unauthorized access to the data.

- **Write/destroy**: The Art. 17 of GDPR requires actors who write or store personal data to provide a capability for their customers to **erase** their personal data at anytime. Moreover, the Art. 5(1)(e) of GDPR does not allow actors to store personal data **longer** than the time which is necessary for data processing.

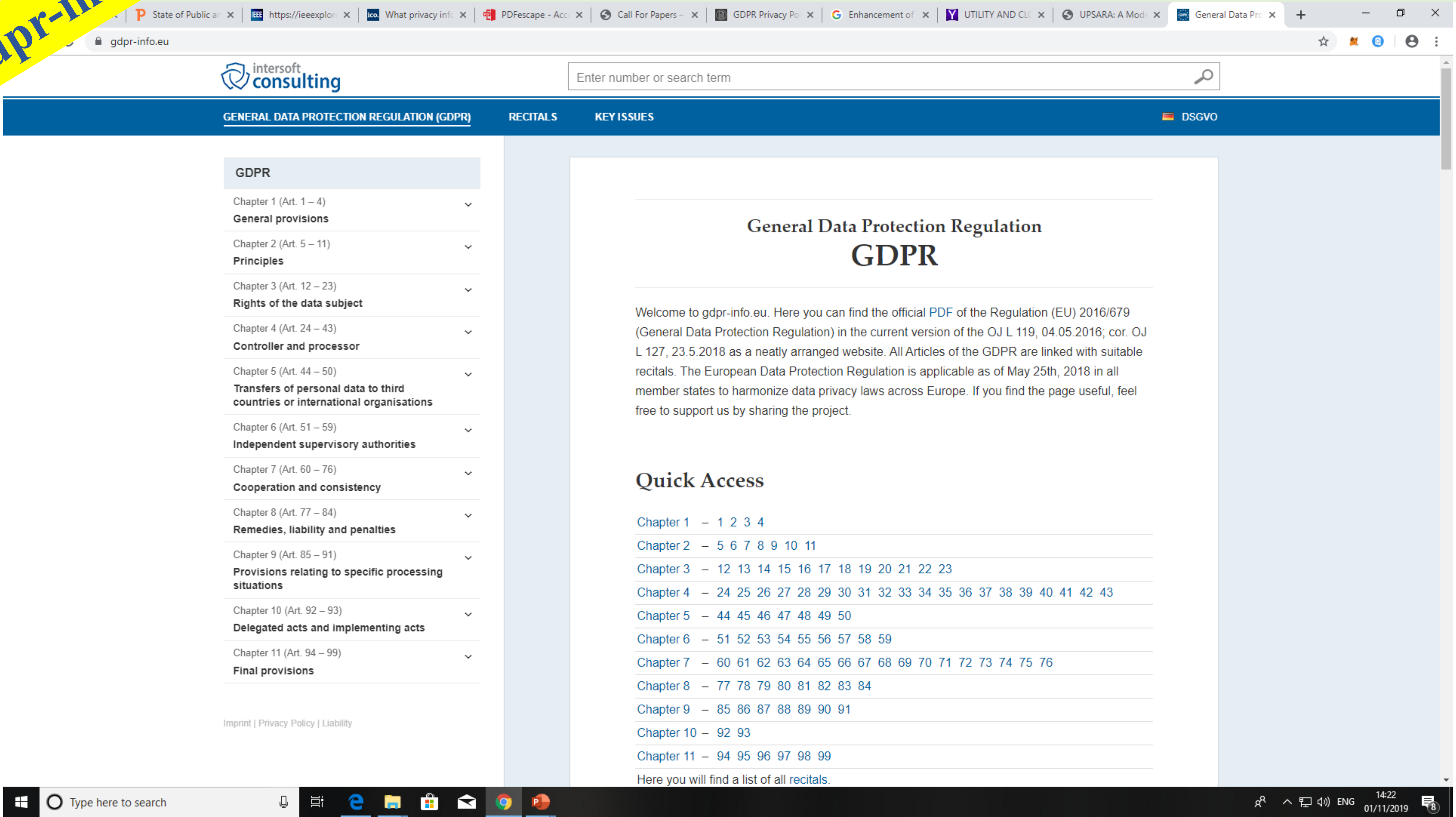
GDPR rules for operations 2

- **Profiling**: The Art. 22 of GDPR states that any automated profiling operation on customers who are **under 18** or whose personal data are in the category of sensitive data is risky.

- **Transfer**: The Art. 44–47 of GDPR restrict actors to transfer personal data only inside **Europe** or the countries holding Binding Corporate Rules (**BCR**) certifications.

GDPR articles

gdpr-info.eu



GDPR

Chapter 1 (Art. 1 – 4)
General provisions

Chapter 2 (Art. 5 – 11)
Principles

Chapter 3 (Art. 12 – 23)
Rights of the data subject

Chapter 4 (Art. 24 – 43)
Controller and processor

Chapter 5 (Art. 44 – 50)
Transfers of personal data to third countries or international organisations

Chapter 6 (Art. 51 – 59)
Independent supervisory authorities

Chapter 7 (Art. 60 – 76)
Cooperation and consistency

Chapter 8 (Art. 77 – 84)
Remedies, liability and penalties

Chapter 9 (Art. 85 – 91)
Provisions relating to specific processing situations

Chapter 10 (Art. 92 – 93)
Delegated acts and implementing acts

Chapter 11 (Art. 94 – 99)
Final provisions

Imprint | Privacy Policy | Liability

General Data Protection Regulation
GDPR

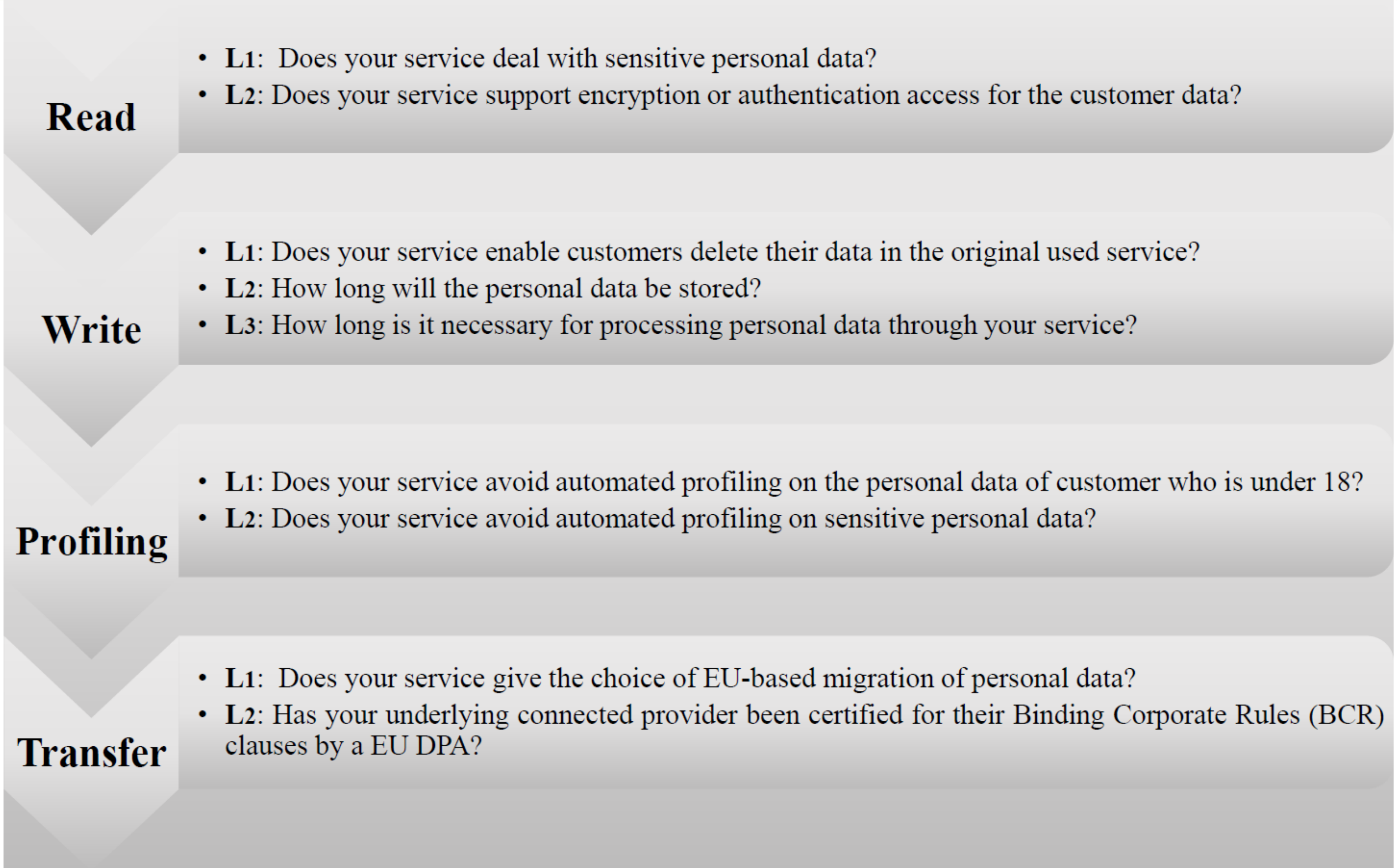
Welcome to gdpr-info.eu. Here you can find the official PDF of the Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018 as a neatly arranged website. All Articles of the GDPR are linked with suitable recitals. The European Data Protection Regulation is applicable as of May 25th, 2018 in all member states to harmonize data privacy laws across Europe. If you find the page useful, feel free to support us by sharing the project.

Quick Access

Chapter 1 –	1 2 3 4
Chapter 2 –	5 6 7 8 9 10 11
Chapter 3 –	12 13 14 15 16 17 18 19 20 21 22 23
Chapter 4 –	24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
Chapter 5 –	44 45 46 47 48 49 50
Chapter 6 –	51 52 53 54 55 56 57 58 59
Chapter 7 –	60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76
Chapter 8 –	77 78 79 80 81 82 83 84
Chapter 9 –	85 86 87 88 89 90 91
Chapter 10 –	92 93
Chapter 11 –	94 95 96 97 98 99

Here you will find a list of all recitals.

Classification of purposes of data processing



Read

- **L1**: Does your service deal with sensitive personal data?
- **L2**: Does your service support encryption or authentication access for the customer data?

Write

- **L1**: Does your service enable customers delete their data in the original used service?
- **L2**: How long will the personal data be stored?
- **L3**: How long is it necessary for processing personal data through your service?

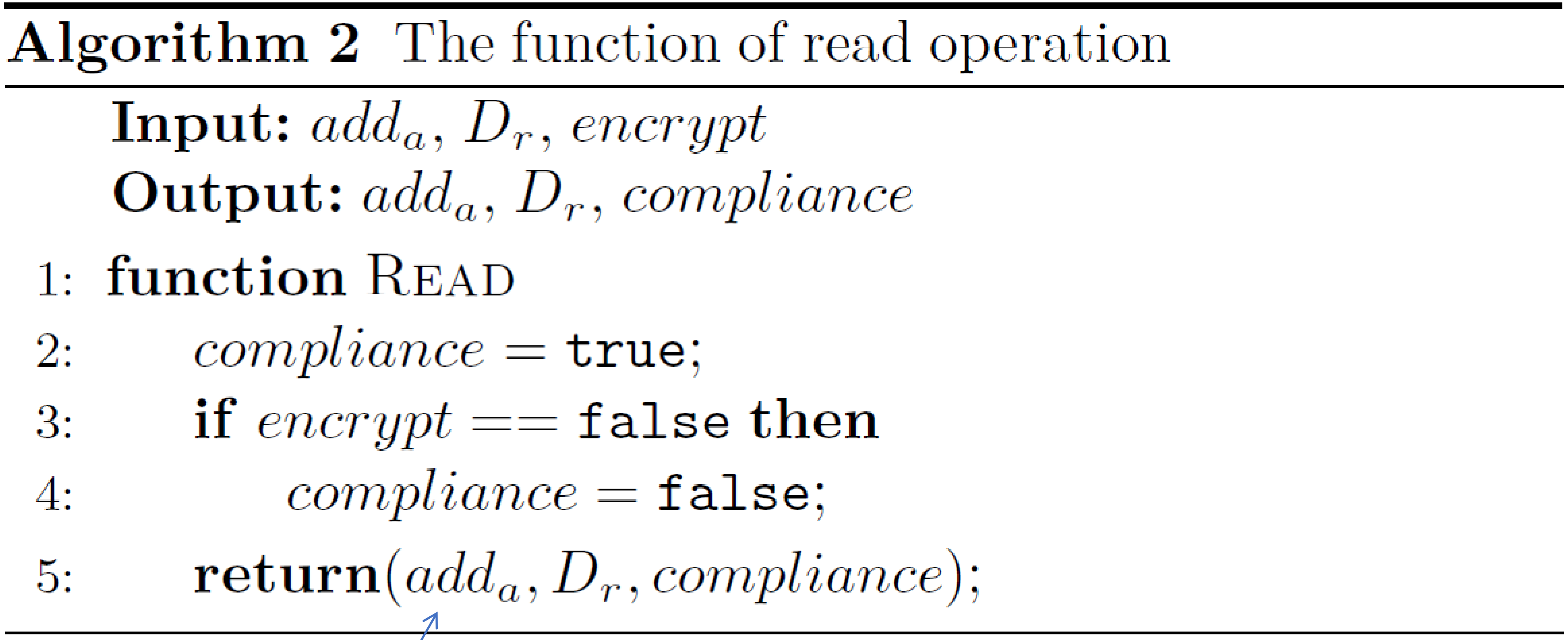
Profiling

- **L1**: Does your service avoid automated profiling on the personal data of customer who is under 18?
- **L2**: Does your service avoid automated profiling on sensitive personal data?

Transfer

- **L1**: Does your service give the choice of EU-based migration of personal data?
- **L2**: Has your underlying connected provider been certified for their Binding Corporate Rules (BCR) clauses by a EU DPA?

Read operation

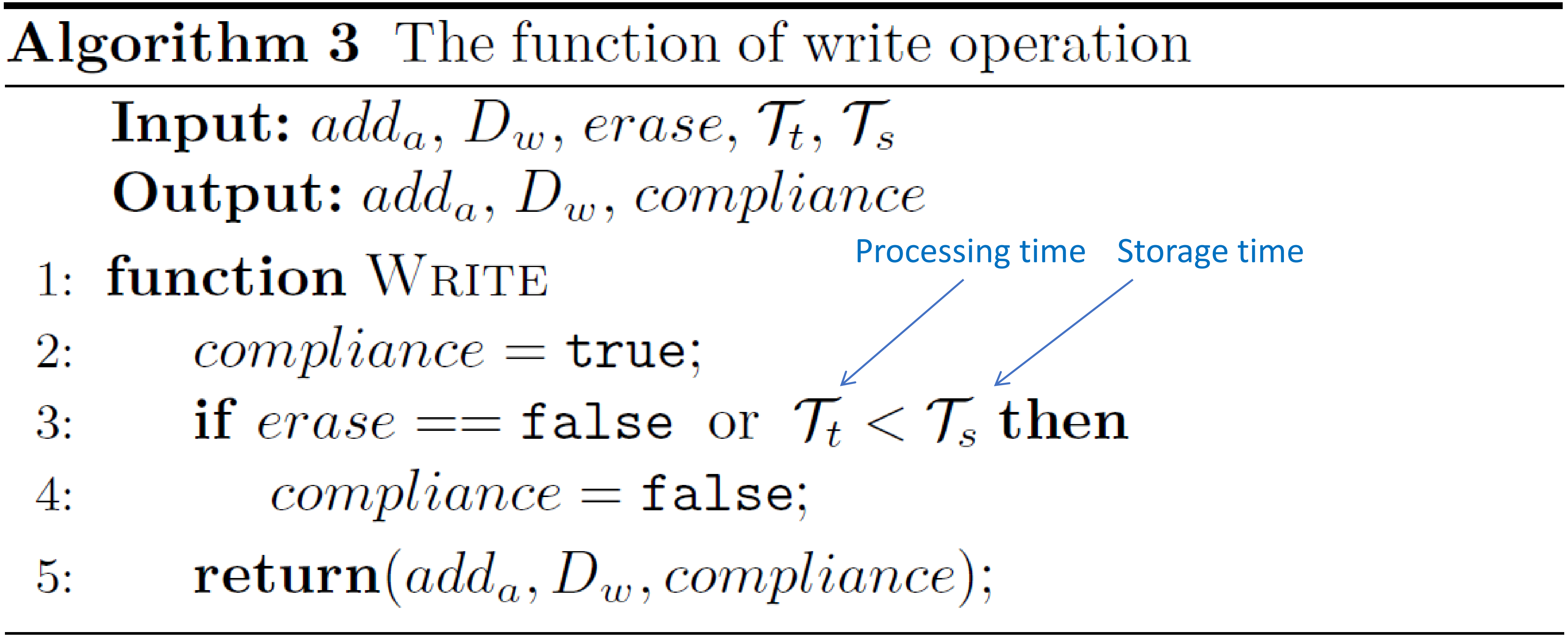


Algorithm 2 The function of read operation

```
Input: $add_a$, $D_r$, $encrypt$
Output: $add_a$, $D_r$, $compliance$
function READ
    $compliance$ = true;
    if $encrypt$ == false then
        $compliance$ = false;
    return($add_a, D_r, compliance$);
```

Actor address

Write operation



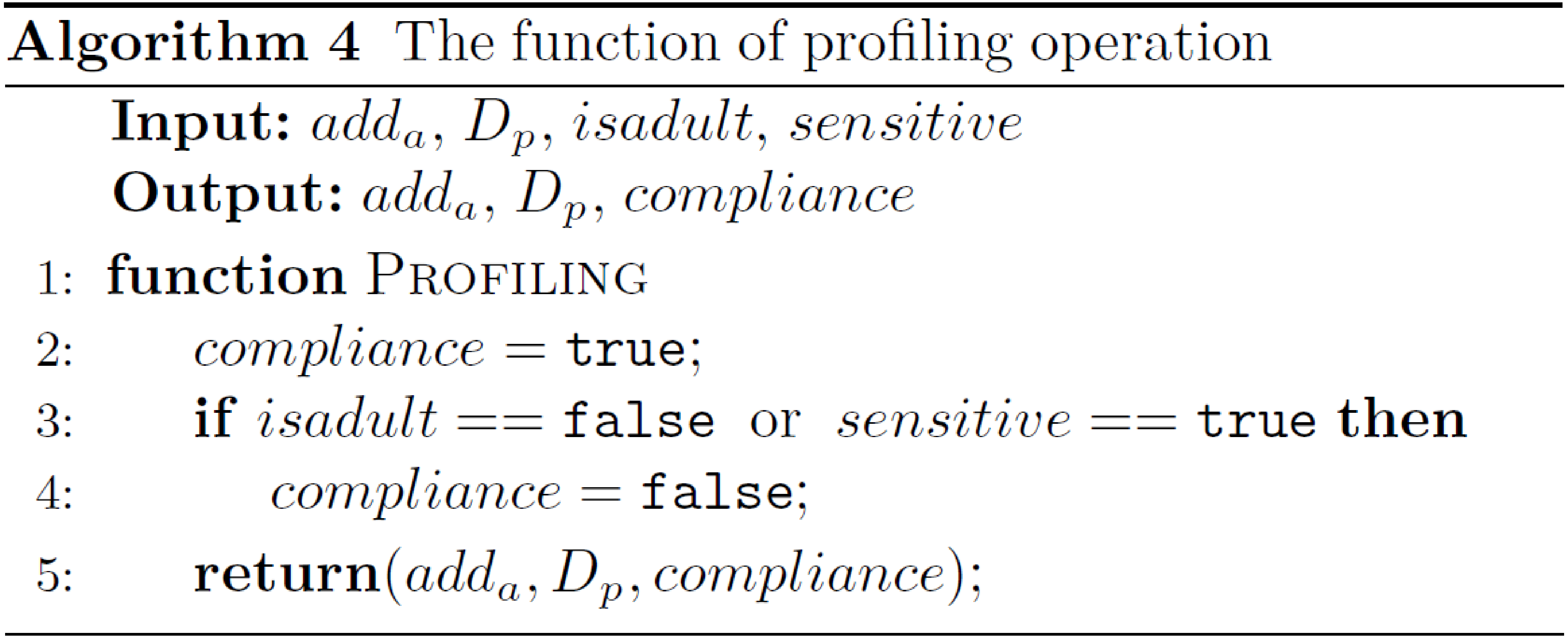
Algorithm 3 The function of write operation

```
    Input: $add_a$, $D_w$, $erase$, $\mathcal{T}_t$, $\mathcal{T}_s$
    Output: $add_a$, $D_w$, $compliance$
function WRITE
    $compliance$ = true;
    if $erase$ == false or $\mathcal{T}_t < \mathcal{T}_s$ then
        $compliance$ = false;
    return($add_a$, $D_w$, $compliance$);
```

Processing time

Storage time

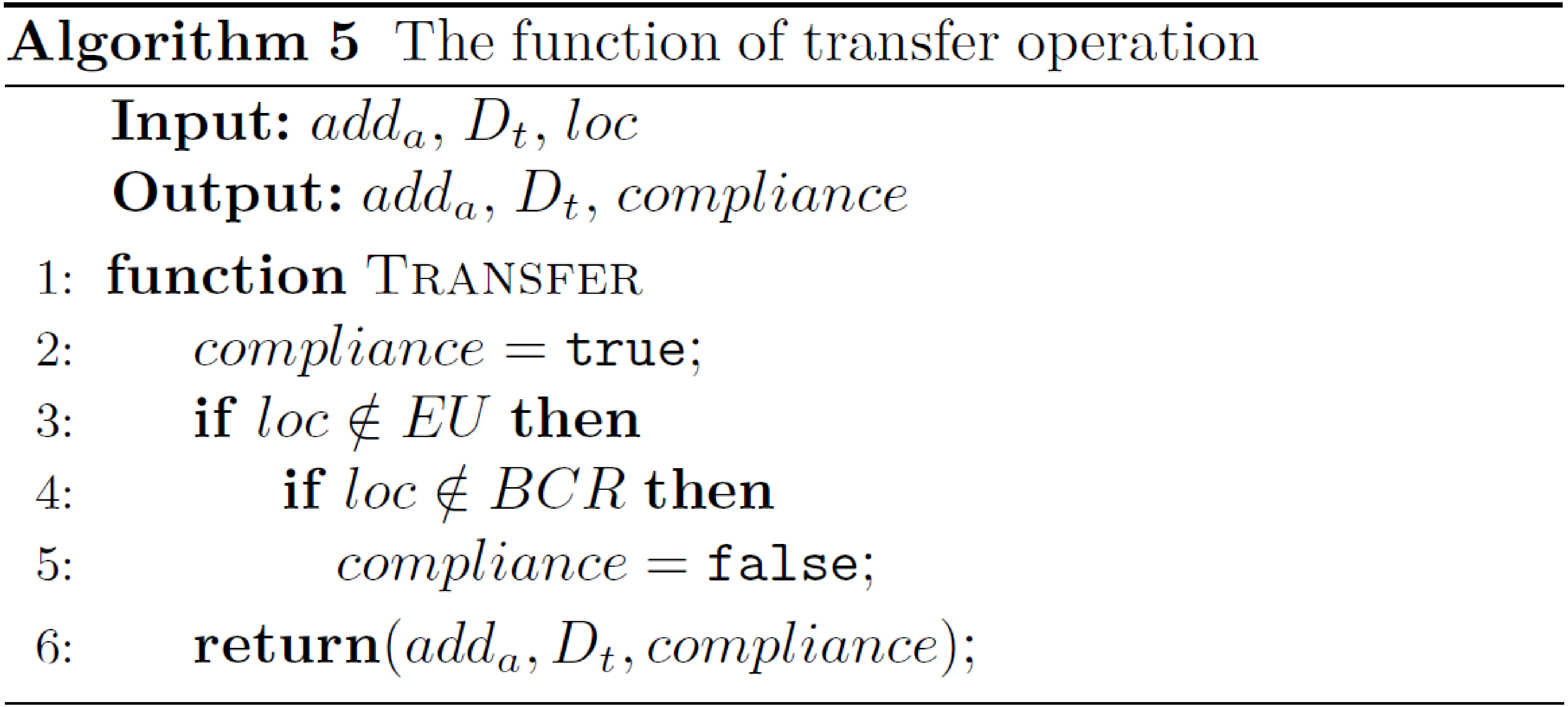
Profiling operation



Algorithm 4 The function of profiling operation

```
Input: $add_a$, $D_p$, $isadult$, $sensitive$
Output: $add_a$, $D_p$, $compliance$
function PROFILING
    $compliance = \texttt{true}$;
    if $isadult == \texttt{false}$ or $sensitive == \texttt{true}$ then
        $compliance = \texttt{false}$;
    return($add_a, D_p, compliance$);
```

Transfer operation



Algorithm 5 The function of transfer operation

```
Input: $add_a$, $D_t$, $loc$
Output: $add_a$, $D_t$, $compliance$
function Transfer
    $compliance = $ true;
    if $loc \notin EU$ then
        if $loc \notin BCR$ then
            $compliance = $ false;
    return($add_a, D_t, compliance$);
```

Thank you very much for your attention

Who is data controller, processor?
What is purpose of data processing?

- Car4you company has entered into a contract with Marketing1 company, providing clear instruction to Marketing1 to send an email, advertising their new range of cars.
- They provide Marketing1 with an email template and a spreadsheet of personal email addresses (all obtained with valid GDPR consent).
- Car4you outline the spreadsheet is only to be used for sending this advertising email.
- Marketing1 are bound by Car4you instructions.