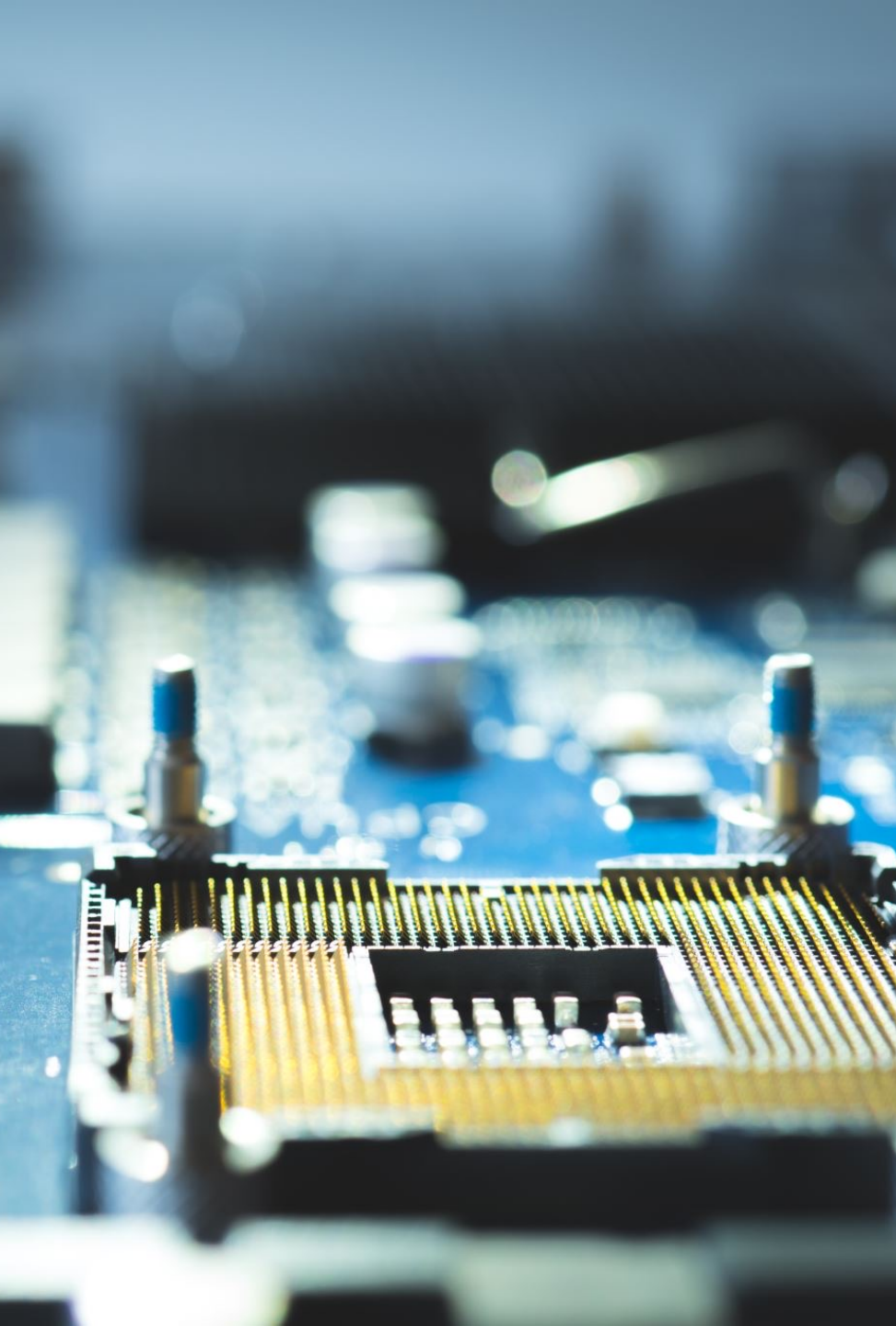


The Duties of the Controller and Processor (I)

Elisa Spiller, Ph.D.

University of Padova | Dept. of Mathematics

Course of Law and Data 2022-2023



learning objectives

- Controllers and joint-controllership
- Processors
- Security duties



1. Controller

Who is the **controller**?

GDPR, Article 4 – *Definitions*

«For the purposes of this Regulation:

(7) '**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data»

(a) natural or legal person, public authority, agency or other body

(b) which determines

(c) alone or jointly with others

(d) purposes and means

(e) of the processing of personal data

(a) Subjects

natural person

legal person

public authority

agency

other body

- **In principle, there is no limitation** as to the type of entity that may assume the role of a controller
- It might be an organisation, but it might also be an individual or a group of individuals
- **In practice, however, it is usually the organisation as such, and not an individual within the organisation** (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR.

(b) Control

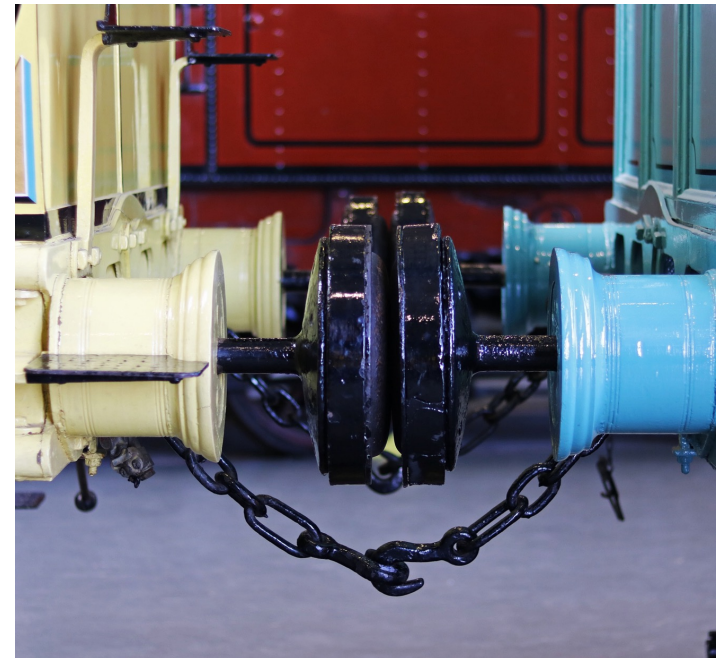
- The controller has an influence over the processing, by virtue of an exercise of decision-making power
- A controller is a body that decides certain key elements about the processing
- This controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case
- Controller is a functional concept, it is therefore based on a factual rather than a formal analysis

why is this processing taking place?

who decided that the processing should take place for a particular purpose?

(c) **Alone** or **jointly** with others

- This means that **several different entities may act as controllers for the same processing**, with each of them then being subject to the applicable data protection provisions. Correspondingly, an organization can still be a controller **even if it does not make all the decisions as to purposes and means**.
- → *see Joint controllers later*



(d) Purposes and Means

- Determining the purposes and the means amounts to **deciding respectively the "why" and the "how"** of the processing
- The controller **must decide on both purpose and means** of the processing. As a result, the controller cannot settle with only determining the purpose. It must also make decisions about the means of the processing.
- Even though decisions on non-essential means (*e.g.* type of software) can be left to the processor, the controller must still stipulate certain elements in the processor agreement, such as in relation to the security requirement

PURPOSE

- as an anticipated outcome that is intended or that guides your planned actions

MEANS

- as how a result is obtained or an end is achieved
 - Essential means
 - Non-essential means

(e) Processing of personal data

- GDPR, Article 4 – *Definitions*
- «For the purposes of this Regulation:
- (2) ‘**processing**’ means *any operation or set of operations which is performed on personal data or on sets of personal data*, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction»

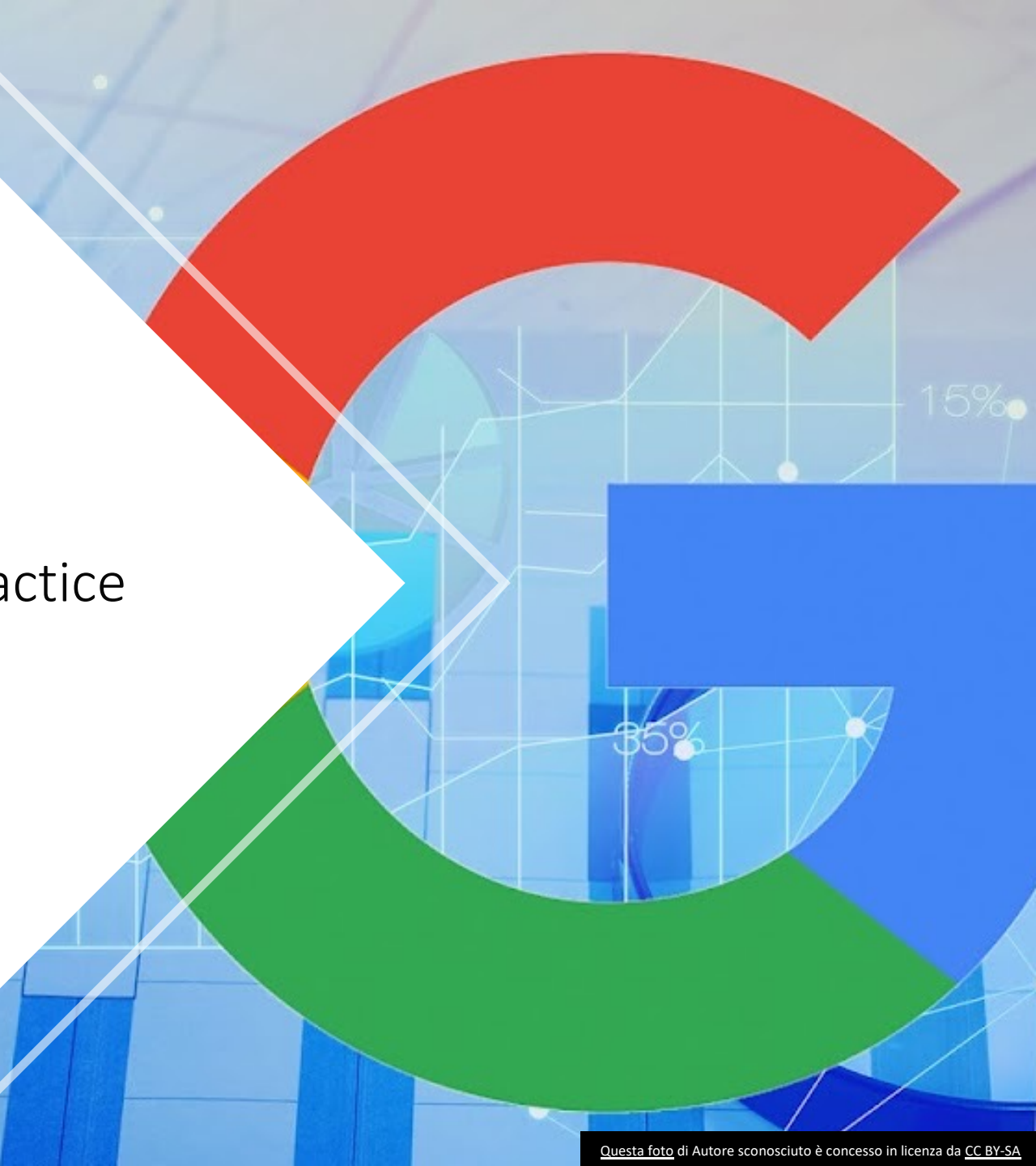
→ In theory, concept of a controller can be linked either to a single processing operation or to a set of operations

→ In practice, this may mean that the control exercised by a particular entity may extend to the entirety of processing at issue but may also be limited to a particular stage in the processing.

Anyone who decides to process data must consider whether this includes personal data and, if so, what the obligations are according to the GDPR



In practice



Joint controllers

GDPR, Article 26 – Joint Controllers

«[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.»

- Assessing the existence of joint controllers requires examining **whether the determination of purposes and means** that characterize a controller **are decided by more than one party**
- The assessment of joint controllership should be carried out on a **factual, rather than a formal, analysis of the actual influence** on the purposes and means of the processing.

Joint controllers

- Joint participation can take the form of:
 - a **common decision** taken by two or more entities
 - or **result from converging decisions** by two or more entities regarding the purposes and essential means
- Decisions can be considered as converging on purposes and means if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing.
- As such, an important criterion to identify converging decisions in this context is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.

joint controllership


determine their respective responsibilities in a transparent way



possibly by means of an arrangement



the essence of the arrangement shall be made available to the data subject



the arrangement may designate a contact point for data subjects

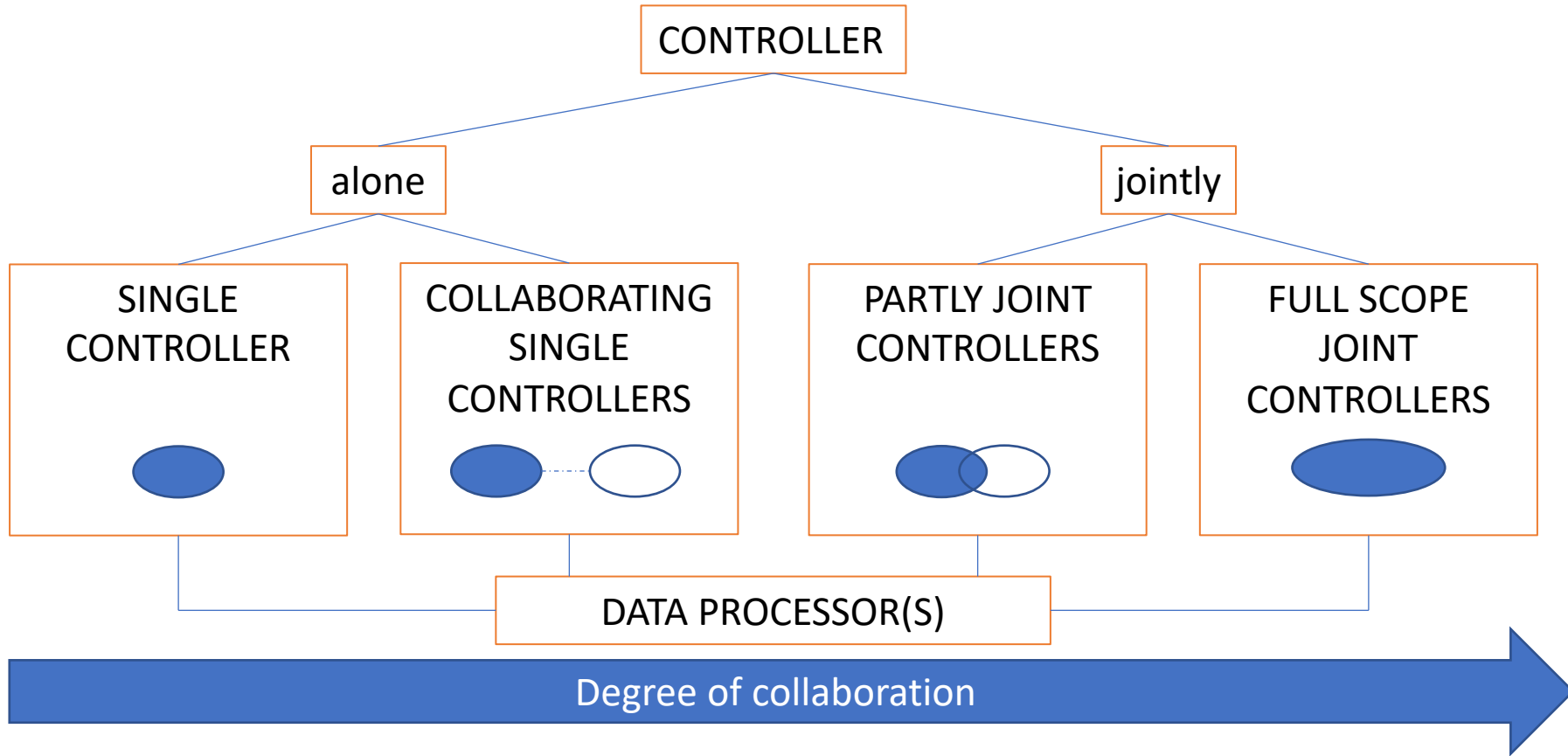


the data subject may exercise his/her rights against each controllers, irrespective of the terms of the arrangement



In practice

The typology of Olsen and Mahler





2. Processor

Who is the **processor**?

GDPR, Article 4 – *Definitions*

«For the purposes of this Regulation:

(8) ‘processor’ means a natural or legal person, public authority, agency or other body **which processes personal data on behalf of the controller**»

Two basic conditions for qualifying as processor are:

(a) being a separate entity in relation to the controller

(b) processing personal data on the controller’s behalf

Controller and Processor

(a) natural or legal person, public authority, agency or other body

(b) which determines

(c) alone or jointly with others

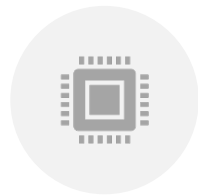
(d) purposes and means

(e) of the processing of personal data

(a) being a separate entity in relation to the controller

(b) processing personal data on the controller's behalf

CONTROLLER / PROCESSOR



the processor **must** act only on the controller's instruction (***bound by instruction***)



a ***contract or other legal act binding*** the processor to the controller **must** be in place



the controller has a ***due diligence obligation*** in the choice of the processor



the controller has to ascertain whether the processor provides **sufficient guarantees** in respect of the technical and organizational measure (***vetting***)



the processor could **document the appropriateness of its practice** with reference to one or more external standards (***standards, code and certificate***)



the contract must stipulate that the processor makes available to the controller all the information to demonstrate compliance with the GDPR and contribute to the audit, including inspections (***oversight***)

PRELIMINARY QUESTIONS

What kind of **burden**?



What kind of **object**?



What kind of **consequence**?

CONTROLLERS & PROCESSORS

Relevant provisions	Controller	Processor
Principles	✓	✗
Lawfulness of processing	✓	✗
Special categories of data	✓	✗
Transparency and modalities	✓	✗
Data Subject Rights	✓	Duty to assist
...		



3. Security Duties

Premise

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons,



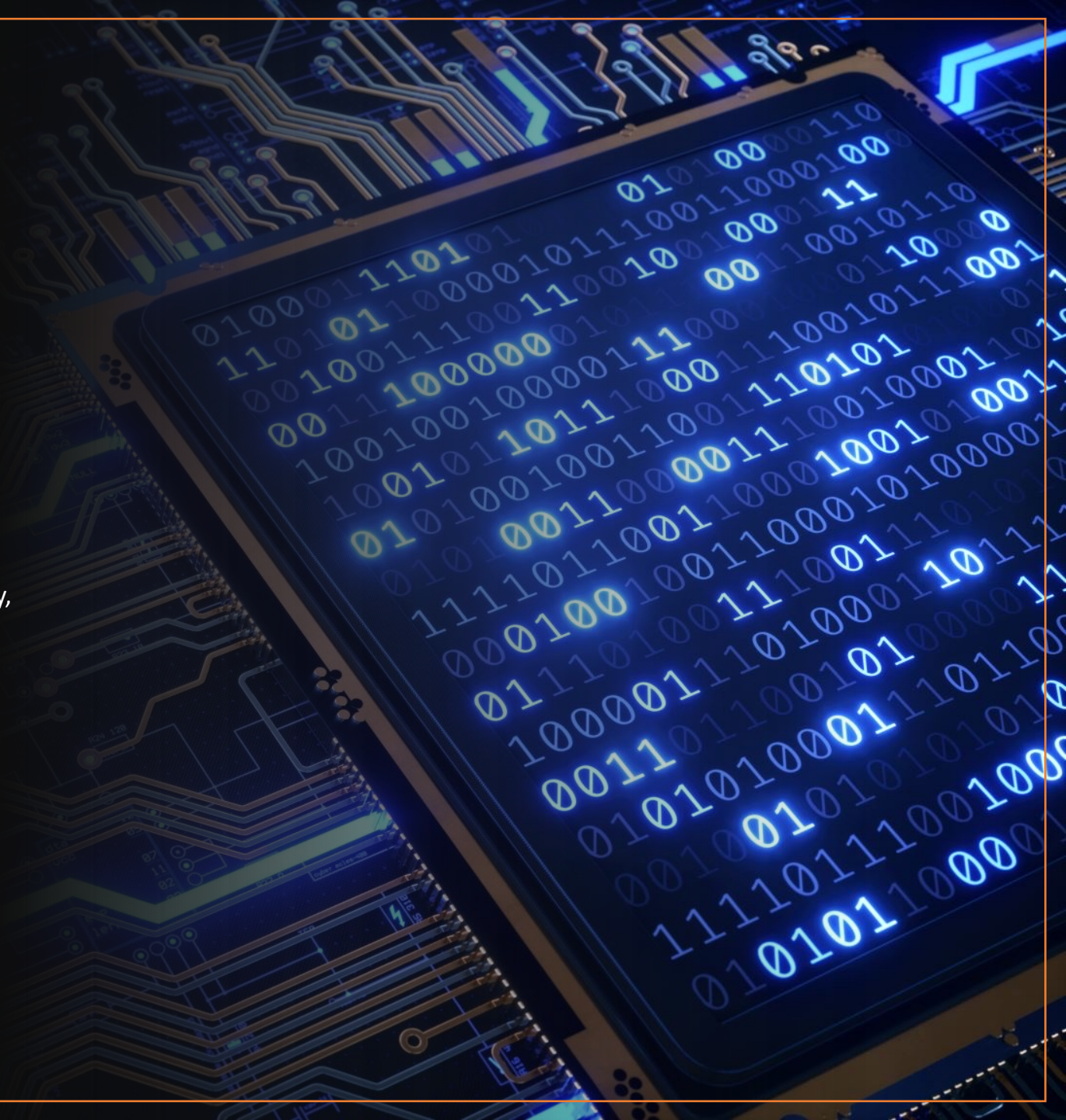
The controller



- shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.
- shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

the controller and the processor

- the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - the pseudonymisation and encryption of personal data;
 - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing



Problem solving

Due to the pandemic crisis, GreatCompany Corporation launched a new corporate welfare program for all its employees. To benefit of the program, you have to download the app of a new business partner, WeCare Inc. Once register and obtain your personal account, you have to enter all the data concerning your health and wellbeing, and the app will provide you a series of target discounts for medical visits and exam.

Considering the categories of data at issues, what are the problematic aspects of this policy?