

How to deal with Research Data

4th Taskforce GDPR Meeting, GÉANT,
Barcelona, April 23 2018

Marlon Domingus, CIPP/e, CIPM,
DPO Erasmus University Rotterdam



Itinerary

1. Privacy in the Context of Academic Research
2. Open Science/ F.A.I.R. / Privacy/ Intellectual Property Rights

Privacy in the Context of Academic Research

4th Taskforce GDPR Meeting, GÉANT,
Barcelona, April 23 2018

Marlon Domingus, CIPP/e, CIPM,
DPO Erasmus University Rotterdam



Safeguarding Privacy - Why



Principles and elaborations

1. Honesty and scrupulousness

Principle

Academic practitioners are honest and forthright about their research and its applications. Scientific and scholarly activities are performed scrupulously and should remain unaffected by the pressure to achieve.

Elaboration

- 1.1. Academic practitioners know that the ultimate aim of science is to establish facts and they therefore must present the nature and scope of their results with the greatest possible precision. Accordingly, they do not prevaricate about their findings or about attendant uncertainties. Scrupulousness also entails the presentation of doubts and contraindications.
- 1.2. Every academic practitioner demonstrates respect for the people and animals involved in scientific teaching and research. Research on human subjects is exclusively permitted if the persons concerned have freely given informed consent, the risks are minimal and their privacy is sufficiently safeguarded. Research involving animals is only permitted if the statutory permits have been granted and in conformity with the relevant legislation.

* The Netherlands Code of Conduct for Academic Practice 2004 (version 2014). Online available at: <http://vsnu.nl/files/documenten/Domeinen/Onderzoek/The%20Netherlands%20Code%20of%20Conduct%20for%20Ac>

Safeguarding Privacy - Why

- (75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

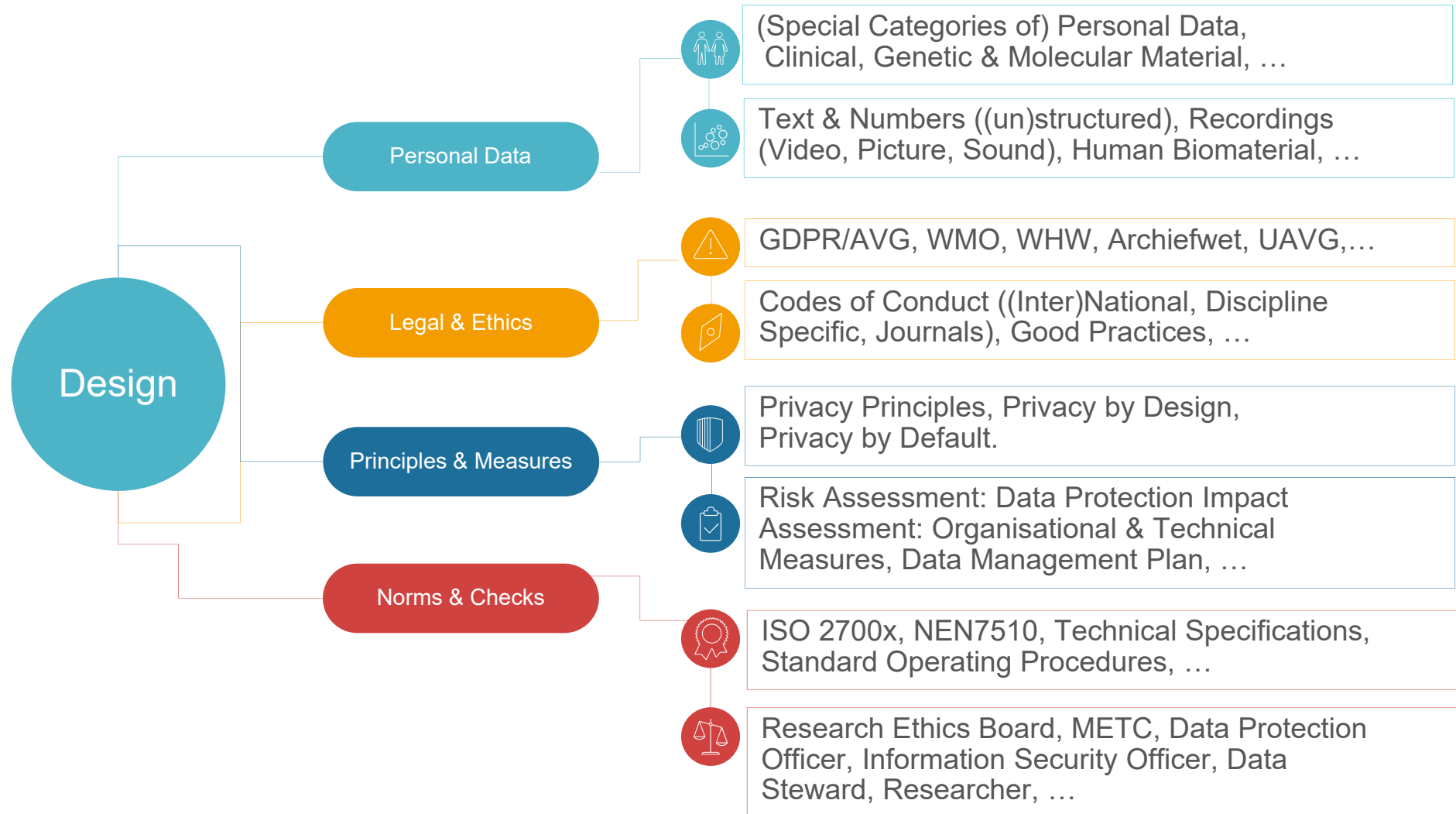
* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

GDPR Readiness

	unaware	aware
unable	<p>GDPR?</p>	<p><i>"I safeguard privacy in research, given my research tradition, culture and codes - but is it compliant to the GDPR?"</i></p>
able	<p><i>"I know I have to do stuff because of the GDPR - provide me the checklist"</i></p>	<p><i>"The GDPR is not so different from the Wet Bescherming Persoonsgegevens - we had our GDPR compliant milestone party last September"</i></p>



Safeguarding Privacy in Research Design - a Dutch Perspective



The General Data Protection Regulation (GDPR)

see: <https://teachprivacy.com/training-gdpr-whiteboard-interactive/>

The Implementation of the GDPR

1. Strategy

-Vision/ Mission * *Why (30 sec.), scope, legal challenges, requirements*

-Strategy * *Stakeholders (internal/ external), key functions, interface + workshop(multi-stakeholder),*

Datagovernance: --Collection-----Authorized Use-----Access-----Security-----Destruction--

* *Governance model, organizational model, measurement professional competence*

-Privacy Team

2. Framework

-Goal?

-Policies/ standards/ guidelines

o Business Case;

i. privacy team (skills etc.), internal policy compliance, inventory

ii. definition; baseline, domains

iii. laws and regulations; penalties, scope

iv. technical and physical controls

v. organizations

vi. industry frameworks

vii. PET

viii. innovation

ix. education and awareness

x. assurance

o GAP analysis

o Review process and monitoring

3. Performance Measurement

-*Metric lifecycle;*

identify audience (who uses the data?)

define reporting resources (who owns and why?)

select privacy metrics (what?)

collect systems (where, when, why?)

analyze data (value, feedback quality)

Asses

Privacy Maturity Model

Privacy by Design

Data, systems, process

i. Audit, risk mngt

ii. IT

iii. IS

iv. Human resources/ Ethics

v. Legal compliance

vi. Processors and 3rd party

vii. Marketing/ business development

viii. Finance/ business controls

Privacy operational lifecycle

Respond

Information requests

Legal compliancy

Incident planning

Incident handling

Progress reporting

Response evaluation and modifications

Protect

Data Life Cycle mngt.

IS Practices

Privacy by design

Conduct Analysis and Assessments

Sustain

Monitor

Audit

Communication

Privacy in the Context of Academic Research

4th Taskforce GDPR Meeting, GÉANT,
Barcelona, April 23 2018

Marlon Domingus, CIPP/e, CIPM,
DPO Erasmus University Rotterdam



The GDPR - Personal Data



PERSONAL DATA



Identified

Identifiable

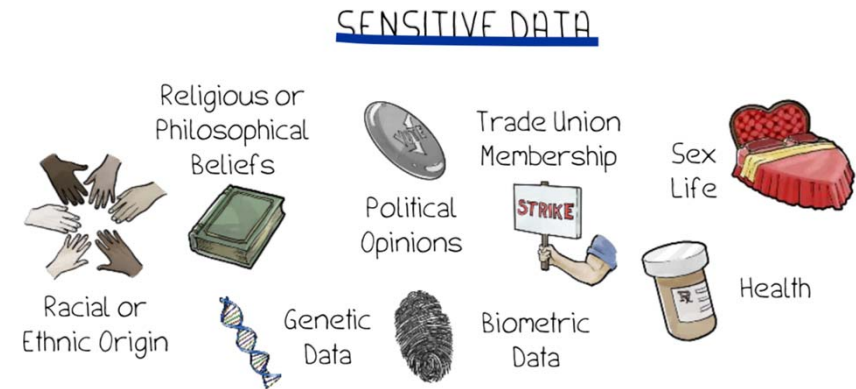
"Personal Data" (GDPR*, Article 4):

Any information relating to an identified or identifiable natural person:

a name, an identification number, location data, an online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

The GDPR - Special Categories of Personal Data



"Special Categories of Personal Data (Sensitive Data)" (GDPR, Article 9):

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

EU General Data Protection Regulation

Responsibilities in Academia

Who

University: provide *necessary general conditions* to enable researchers to comply; policy, guidelines, infrastructure and skilled and available research support staff.

Dean: provide *additional necessary discipline specific conditions* to enable researchers to comply; policy, guidelines, infrastructure and skilled and available research support staff.

Faculty: follow privacy principles & use the provided privacy enabling conditions (policy, guidelines, infrastructure and skilled and available research support staff).

Privacy: Maturity Model

Capability Maturity Model for Safeguarding Privacy in Academic Research or: *The GDPR* Readiness Levels*

Marlon Domingus, April 2017 version 0.3

	Level 1. Initial	Level 2. Repeatable	Level 3. Defined	Level 4. Managed	Level 5. Optimised
Across the university	<p>'What is this acronym: "GDPR" everyone is talking about?'</p> <p>'I'm afraid we have to do something related to this, but don't know what, why and how.'</p> <p>University appoints a <i>Data Protection Officer (DPO)</i>.</p>	<p>People across the university are meeting on a regular basis to share their practices, based on application of the <i>Privacy Impact Assessment (PIA)</i>. A common language and understanding emerges on how to safeguard the privacy of data subjects in the collection, processing and sharing of personal data.</p>	<p>A <i>standard data protection process</i> is defined and communicated, in which people in various roles have a responsibility for their part and/or the whole. Generic instruments are evaluated, selected and implemented. A shared vocabulary exists to understand each other whilst working on tailored solutions.</p>	<p>Typical research scenarios are fully supported, <i>GDPR</i> compliant, as a standard service. Ongoing evaluation is in place for improving the quality of the <i>GDPR</i> compliancy support. Tailored support is in place for specific (new / complex) aspects in research scenarios.</p>	<p><i>GDPR</i> is considered a starting point for the University to develop its own distinctive position. This position is <i>above par</i> and reflected in the University's policy, guidelines, principles of ethics committees, and as such recognisable both in research and research support.</p>
Faculty	<p>Faculty dealing with sensitive data have a heterogeneous understanding of <i>privacy</i> and <i>data protection</i>.</p> <p>What appropriate behaviour is, is a matter of opinions. In general 'privacy' is considered relevant, but a black box.</p>	<p>Faculty are discussing data protection practices from within their discipline.</p> <p>Faculty develop a strategy (with or without central support) to comply to various (external) data protection requirements by, e.g. research funders.</p>	<p>Faculty are familiar with what is expected of them in terms of safe-guarding the privacy of their data subjects, and have access to tooling and support to do so, in their administrative tasks and teaching capacities.</p> <p>Solutions for generic research scenarios are available for faculty.</p>	<p>Faculty routinely design their research in terms of <i>PBD</i> and have access to a library of relevant and tailored documents to support them. Privacy is no longer considered an <i>external threat</i>, or burden, but the obvious way to be transparent on how to treat the rights of data subjects / citizens.</p>	<p><i>GDPR</i> is considered the baseline from a research professionalism perspective. Privacy is seen as an <i>important strength</i>. By ensuring <i>trust</i> in transparent and responsible research, privacy is an enabler of societal relevance and impact of research..</p> <p>Regular checks are built in, to check what to improve and how.</p>
Legal	<p>Legal staff is getting acquainted with the <i>GDPR</i>. Examining the rights, responsibilities, roles and responsibilities.</p> <p>Discussing available relevant (best and worst) practices.</p>	<p>Relevant examples, practices, instruments and relevant legal expertise are combined. Templates and model provisions are drafted to cover the relevant area.</p> <p>The first <i>Register</i> draft is created. <i>PIA</i> strategies are explored.</p>	<p>All <i>GDPR</i> concepts, rights and roles are clear, defined and documented in the context of academic research.</p> <p>Legal staff pro actively contribute to research support with <i>Privacy By Design and by Default (PBD)</i> implementations.</p>	<p>All roles, instruments, contracts and template wordings are in place for <i>GDPR</i> compliant support in various research scenarios. Legal staff act as embedded research supporters, in cooperation with the <i>DPO</i> and the ethical committee(s).</p>	<p>Legal staff is actively involved in privacy impact assessments of (1) new innovative tooling and instruments and (2) innovative forms of cooperation in research, to assess the responsible application for research purposes.</p>
CIO	<p>Privacy is discussed in the context of governance and e-strategy. Privacy principles are discussed in the context of Higher Education Reference Architecture.</p>	<p>Privacy is included in the Business Function Model, Information Model, Business Process Model, Application Model & Platform. A privacy policy is drafted.</p>	<p>A privacy policy enters into force. Guidelines are distributed. An updated information security policy is implemented. CIO designs <i>PBD</i> strategies.</p>	<p>All relevant <i>GDPR</i> aspects are addressed in the privacy-, information security policy and governance.</p> <p>CIO appoints privacy officers in collaboration with Legal.</p>	<p>CIO is at all times willing and able to demonstrate the <i>GDPR</i> compliancy of information processing within the university. Checks and balances are in place to stimulate responsible behaviour.</p>
IT	<p>Privacy is typically approached from a information security point of view. Typically public cloud tooling is banned, usually with no alternative available. Many opinions on what is relevant and required.</p>	<p>Relevant <i>Privacy Enhancing Technologies (PETS)</i> are explored and tested in pilots with faculty. IT recognises the validity of research as a target group, distinct from support for education and business operations.</p>	<p>A chain of <i>PETS</i> is implemented as basic services for research.</p> <p>Selection and prioritisation in collaboration with Faculty, Legal and CIO.</p>	<p>The baseline <i>PETS</i> are embedded in the working environment of researchers and supported (both individually and in workshops for faculty).</p>	<p>Support for the whole research life cycle for both open science and closed science is available as self service from the IT service catalogue. A process is in place to design, implement and steward tailored <i>PET</i> solutions.</p>



See: <https://creativecommons.org/licenses/by-nc/4.0/legalcode>

* See for EU General Data Protection Regulation (GDPR): <http://www.privacy-regulation.eu/en/index.htm>

Privacy in the Context of Academic Research

4th Taskforce GDPR Meeting, GÉANT,
Barcelona, April 23 2018

Marlon Domingus, CIPP/e, CIPM,
DPO Erasmus University Rotterdam



Balancing the legitimate interests of the researcher and the privacy rights of the individual

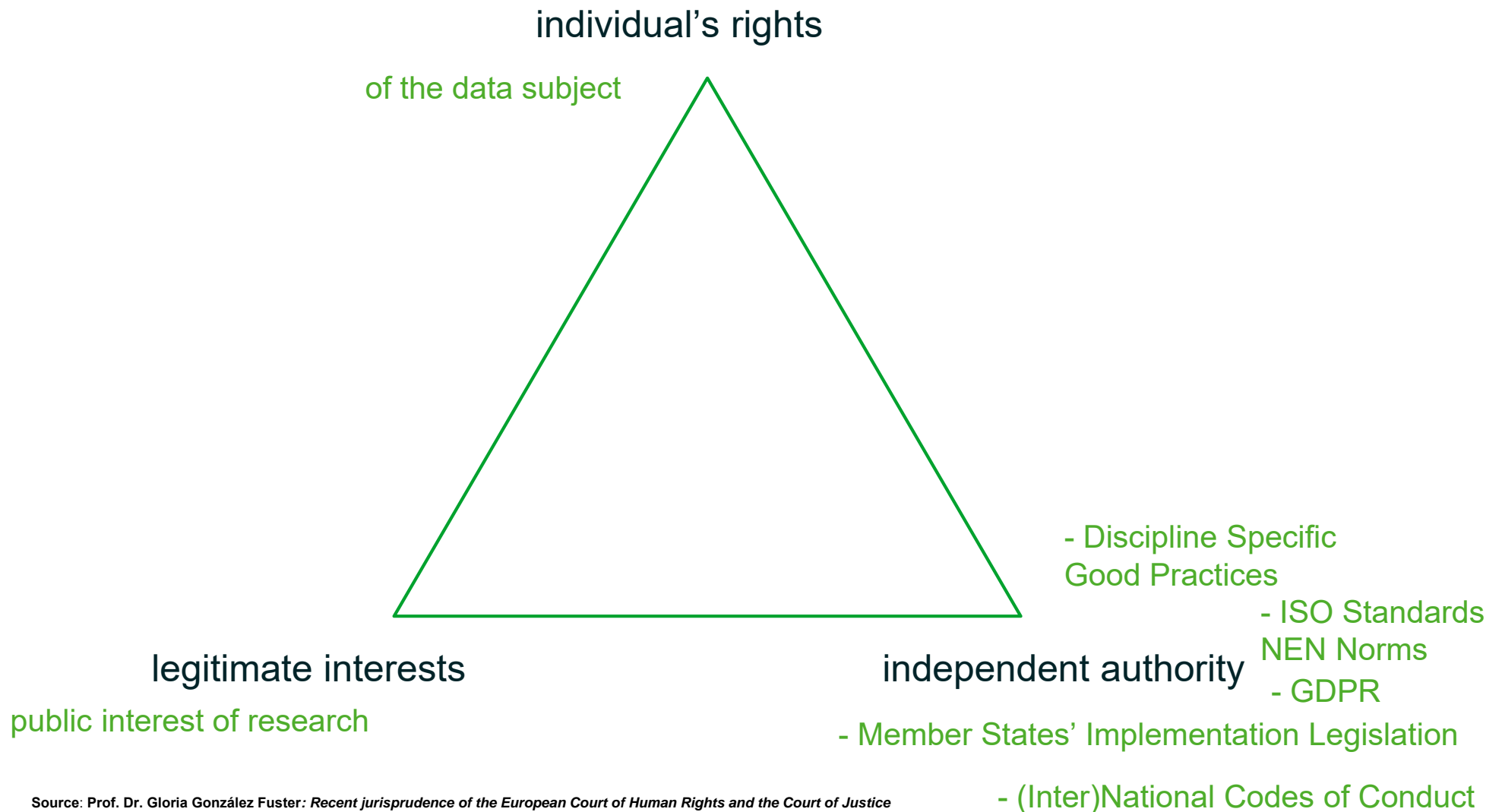
“The right to the protection of personal data is **not an absolute right**; it must be considered in relation to its function in society and be **balanced** against other fundamental rights, in accordance with the **principle of proportionality**.”

Recital (4) GDPR

“processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject [...]”

Article 6(1)f GDPR

Balancing the legitimate interests of research and the privacy rights of the individual



Balancing: Four Steps

1. Legitimate interests of controller or 3rd party

- freedom of expression
- direct marketing and other forms of advertisement
- enforcement of legal claims
- prevention of fraud, misuse of services, or money laundering
- physical safety, security, IT and network security
- whistle-blowing schemes

2. Impact on data subject

Actual and potential repercussions

- Nature of the data
- How the data are processed
- Reasonable expectations data subject
- Nature of controller vis-à-vis data subject

3. Make provisional balance

“Necessary”

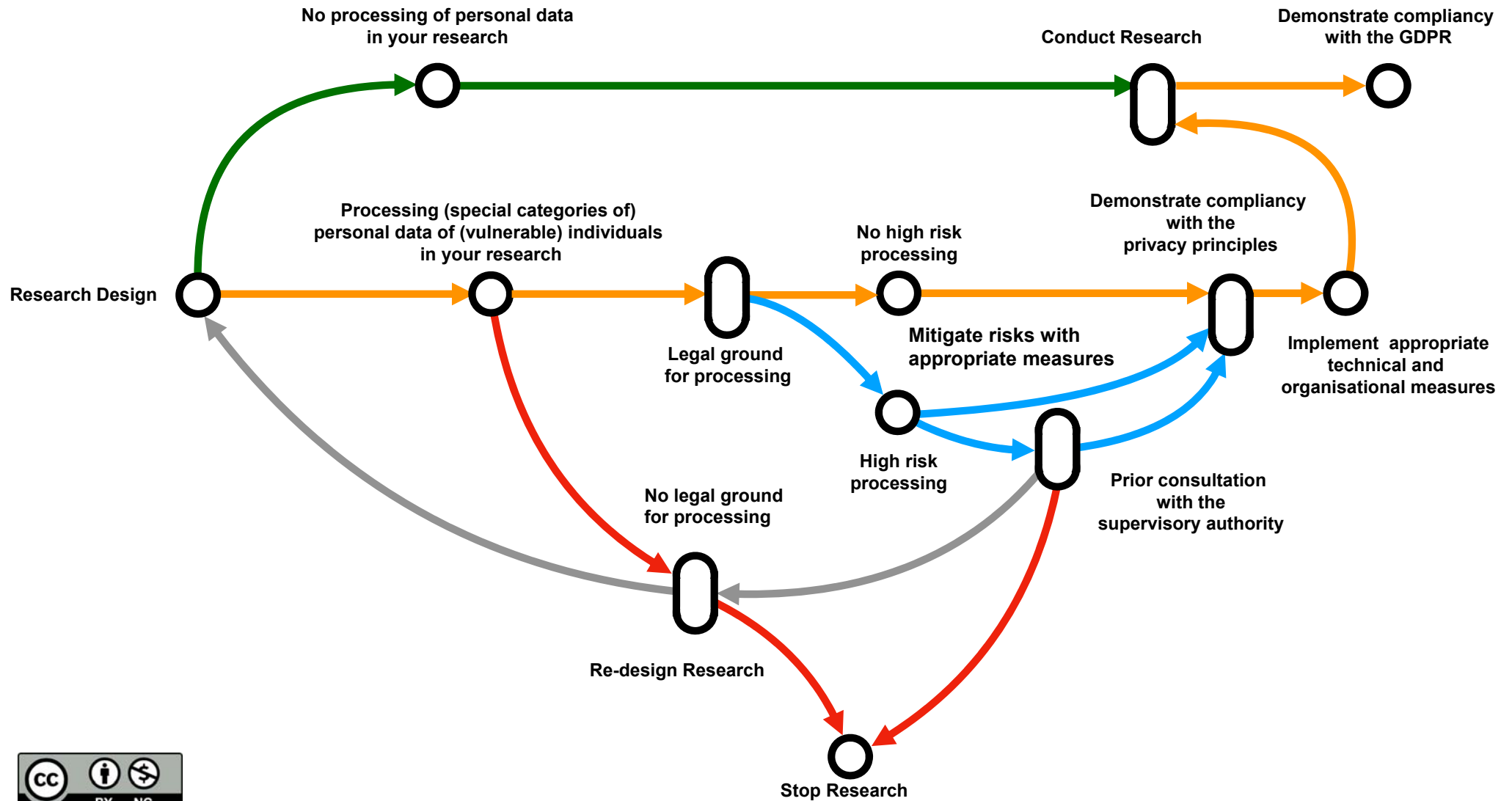
- Least intrusive means
- Reasonably effective
- Balance of interests

4. Safeguards

Measures to ensure that the data cannot be used to take decisions or other actions with regard to individuals.

- anonymisation techniques, aggregation of data
- privacy-enhancing technologies, privacy by design
- increased transparency
- general and unconditional right to opt-out

The Privacy Impact Assessment (PIA) Route Planner for Academic Research Inspired by Harry Beck's London Metro Map



The Logic of a Privacy Impact Assessment (PIA) for Academic Research

Q1. Do you process (special categories of) personal data of (vulnerable) individuals in your research?



YES →

NO
Proceed - no measures required for safeguarding privacy.

"Personal Data" (GDPR*, Article 4):

Any information relating to an identified or identifiable natural person: a name, an identification number, location data, an online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Special Categories of Personal Data (Sensitive Data)" (GDPR, Article 9):

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Action ←

Records of processing activities (GDPR*, Article 30):

The university shall maintain a digital record of the processing activities in your research to demonstrate compliance to the GDPR. This register contains:

1. The name and contact details of the researcher, the research partners and service providers;
2. The purposes of the processing;
3. A description of the categories of data subjects and of the categories of personal data;
4. The categories of recipients to whom the data have been or will be



Q2. What is the legal ground for this processing?

Lawfulness of Processing (GDPR*, Article 6, 89):

1. The individuals participating in your research have freely given their explicit consent for one or more specific purposes.
2. Your research contributes to a legitimate interest, yet results in no high risks for the individuals participating in the research.
3. Your research has a scientific, historical or statistical purpose, yet results in no high risks for the individuals participating in the research.

Action ←

Data protection by design and by default (GDPR*, Article 25):

Implement appropriate technical and organisational measures:

1. **Individual participating in your research (data subject).** Is the participant well informed, aware of possible risks for her/him and aware of the purpose of the research?
2. **Data.** Is the data de-identified and encrypted?
3. **Access Management.** How is access managed and controlled for the PI / team (expanded) / public?
4. **Software / Platform.** Are the *Terms of Service* for used software / platform checked (where is the data and who has access and has which usage rights)?
5. **Devices.** Are devices used safe? Encrypted drive, encrypted communication, strong password / two factor authentication.
6. **Partners.** Are the research partners / service partners trusted and are appropriate legal agreements made, with regards to roles, rights and responsibilities?
7. **Safe and secure collaboration.** Is the ((cross border) communication to, in and from the) collaboration platform end to end encrypted, are roles and permissions defined and implemented, is logging and monitoring implemented?

YES →

NO
Stop research or redefine research.

Q3. Is this processing a high risk processing?

Criteria for high risk processing (WP29 - DPIA Guideline):**

1. Evaluation or scoring
2. Automated-decision making with legal or similar significant effect
3. Systematic monitoring
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. When the processing itself prevents data subjects from exercising a right or using a service or a contract

YES

NO
Proceed - measures required for safeguarding privacy.

Action ←

Prior consultation (GDPR*, Article 36):

1. The Data Protection Officer shall, on behalf of the researcher, consult the supervisory authority, prior to the processing (the research) when the processing would result in a high risk *in the absence of measures* to mitigate the risk.

Action ←

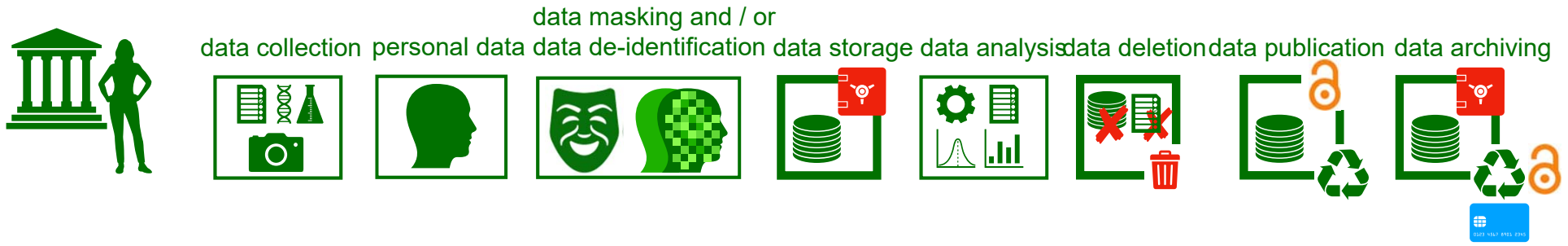
Principles relating to processing of personal data (GDPR*, Article 5):

Demonstrate compliance with the principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability.

* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=do>

** Article 29 Data Protection Working Party: *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of I* Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017. Online available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Academic Research: Scales of Collaboration and Accompanying Appropriate Privacy Enhancing Measures



- (non)academic research project team members
- (non) academic peers
- service providers
- research funders
- journals

- devices (corporate owned, company enabled / corporate owned, personally enabled / personally owned, company enabled / personally owned, personally enabled)
- software (proprietary / public cloud / open source / own)
- services (proprietary / public cloud / open source / own)
- platforms (proprietary / public cloud / open source / own)

- demonstrate compliancy with regards to the General Data Protection Regulation
- demonstrate compliancy with regards to the GDPR privacy principles.
- assess the researcher's privacy awareness and privacy enhancing conduct
- provide awareness sessions and training fit for researcher's purposes
- provide policy, guidelines, tooling and support for researchers to stimulate privacy enhancing conduct

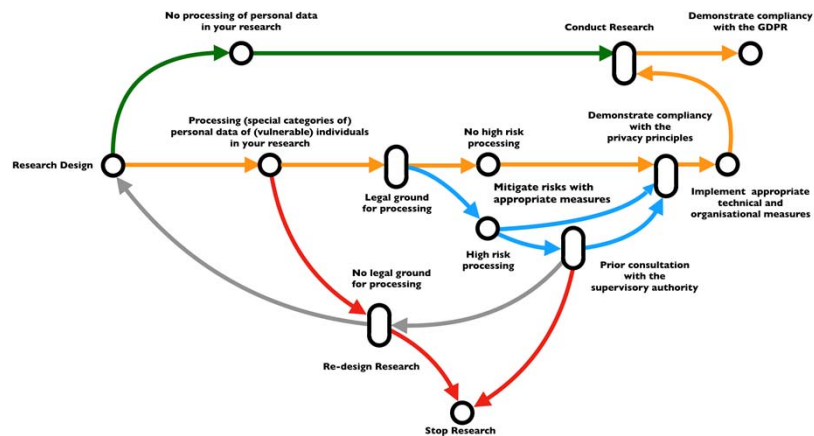
- **access** - who is allowed access to which data for which purpose for which period of time?
- **data** - access to: personal data, masked and/or de-identified data?
- **security standards** - which communication / storage is encrypted?
- **accountability** - who is responsible for which processing in which role?
- **governance** - who collects which metrics to check on responsible conduct and takes which agreed appropriate measures?

- **Terms of Service (TOS)** - have the TOS been analysed for legal and technical compliancy to relevant legislation (hard law and soft law) and which agreed actions are taken by whom in case of discrepancies?
- **data** - who has access to the research data for which purpose on the device / software / service / platform and is this compliant to agreements and legislation?

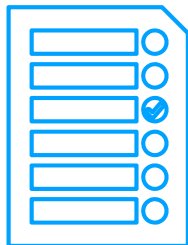
- **Data subject's privacy rights and freedoms** are placed central in the research project from the research design to the archiving of the research findings
- **Communication** on data subject's privacy rights is stated clearly in the university privacy statement, privacy policy and guidelines, as well as in the research project informed consent forms, data processing agreements, consortium agreement, ethical assessment, data management plan and data protection impact assessment

Privacy Before Research: Research Design Result: DMP & Legal Agreements

1 Privacy Risk Assessment

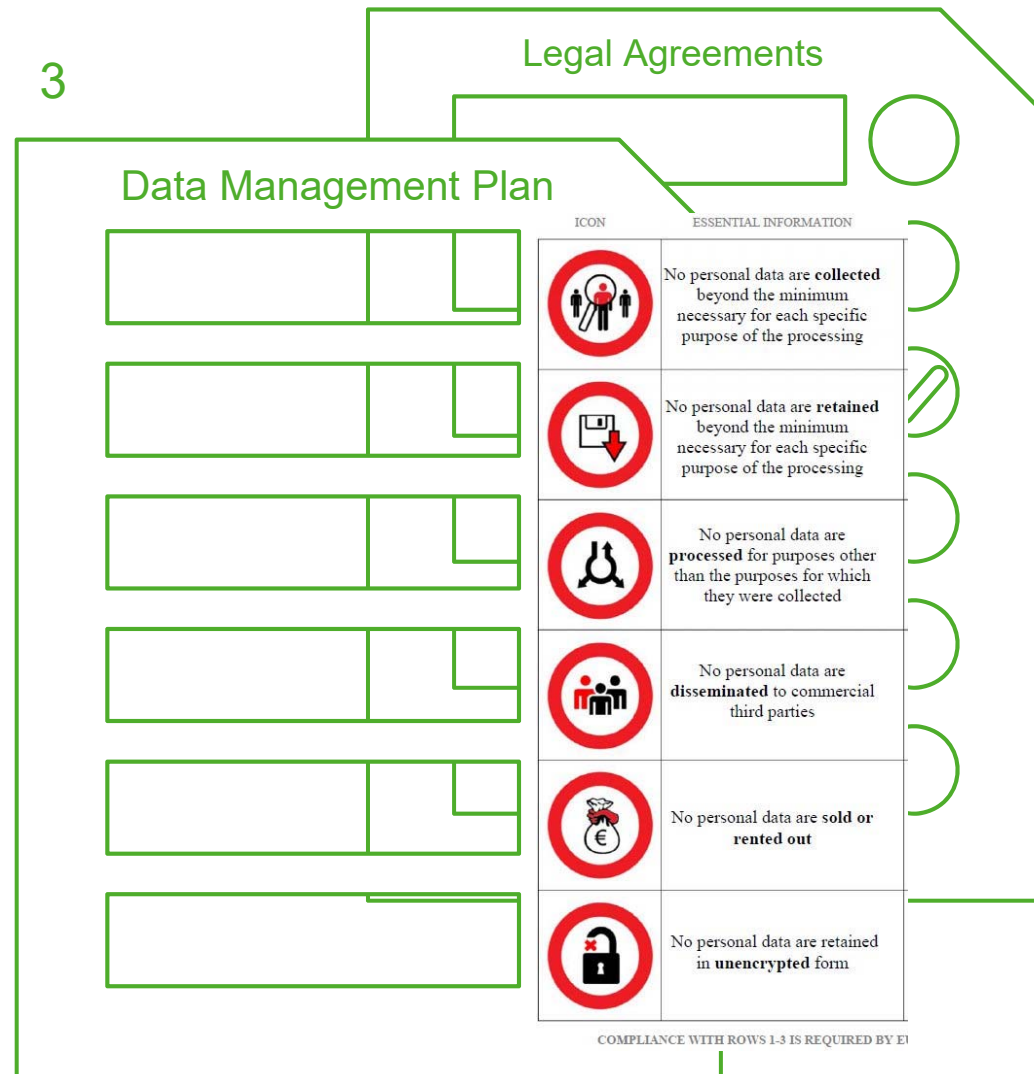


2



Risks, Appropriate Organisational and Technical Measures, Ethical Self Assessment

3



Privacy in the Context of Academic Research

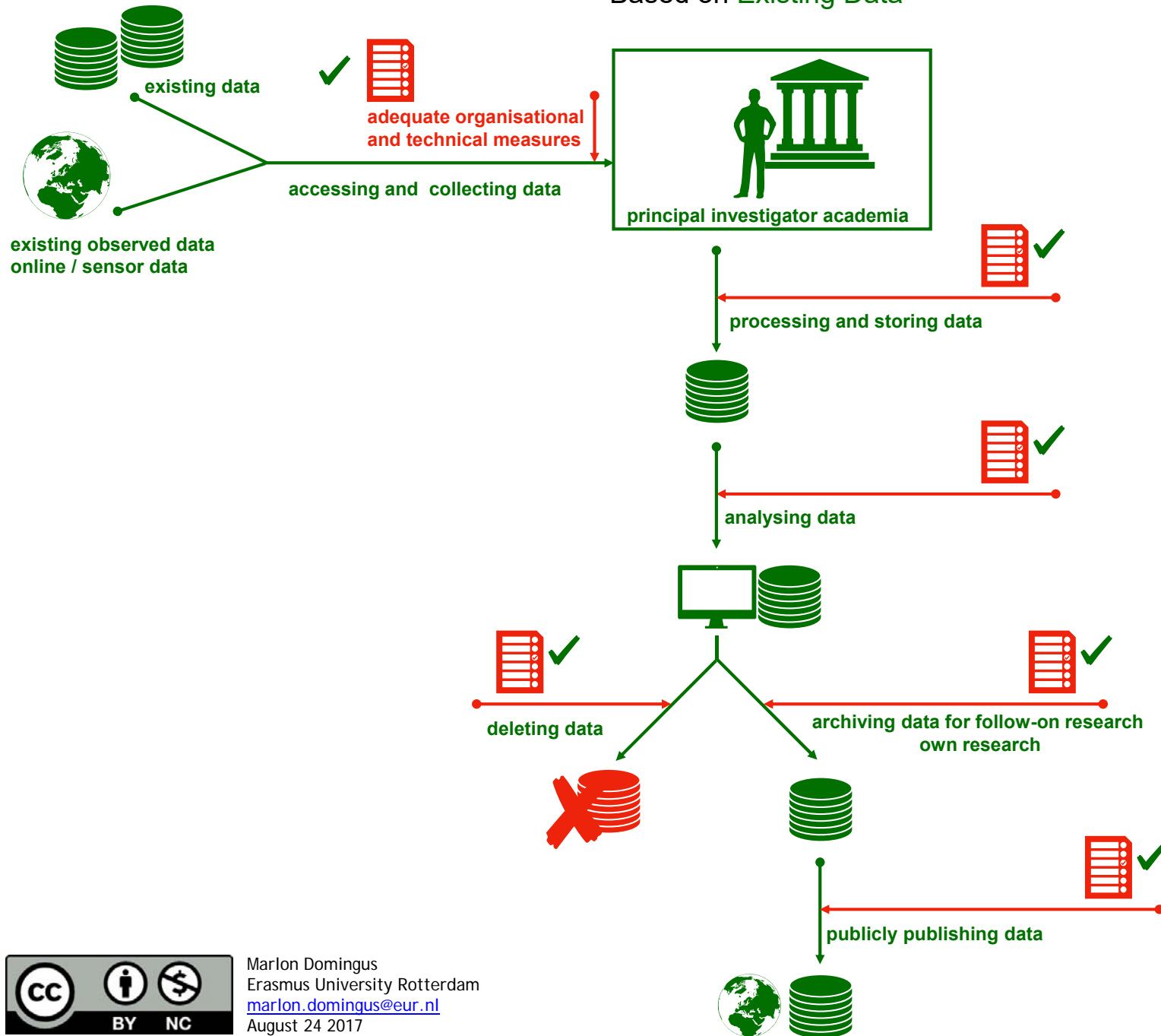
4th Taskforce GDPR Meeting, GÉANT,
Barcelona, April 23 2018

Marlon Domingus, CIPP/e, CIPM,
DPO Erasmus University Rotterdam



Research Scenarios and the General Data Protection Regulation:

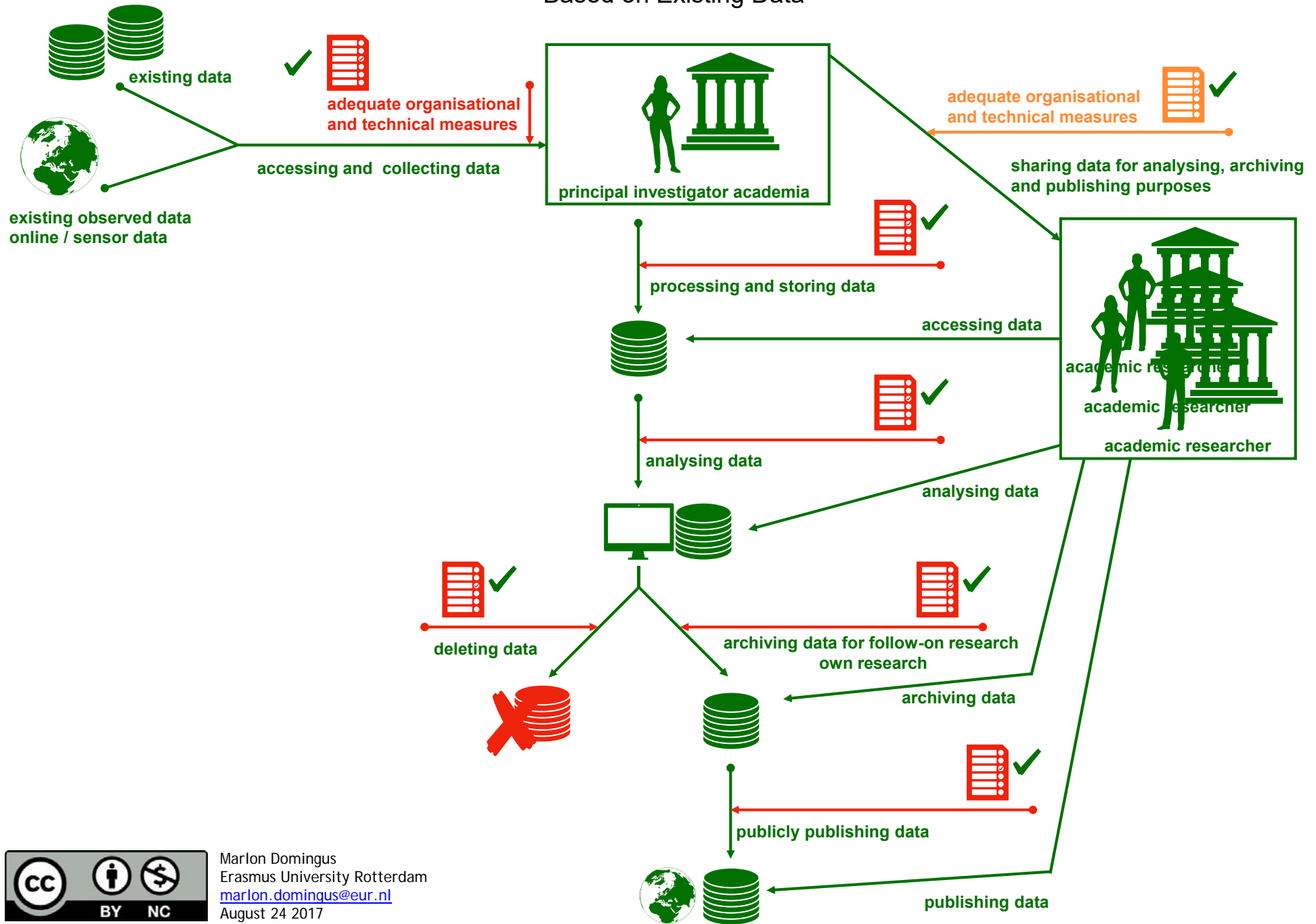
1. Individual Academic Research Based on Existing Data



Research Scenarios and the General Data Protection Regulation:

2. Academic Research by an International Research Group

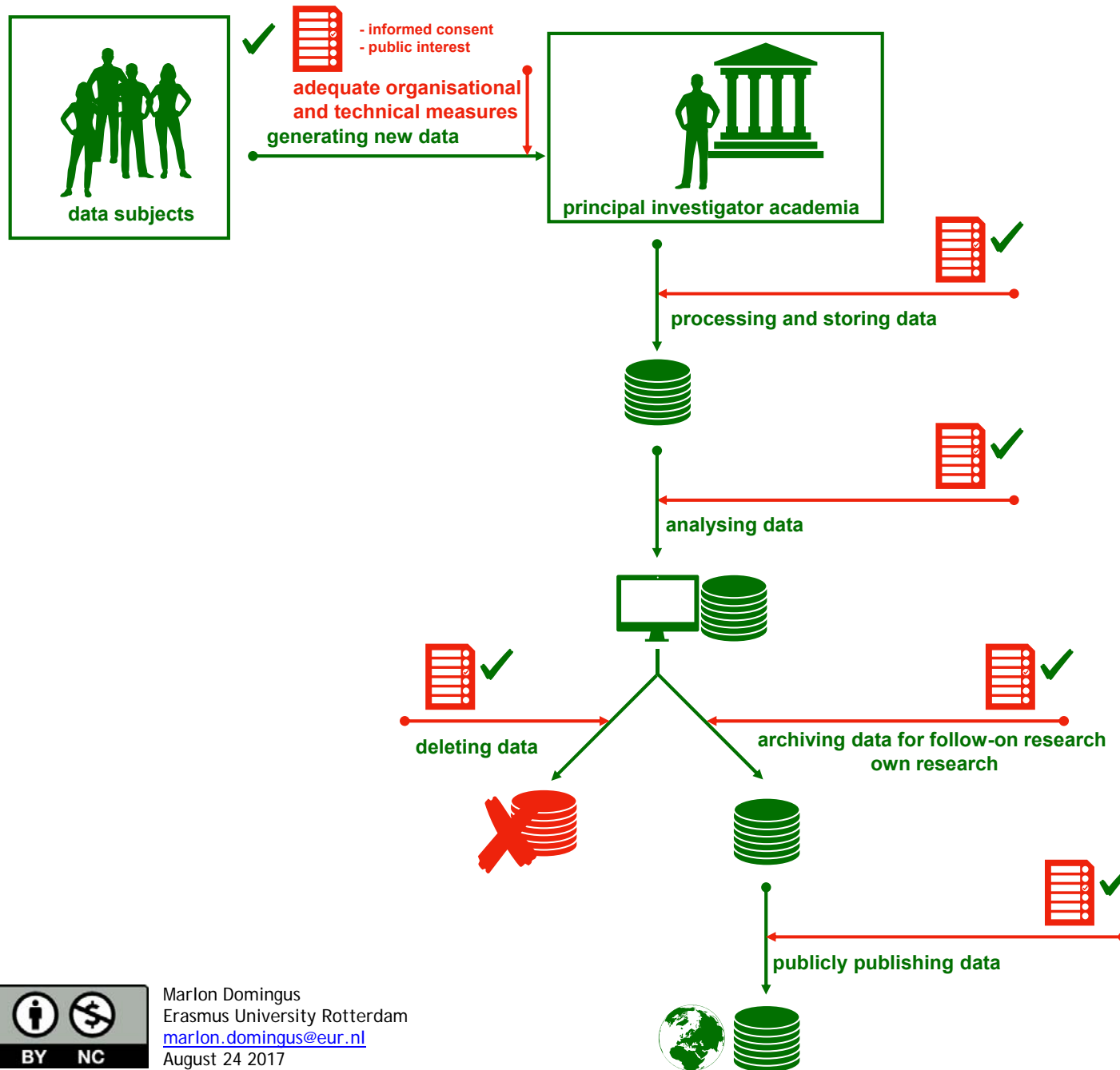
Based on Existing Data



Research Scenarios and the General Data Protection Regulation:

3. Individual Academic Research

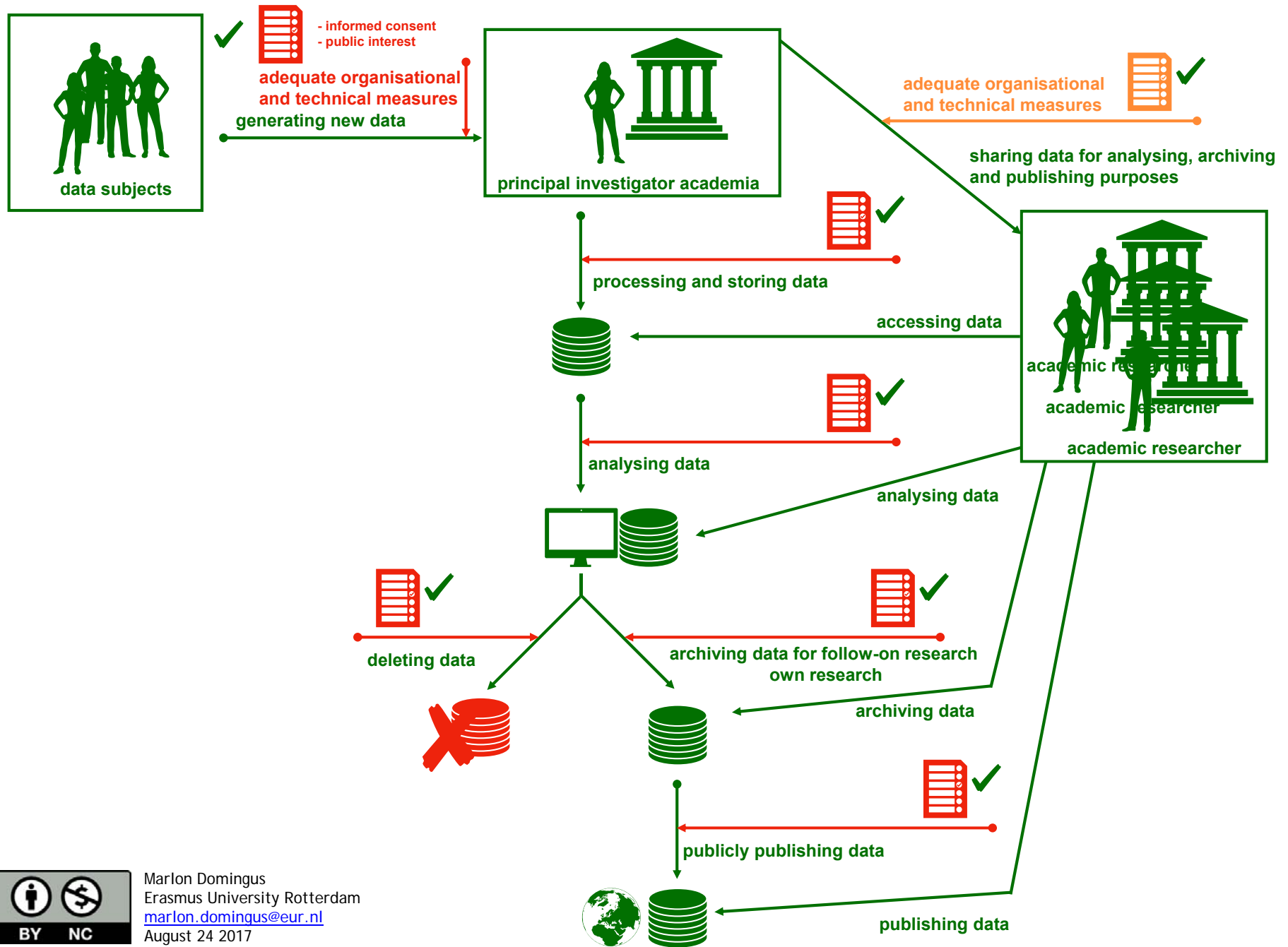
Based on **Generated Data from Data Subjects**



Research Scenarios and the General Data Protection Regulation:

4. Academic Research by an International Research Group

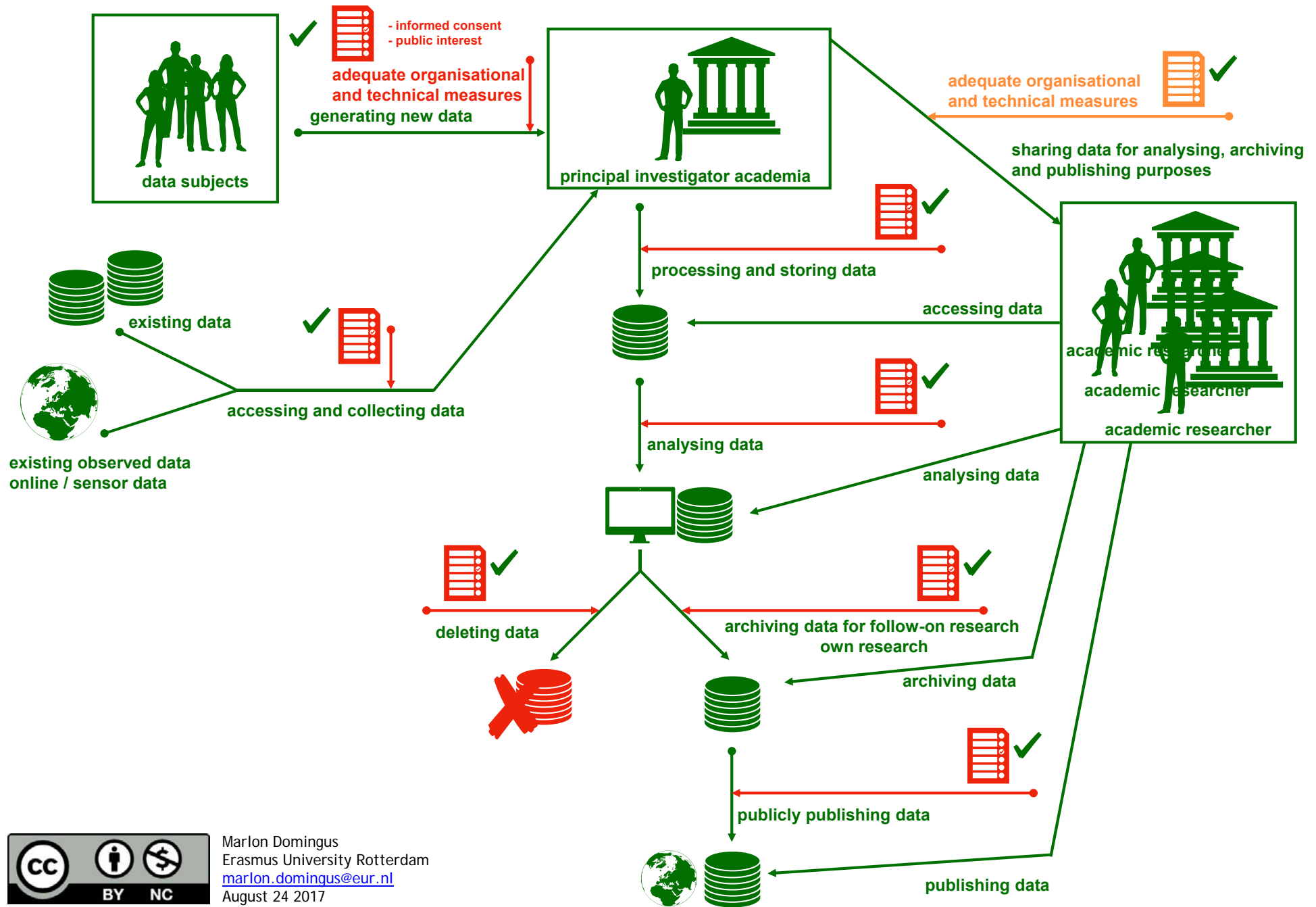
Based on Generated Data from Data Subjects



Research Scenarios and the General Data Protection Regulation:

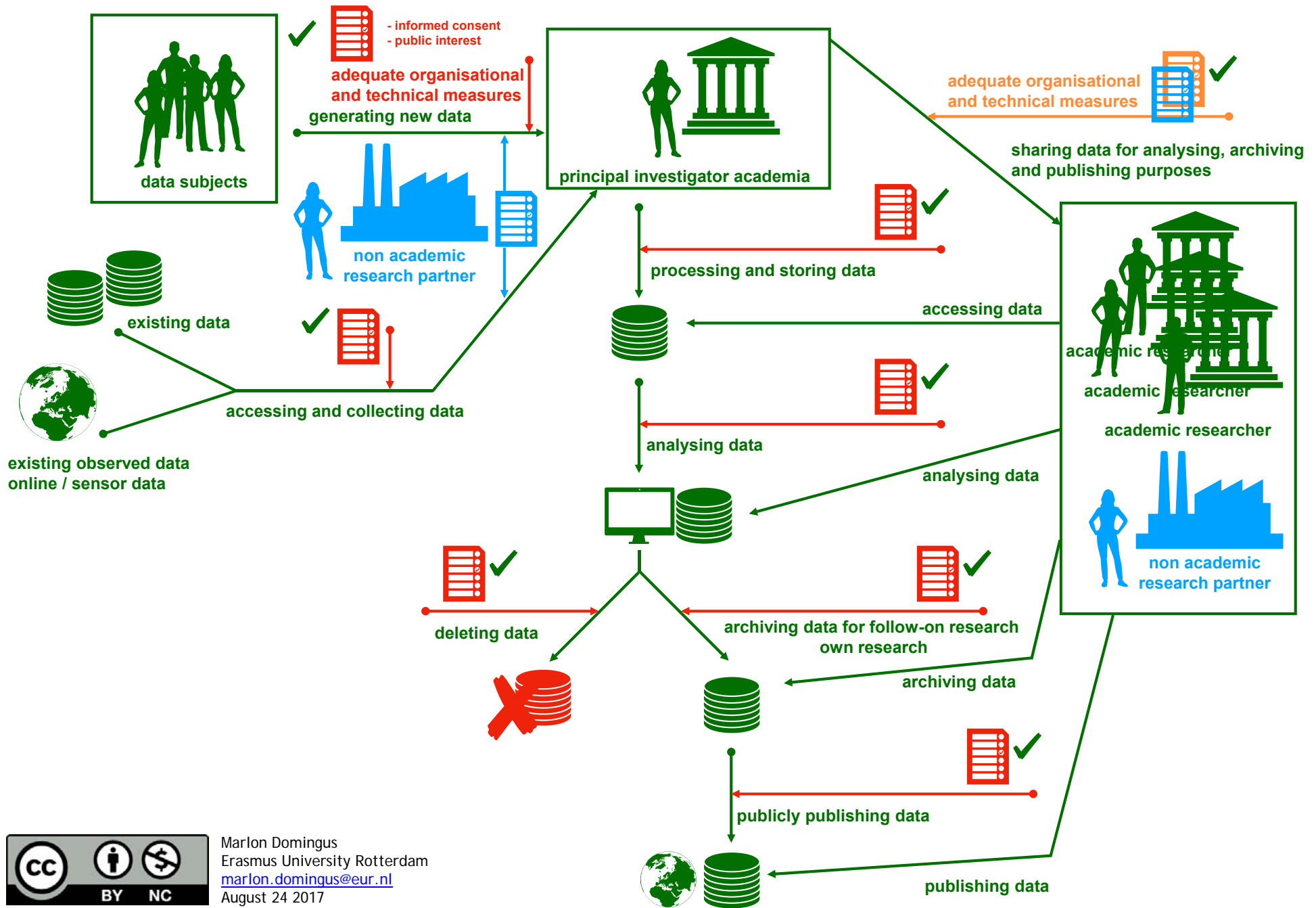
5. Academic Research by an International Research Group

Based on Generated Data from Data Subjects Combined With Existing Data



Research Scenarios and the General Data Protection Regulation:

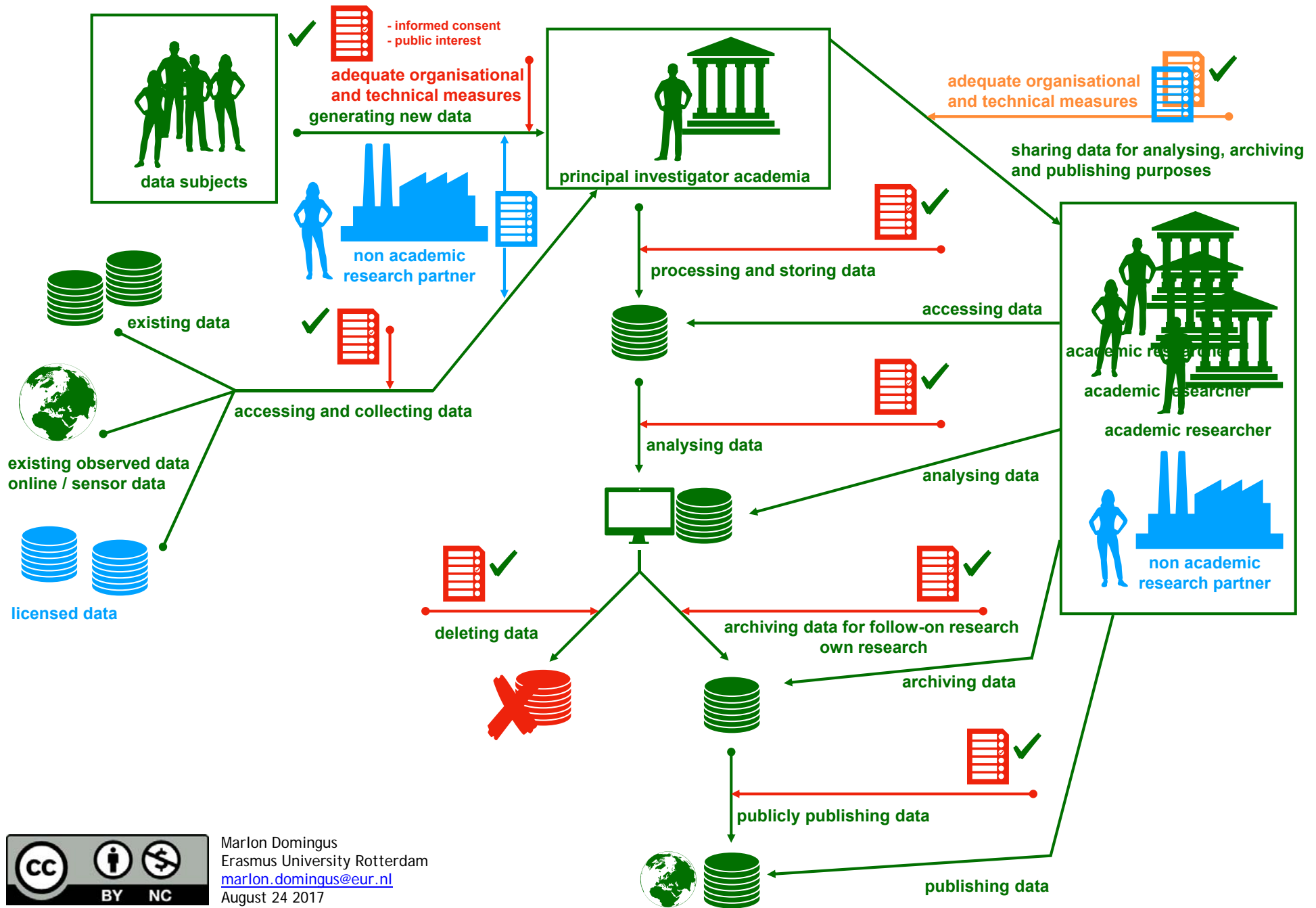
6. Academic Research by International Public - Private Research Group Based on Generated Data from Data Subjects Combined With Existing Data



Research Scenarios and the General Data Protection Regulation:

7. Academic Research by International Public - Private Research Group

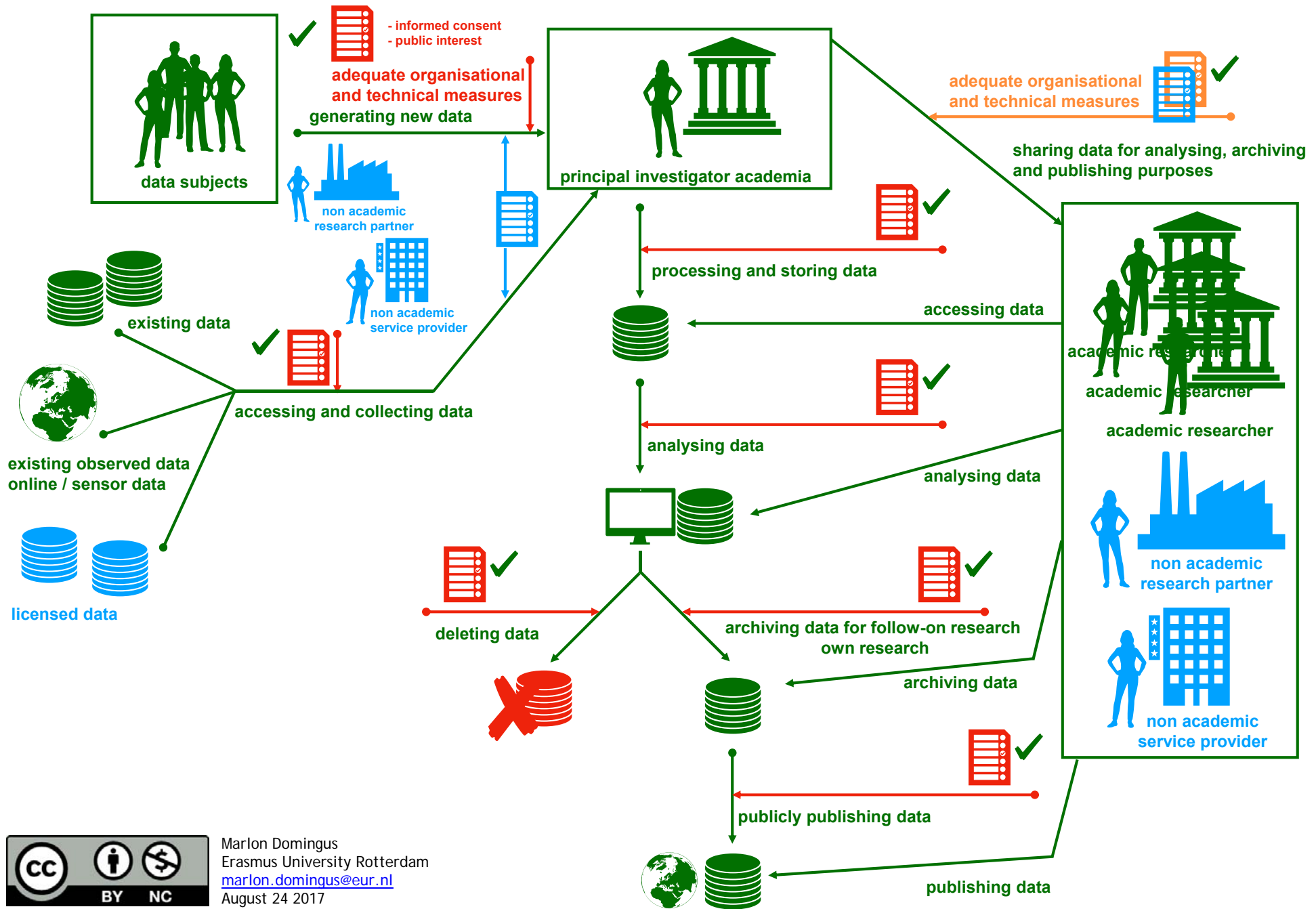
Based on Generated Data from Data Subjects Combined With Existing Data and Licensed Data



Research Scenarios and the General Data Protection Regulation:

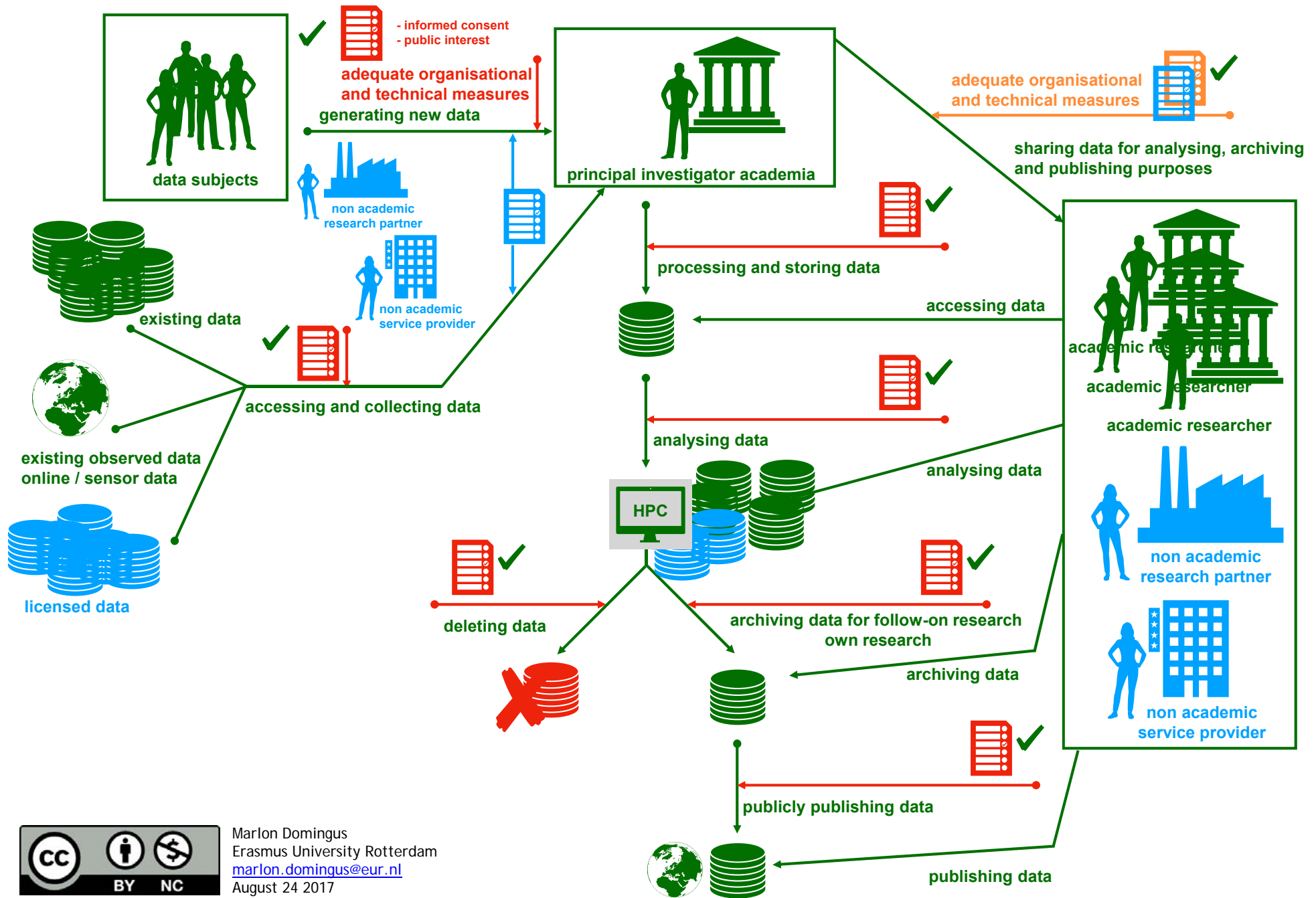
8. Academic Research by International Public - Private Research Group & Third Parties

Based on Generated Data from Data Subjects Combined With Existing Data and Commercial Data



Research Scenarios and the General Data Protection Regulation:

9. Academic Big Data Research by International Public - Private Research Group & Third Parties Based on Generated Data from Data Subjects Combined With Existing Data and Commercial Data



Open Science/ F.A.I.R. / Privacy/ Intellectual Property Rights

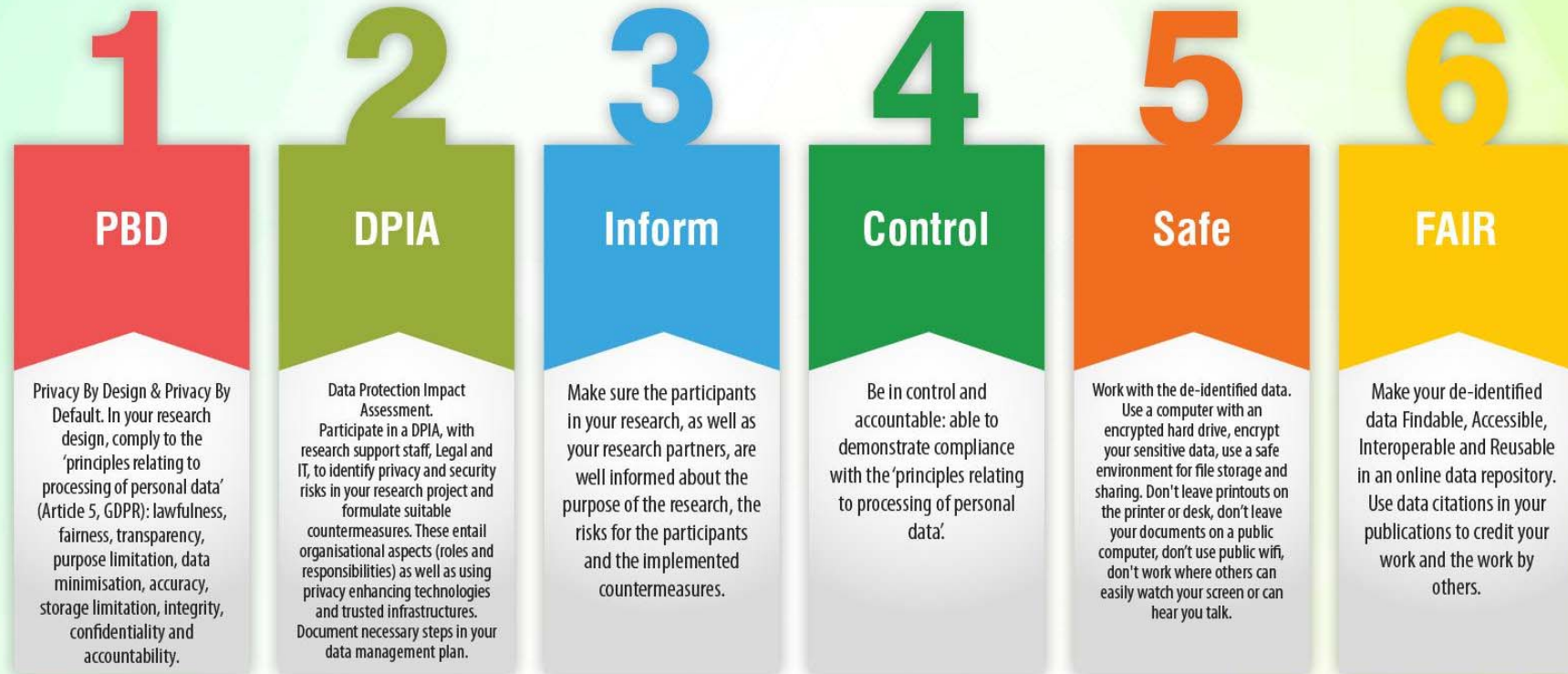
4th Taskforce GDPR Meeting, GÉANT,
Barcelona, April 23 2018

Marlon Domingus, CIPP/e, CIPM,
DPO Erasmus University Rotterdam



EU General Data Protection Regulation: Privacy Before, During and After Research

HOW TO TREAT PERSONAL DATA IN RESEARCH. RESPONSIBLE USE OF PERSONAL DATA BEFORE, DURING AND AFTER RESEARCH.



For More Information visit
www.gdprcoalition.ie

Twitter
[@GDPR_Coalition](https://twitter.com/GDPR_Coalition)

Linkedin
gdpr Coalition

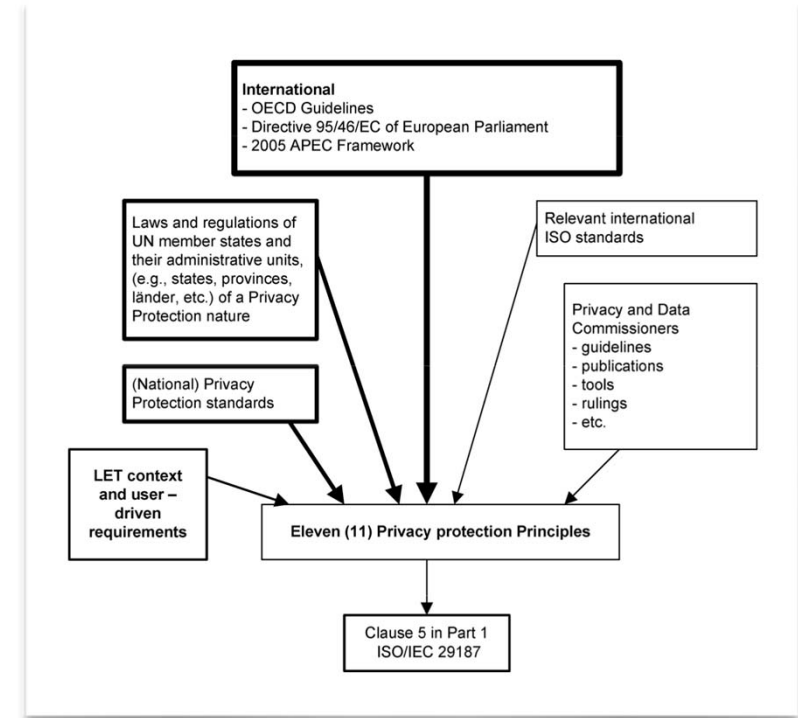
Brought to you by:



Created in collaboration with the GDPR Coalition

Privacy Principles

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimisation
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security
11. Privacy compliance



Source: Information technology — Identification of privacy protection requirements pertaining to learning, education and training (LET) — Part 1: Framework and reference model. ISO/IEC 29187-1:2013

Online: http://standards.iso.org/ittf/PubliclyAvailableStandards/c045266_ISO_IEC_29187-1_2013.zip

Privacy Before Research:

	PRIVACY BY DESIGN STRATEGY	DESCRIPTION
1	Minimize	The amount of personal data should be restricted to the minimal amount possible (data minimization).
2	Hide	Personal data and their interrelations should be hidden from plain view.
3	Separate	Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4	Aggregate	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	Inform	Data subjects should be adequately informed whenever processed (transparency).
6	Control	Data subjects should be provided agency over the processing of their personal data.
7	Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	Demonstrate	Data controllers must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

Privacy Before Research: Privacy by Design Strategy (Big Data)

	BIG DATA VALUE CHAIN	KEY PRIVACY BY DESIGN STRATEGY	IMPLEMENTATION
1	Data acquisition/collection	MINIMIZE	Define what data are needed before collection, select before collect (reduce data fields, define relevant controls, delete unwanted information, etc), Privacy Impact Assessments.
		AGGREGATE	Local anonymization (at source).
		HIDE	Privacy enhancing end-user tools, e.g. anti-tracking tools, encryption tools, identity masking tools, secure file sharing, etc.
		INFORM	Provide appropriate notice to individuals – Transparency mechanisms.
		CONTROL	Appropriate mechanisms for expressing consent. Opt-out mechanisms. Mechanisms for expressing privacy preferences, sticky policies, personal data stores.
2	Data analysis & data curation	AGGREGATE	Anonymization techniques (k-anonymity family, differential privacy).
		HIDE	Searchable encryption, privacy preserving computations.
3	Data storage	HIDE	Encryption of data at rest. Authentication and access control mechanisms. Other measures for secure data storage.
		SEPARATE	Distributed/ de-centralised storage and analytics facilities.
4	Data use	AGGREGATE	Anonymisation techniques. Data quality, data provenance.
5	All phases	ENFORCE/ DEMONSTRATE	Automated policy definition, enforcement, accountability and compliance tools.

Privacy Before Research: Privacy Enhancing Technologies in Big Data

Anonymization in big data (and beyond)

- Utility and privacy
- Attack models and disclosure risk
- Anonymization privacy models
- Anonymization privacy models and big data
- Anonymization methods
- Some current weaknesses of anonymization
- Centralized vs decentralized anonymization for big data
- Other specific challenges of anonymization in big data
- Challenges and future research for anonymization in big data

Encryption techniques in big data

- Database encryption
- Encrypted search

Security and accountability controls

- Granular access control
- Privacy policy enforcement
- Accountability and audit mechanisms
- Data provenance

Transparency and access

Consent, ownership and control

- Consent mechanisms
- Privacy preferences and sticky policies
- Personal data stores



WP Art 29: Big Data Concerns:

- the sheer **scale** of data collection, tracking and profiling, also taking into account the **variety** and **detail** of the data collected and the fact that data are often combined from many different sources;
- the **security** of data, with levels of protection shown to be lagging behind the expansion in volume;
- **transparency**: unless they are provided with sufficient information, individuals will be subject to decisions that they do not understand and have no control over;
- **inaccuracy, discrimination, exclusion and economic imbalance**;
- increased possibilities of **government surveillance**.

Open Science/ F.A.I.R. / Privacy/ Intellectual Property Rights

4th Taskforce GDPR Meeting, GÉANT,
Barcelona, April 23 2018

Marlon Domingus, CIPP/e, CIPM,
DPO Erasmus University Rotterdam



Open Science: As Open As Possible, As Closed As Necessary



EUROPEAN COMMISSION
Directorate-General for Research & Innovation

H2020 Programme

Guidelines to the Rules on
Open Access to Scientific Publications
and
Open Access to Research Data
in Horizon 2020

Version 3.2
21 March 2017



Opting out – partially or entirely

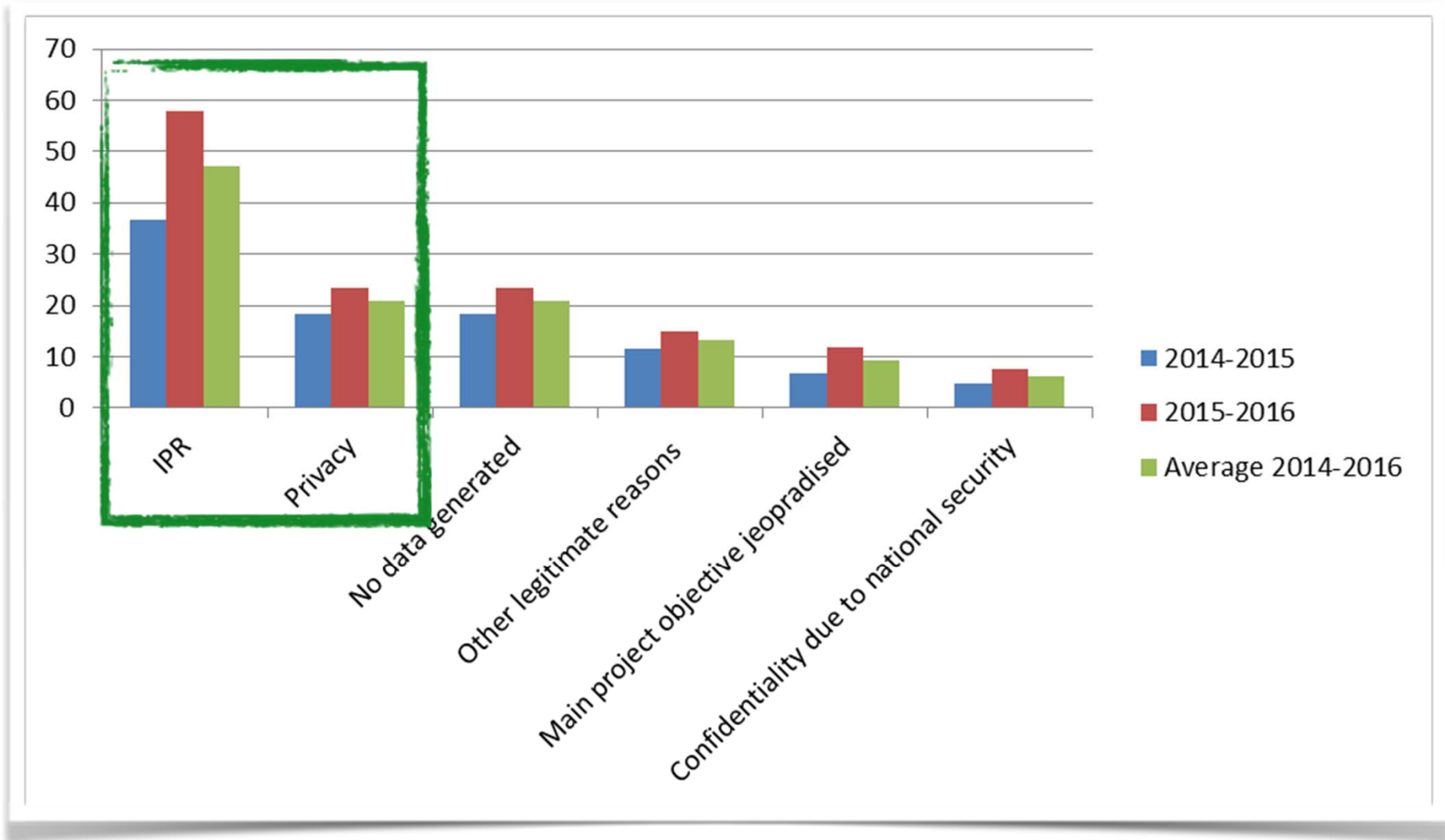
By extending the pilot, open access becomes the default setting for research data generated in Horizon 2020.

However, not all data can be open. Projects can therefore opt out at any stage (either before or after signing the grant) and so free themselves retroactively from the obligations associated with the conditions – if:

- participation is incompatible with the obligation to protect results that can reasonably be expected to be commercially or industrially exploited
- participation is incompatible with the need for confidentiality in connection with security issues
- participation is incompatible with rules on protecting personal data
- participation would mean that the project's main aim might not be achieved
- the project will not generate / collect any research data or
- there are other legitimate reasons (*you can enter these in a free-text box at the proposal stage*).

The Commission's approach can therefore be described as "*as open as possible, as closed as necessary*".

Lessons Learned: H2020 ORD Pilot Opt Out Reasons



Lessons Learned: IPR Helpdesk



www.iprhelpdesk.eu

European IPR Helpdesk

Fact Sheet *IP joint ownership*

October 2015¹

European IPR Helpdesk

We believe that knowing how to manage Intellectual Property Rights (IPR) is the ticket to innovation and competitiveness in Europe. The European IPR Helpdesk offers free of charge, first-line support on IP and IPR for research projects and EU SMEs involved in transnational research projects, especially within the Enterprise Europe Network.

Introduction.....	1
1. IP joint ownership	2
2. Allocation of shares between joint owners in collaborative research projects	4
2.1. Background	4
2.2. IP joint ownership	4
3. Conditions of use and exploitation of the jointly owned IP.....	5
3.1. Rights of use	5
3.2. Rights of exploitation	6
3.3. Dissemination and confidentiality	7
4. Management of the jointly owned IP	8
4.1. IPR protection	8
4.2. IPR infringement and enforcement issues.....	9
5. Governing law and jurisdiction	9
Useful Resources	10

IPR Helpdesk: Copyright Essentials

Copyright is an intellectual property right (IPR) that grants authors, artists and other creators protection for their literary, artistic and scientific creations, generally referred to as “works”.

No matter if you are a copyright owner or a copyright user, the understanding of the copyright basics is crucial to any business. In essence, it must be borne in mind that safeguarding your own copyright and securing the permission of third parties before using copyrighted materials is not only legally required but also a good business practice.

IPR Helpdesk: Copyright Essentials

Copyright protection is obtained automatically in the EU, as in any country which is a signatory to the Berne Convention. It arises **from the moment the work is created** and no registration or other formality is required.

The copyright system allows authors to benefit commercially from their work, through: **Economic** rights and **Moral** rights.

Some examples of economic rights

- right of reproduction, e.g. to make copies of the work such as printed publications or sound recordings
- right of distribution, e.g. to distribute copies of the work
- right of fixation, e.g. to record the work in, for example, a CD or DVD
- right of communication to the public, e.g. broadcasting via radio, TV or Internet
- right to perform the work publicly, e.g. to authorise live performances of the work such as in a play
- right to make "derivative works", e.g. to authorise modifications, translations, adaptations such as turning a novel into a screenplay, or other new uses of a work.

IPR Helpdesk: Copyright and other IPRs

	Pros	Cons
Copyright	<ul style="list-style-type: none"> • Automatic protection • No registration costs • Moral rights can be perpetual • Long-term protection for economic rights • Software and databases can also be protected by copyright 	<ul style="list-style-type: none"> • Requirement to qualify as a work • No priority • 20 years protection for neighbouring/related rights¹⁸ • There may be some extra requirements for designs to be copyrighted in some countries¹⁹
Patents	<ul style="list-style-type: none"> • Exclusive rights • 12 months priority • Stronger protection 	<ul style="list-style-type: none"> • Costly and lengthy procedures • 20 years protection • Disclosure requirement • Extra requirement for software to receive European patent protection²⁰
Industrial designs	<ul style="list-style-type: none"> • 3 years protection for unregistered designs • 6 months priority • Harmonisation at EU level • Some harmonisation at international level²¹ 	<ul style="list-style-type: none"> • Maximum non-renewable 25 years protection for registered Community designs²² • No renewable protection for unregistered Community designs
Databases ²³	<ul style="list-style-type: none"> • Exclusive rights • Secure protection 	<ul style="list-style-type: none"> • No priority • EU right only • 15 years protection²⁴
Trade marks	<ul style="list-style-type: none"> • Renewable indefinitely for periods of 10 years • 6 months priority • Harmonisation at EU level • Some harmonisation at international level²⁵ 	<ul style="list-style-type: none"> • Obligation to use²⁶

IPR Helpdesk: Joint Ownership

Joint ownership (co-ownership) refers to a situation in which two or more persons have proprietary shares of an asset: they co-own a property. **Joint ownership of IP**, in particular, frequently arises in **collaborative projects** when the **results have been jointly generated by the partners** and the share of work is not easily ascertainable.

Conditions of use and exploitation of the jointly owned IP:

- Rights of use
- Rights of exploitation
- Dissemination and confidentiality

IPR Helpdesk: Joint Ownership - Sample Clauses

RIGHT OF USE

OWNERSHIP OF INTELLECTUAL PROPERTY RIGHTS

RIGHT OF USE – background

RIGHT

RIGHT OF EXPLOITATION – second option [consent not required]

DISSEMINATION

1. If a Party intends to publish information and other research materials related to the collaboration project hereof, such a party shall, prior to publication, provide [...] days as examination period for the other party to verify whether the contents of such dissemination disclosed should be kept confidential. Such other party may request in writing to extend the examination period, due to the importance of the information disclosed.

CONFIDENTIALITY

2. Confidential Information shall not be disclosed, copied, reproduced, or otherwise made available to any other third party without the consent of the other Parties. Each Party agrees to use its best efforts to maintain the confidentiality and to keep data and research materials confidential until published or until corresponding patent applications are filed;
3. Confidentiality obligation shall expire at the earlier of the date when the information is publicly known or [...] years after the expiration or termination date of this Agreement. Each Party may request an extension to this term when necessary to protect confidential information relating to foreground not yet commercialised.

[sample clauses]

e of its interest in
to the other Party

Its to third parties

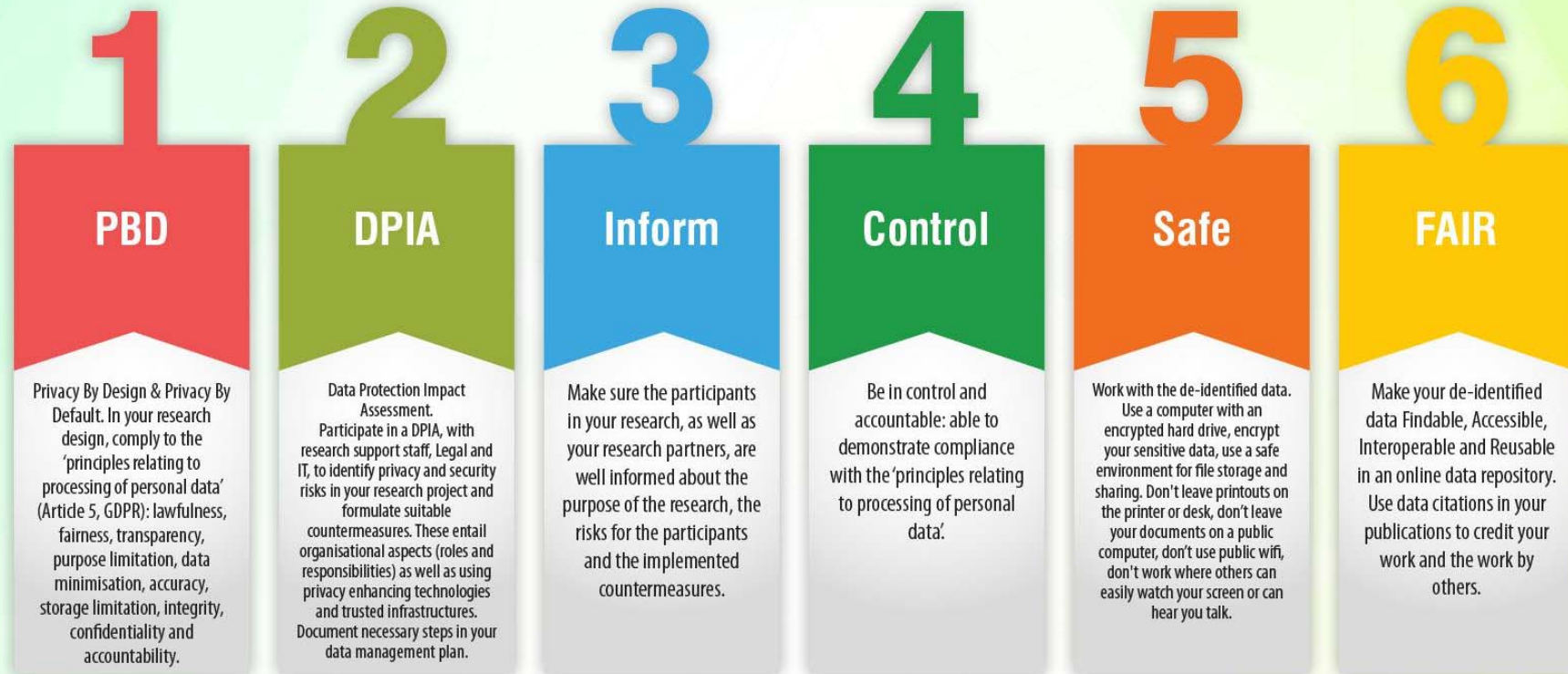
f the foreground shall
o the type of license
it by the Parties.

[sample clauses]



EU General Data Protection Regulation: Privacy Before, During and After Research

HOW TO TREAT PERSONAL DATA IN RESEARCH. RESPONSIBLE USE OF PERSONAL DATA BEFORE, DURING AND AFTER RESEARCH.



For More Information visit
www.gdprcoalition.ie

Twitter
[@GDPR_Coalition](https://twitter.com/GDPR_Coalition)

Linkedin
gdpr Coalition

Brought to you by:



Created in collaboration with the GDPR Coalition

Questions?

drs. Marlon Domingus, CIPP/e, CIPM
DPO, Erasmus University Rotterdam

T +31 10 4088006

E dpo@eur.nl



Stay in touch via: <https://www.linkedin.com/in/domingus/>

How to deal with Research Data

4th Taskforce GDPR Meeting, GÉANT,
Barcelona, April 23 2018

Marlon Domingus, CIPP/e, CIPM,
DPO Erasmus University Rotterdam



Cross Border Data Transfers

Adequacy Decision

The European Commission decides whether a country outside the EU (a so called 'third country') offers an adequate level of data protection. This decision is called the 'adequacy decision'.

GDPR: EU and EEA

The General Data Protection Regulation (GDPR) applies in the 28 Member States of the EU, as well as in the three European Economic Area (EEA) countries, not in the EU: Norway, Iceland, and Liechtenstein. These three countries will become subject to the GDPR at the same time as the EU countries.

Adequate

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing *adequate protection*.

Adequacy talks are ongoing with Japan and South Korea.

Cross Border Data Transfers



-  Belgique / België
-  Bulgaria
-  Česká republika
-  Danmark
-  Deutschland
-  Eesti
-  Ελλάς / Ελλάδα
-  España
-  France
-  Hrvatska
-  Ireland / Éire
-  Italia
-  Κύπρος / Kypros
-  Latvija
-  Lietuva
-  Luxembourg
-  Magyarország
-  Malta
-  Nederland
-  Österreich
-  Polska
-  Portugal
-  România
-  Slovenija
-  Slovensko
-  Suomi / Finland
-  Sverige
-  United Kingdom
-  Island / Iceland
-  Liechtenstein
-  Norway

Privacy Awareness: Infographics

A RESEARCHER'S PRIVACY REFERENCE CARD

General Data Protection Regulation (GDPR)
WHY? / WHAT? / HOW?

INFORMATIONAL PRIVACY
Protection of personal data
Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned.

BE A TRUSTWORTHY RESEARCH PARTNER
Your focus on respecting fundamental rights and freedoms will not go unnoticed by research funders, research partners and the general public.

PROTECT DATA SUBJECT'S RIGHTS
Be transparent about what happens with the data subjects' data.

LIMIT LIABILITY
Data subjects are to be fully and effectively compensated for the damage they suffer with regards to the processing of their personal data.

Controllers or processors involved in this processing are to be held liable for the entire damage. Furthermore, penalties including administrative fines are to be imposed for any infringement of the data subject's fundamental rights and freedoms.

AVOID BAD PRESS
Damage to your reputation or your university's reputation, due to data leaks or other cases in which data protection where inadequate, is, for obvious reasons, generally undesirable.

ACT IN ACCORDANCE WITH THE LAW
Natural persons, whatever their nationality or residence, have the fundamental right to the protection of their personal data.

Processing of this data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation.

TO BE ELIGIBLE TO EXTERNAL RESEARCH FUNDING
Research funders stipulate applying personal data protection practices in their funding conditions.

BE A TRUSTWORTHY RESEARCHER
Be trustworthy by using of the subject's data with integrity, as a shared responsibility within the research institute.

SHARE, ARCHIVE, PUBLISH RESEARCH DATA
Applying personal data protection practices, which no longer permits the identification of data subjects, ensures usage and reuse of your research data, which enables relevant data citations, thus providing visible credits for your work.

SUPPORT:
Email: researchsupport@eur.nl
Phone: +31 10 4088006

Marlon Domingus, November 2016, version 1.0
<https://creativecommons.org/licenses/by-nc/4.0/>

A RESEARCHER'S PRIVACY REFERENCE CARD

General Data Protection Regulation (GDPR)
WHY? / WHAT? / HOW?

INFORMATIONAL PRIVACY
Protection of personal data
Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned.

PURPOSE LIMITATION
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

DATA PROTECTION IMPACT ASSESSMENT
A data protection impact assessment is performed to evaluate, in particular, the origin, nature, particularity and severity of the risk to the rights and freedoms of natural persons. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to process the personal data.

STORAGE LIMITATION
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes.

PERSONAL DATA?
'Personal data' means any information relating to an identified or identifiable natural person ('data subject').

LAWFULNESS OF PROCESSING
Processing of personal data is lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

INFORMED CONSENT
Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research.

DATA MINIMISATION
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

PSEUDONYMISATION
Pseudonymisation of personal data is one of the measures that can reduce the risks to the data subjects concerned, and help controllers and processors to meet their data-protection obligations.

SUPPORT:
Email: researchsupport@eur.nl
Phone: +31 10 4088006

Marlon Domingus, November 2016, version 1.0
<https://creativecommons.org/licenses/by-nc/4.0/>

HOW TO TREAT PERSONAL DATA IN RESEARCH?

Responsible use of personal data before, during and after research.

PRIVACY BY DESIGN AND BY DEFAULT

BEFORE RESEARCH

- In your research design, address these six security and privacy goals, as identified by: www.datenschutzzentrum.de
- Participate in a *data protection impact assessment* to identify risks and formulate countermeasures.
- Communicate the security and privacy measures for your research in your *data management plan* and with all participants and data subjects.

DURING RESEARCH

- Make sure your data subjects are well informed about the purpose of the research and their risks, before they sign the *informed consent form*.
- Only generate and use data that are relevant for the purpose of your research: *data minimisation*
- Use a computer with an encrypted hard drive, encrypt your sensitive data, use *SURFdrive* for safe and secure file storage and sharing.

AFTER RESEARCH

- Anonymise and / or pseudonymise the data and work with the de-identified data.
- Work safe: don't leave printouts on the printer or desk, don't use public wifi, don't work where others can easily watch your screen or can hear you talk.
- During research feel free to consult us in case of practical issues or just to reflect on aspects.

Share your experiences with us, contact us for support before, during and after research:
DATASUPPORT@UBIB.EUR.NL
+31 10 4088006

SEE ALSO:
[HTTPS://WWW.EUR.NL/RESEARCHMATTERS/RDM/RDM_SERVICES/](https://www.eur.nl/researchmatters/rdm/rdm_services/)

PRIVACY For Academic Research COOKBOOK



a case study: Erasmus University Rotterdam



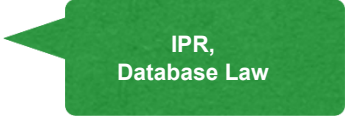
* Images are clickable links *

- Recognise that Research Data Management is a collaborative endeavour to enable responsible research. If personal data is used, safeguarding privacy for data subjects is a concern. Perform a *Privacy Impact Assessment* and add it to the data management plan.
- Invest in explaining the what, why and how of safeguarding privacy in academic research and provide the relevant support, infrastructure, tooling, instruments for data protection.
- Assess the privacy readiness of your organisation and recognise the differences in perspective across the university. Develop a common language by collaborating in shaping privacy in academic research.
- Define and implement a privacy strategy. Many great starting points are available.

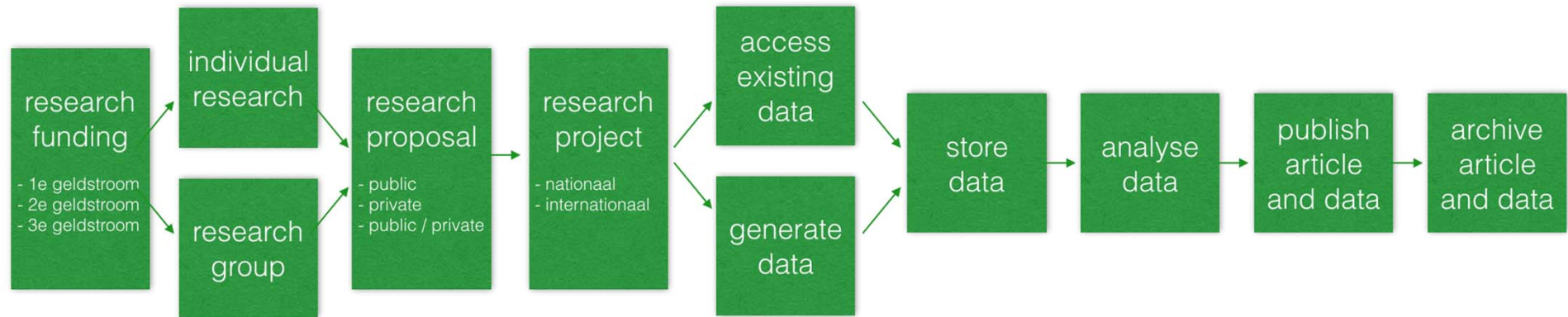
Marlon Domingus | dominguss@ubib.eur.nl | March 2017

EUR Research Assessment

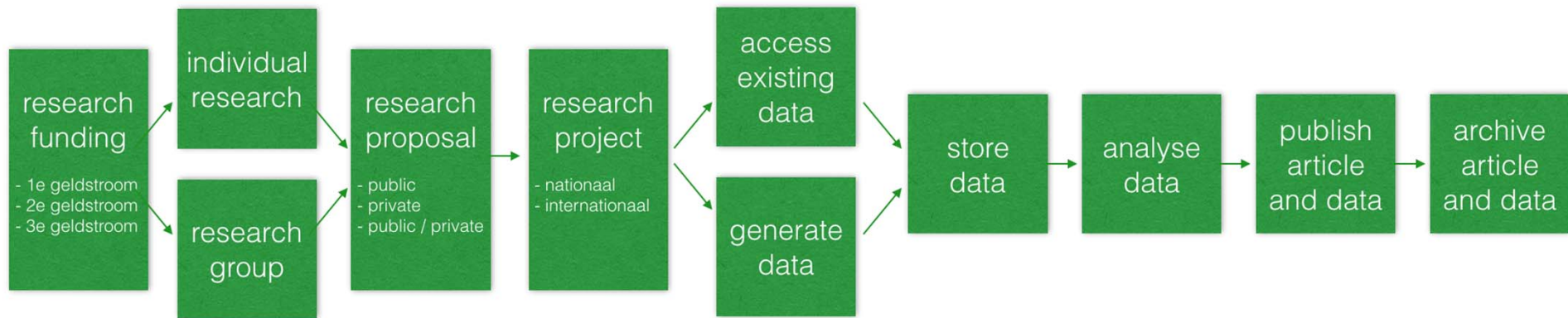
1. Is the research project conducted in an international partnership?

2. Is this partnership a public-private collaboration?

3. Is personal data or confidential data used in the research?

4. Will the research project result in information and/or products that will become open access available, or commercially or both?

5. Is an infrastructure required for the processing / analysis / storage of the research data beyond which is available at the EUR workplace?

6. Will the data processing be a manual activity, or is it automated and executed by scripts?


Data Driven Research



Data Driven Research

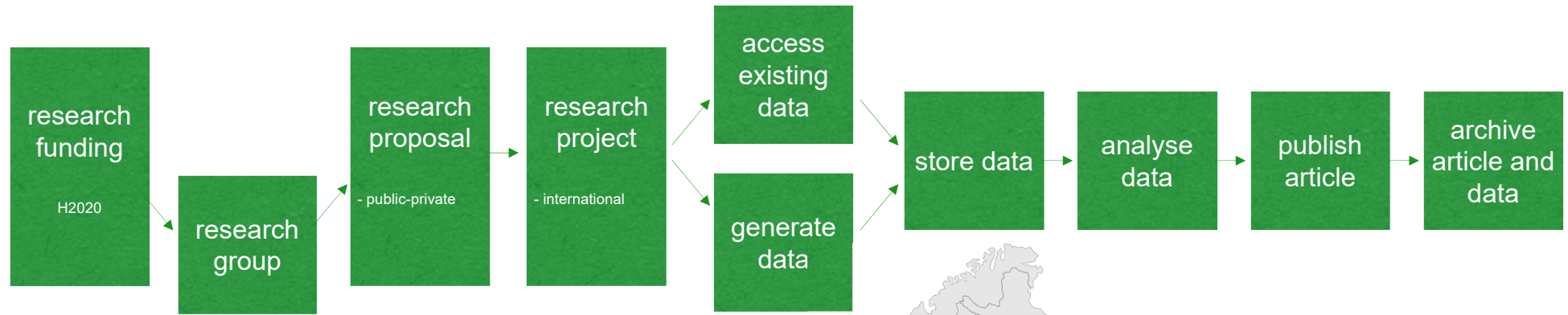


Context								
Policy	1. Research Institute 2. University, LERU, ... 3. OCW/NWO/KNAW 4. External funder (EU, Industry, ...) 5. Publisher / Journal	1. Research Institute 2. University, LERU, ... 3. OCW/NWO/KNAW 4. External funder (EU, Industry, ...) 5. Publisher / Journal	1. Research Institute 2. University, LERU, ... 3. OCW/NWO/KNAW 4. External funder (EU, Industry, ...) 5. Publisher / Journal	1. Research Institute 2. University, LERU, ... 3. OCW/NWO/KNAW 4. External funder (EU, Industry, ...) 5. Publisher / Journal	1. Research Institute 2. University, LERU, ... 3. OCW/NWO/KNAW 4. External funder (EU, Industry, ...) 5. Publisher / Journal	1. Research Institute 2. University, LERU, ... 3. OCW/NWO/KNAW 4. External funder (EU, Industry, ...) 5. Publisher / Journal	1. Research Institute 2. University, LERU, ... 3. OCW/NWO/KNAW 4. External funder (EU, Industry, ...) 5. Publisher / Journal	1. Research Institute 2. University, LERU, ... 3. OCW/NWO/KNAW 4. External funder (EU, Industry, ...) 5. Publisher / Journal
Infra & Tooling	1. Research Institute 2. University 3. National funders 4. European funders 5. Other funders 6. Journals	1. Research Institute 2. University 3. National funders 4. European funders 5. Other funders 6. Journals	1. Research Institute 2. University 3. National funders 4. European funders 5. Other funders 6. Journals	1. Research Institute 2. University 3. National funders 4. European funders 5. Other funders 6. Journals	1. Research Institute 2. University 3. National funders 4. European funders 5. Other funders 6. Journals	1. Research Institute 2. University 3. National funders 4. European funders 5. Other funders 6. Journals	1. Research Institute 2. University 3. National funders 4. European funders 5. Other funders 6. Journals	1. Research Institute 2. University 3. National funders 4. European funders 5. Other funders 6. Journals
Legal & Ethical	1. Contracts & Agreements 2. Codes of conduct (National / EU / ...) 3. Laws & Regulations (National / EU / ...)	1. Contracts & Agreements 2. Codes of conduct (National / EU / ...) 3. Laws & Regulations (National / EU / ...)	1. Contracts & Agreements 2. Codes of conduct (National / EU / ...) 3. Laws & Regulations (National / EU / ...)	1. Contracts & Agreements 2. Codes of conduct (National / EU / ...) 3. Laws & Regulations (National / EU / ...)	1. Contracts & Agreements 2. Codes of conduct (National / EU / ...) 3. Laws & Regulations (National / EU / ...)	1. Contracts & Agreements 2. Codes of conduct (National / EU / ...) 3. Laws & Regulations (National / EU / ...)	1. Contracts & Agreements 2. Codes of conduct (National / EU / ...) 3. Laws & Regulations (National / EU / ...)	1. Contracts & Agreements 2. Codes of conduct (National / EU / ...) 3. Laws & Regulations (National / EU / ...)
Support	1. contact person 2. examples, best practices (website, training) 3. templates (website, training)	1. contact person 2. examples, best practices (website, training) 3. templates (website, training)	1. contact person 2. examples, best practices (website, training) 3. templates (website, training)	1. contact person 2. examples, best practices (website, training) 3. templates (website, training)	1. contact person 2. examples, best practices (website, training) 3. templates (website, training)	1. contact person 2. examples, best practices (website, training) 3. templates (website, training)	1. contact person 2. examples, best practices (website, training) 3. templates (website, training)	1. contact person 2. examples, best practices (website, training) 3. templates (website, training)

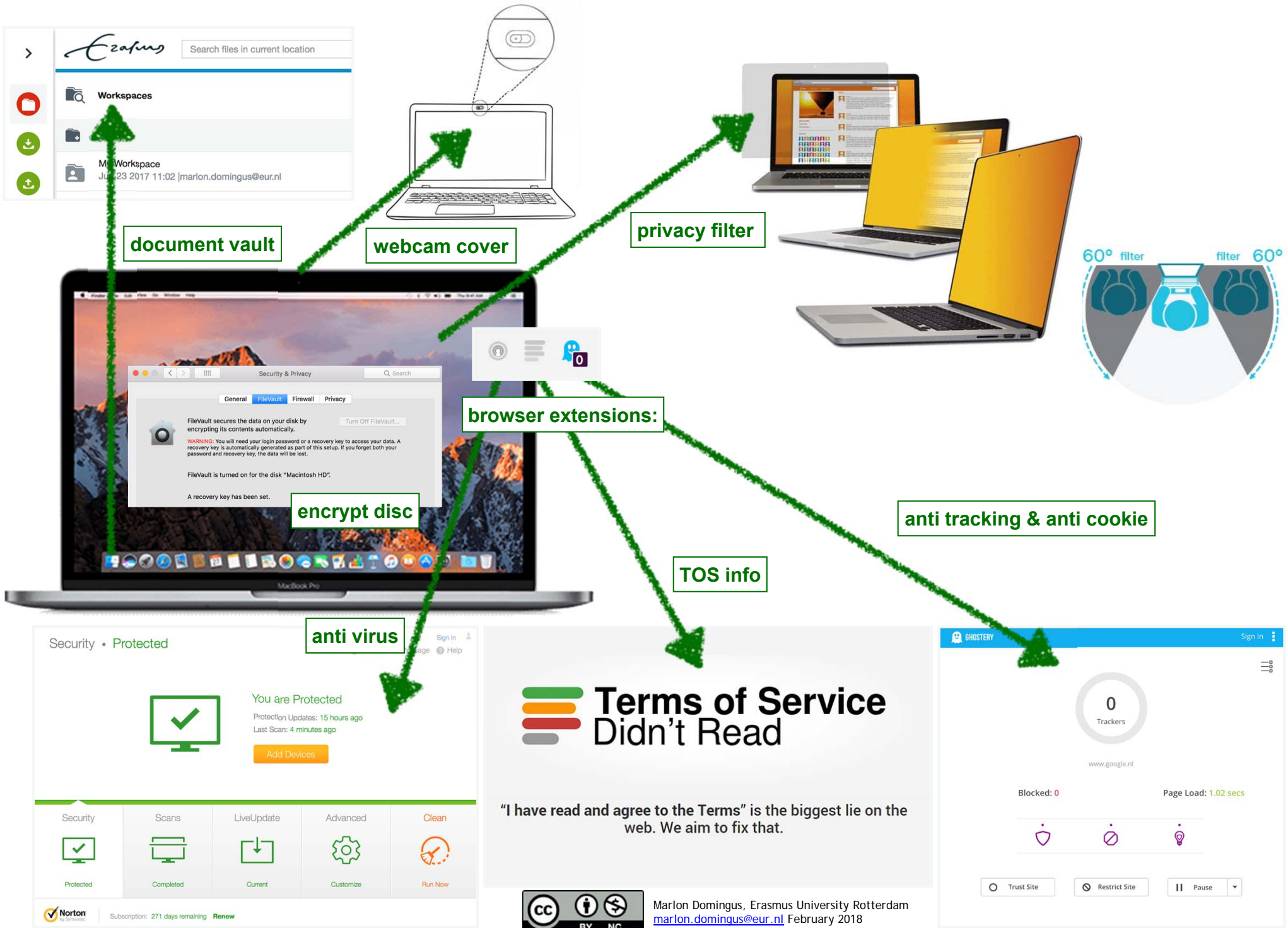


Research Scenario 1

Pan European Public-Private H2020 Funded Consortium: Big Data Health Economics



The EUR Researcher's Guide To Mobile Security



On De-identification

A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.



This is a primer on how to distinguish different categories of data.

DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA
























Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
 DIRECT IDENTIFIERS Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	 INTACT	 PARTIALLY MASKED	 PARTIALLY MASKED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED
 INDIRECT IDENTIFIERS Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	 INTACT	 INTACT	 INTACT	 INTACT	 INTACT	 INTACT	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED	 ELIMINATED or TRANSFORMED
 SAFEGUARDS and CONTROLS Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	 NOT RELEVANT due to nature of data	 LIMITED or NONE IN PLACE	 CONTROLS IN PLACE	 CONTROLS IN PLACE	 LIMITED or NONE IN PLACE	 CONTROLS IN PLACE	 LIMITED or NONE IN PLACE	 CONTROLS IN PLACE	 NOT RELEVANT due to nature of data	 NOT RELEVANT due to high degree of data aggregation

SELECTED EXAMPLES

Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)

Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)

Same as Potentially identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)

Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csr123)

Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = SL7T LX619Z) (unique sequence not used anywhere else)

Same as Pseudonymous, except data are also protected by safeguards and controls

Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)

Same as De-Identified, except data are also protected by safeguards and controls

For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)

Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)