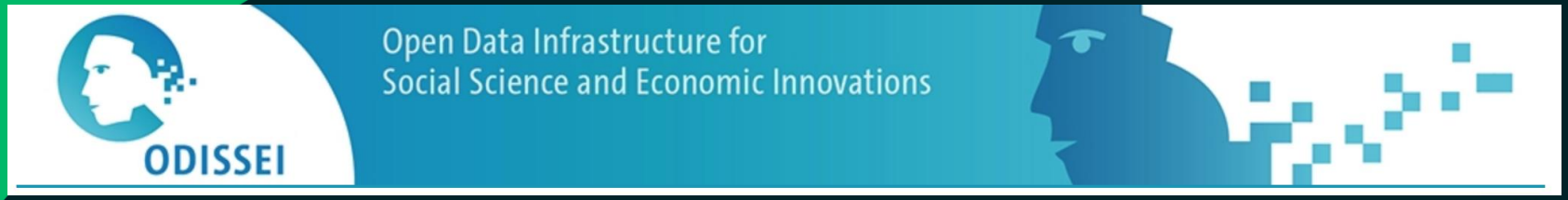
Responsibly Linking Data.

Legal aspects in the GDPR (NL: AVG) Perspective

ODISSEI workshop, Utrecht, October 26 2017

Marlon Domingus



Erasmus University Rotterdam

Agenda

- The GDPR in the context of Academic Research
- Research Scenarios
- Typical issues
- Next Steps

The GDPR
in the context of Academic Research

ODISSEI workshop, Utrecht, October 26 2017

Marlon Domingus

Erasmus University Rotterdam

Does Privacy Threaten Research And / Or Does Research Threaten Privacy?

- The GDPR defines privacy rights and responsibilities
- but with the intend to facilitate the responsible free floating of data within the EU to strengthen the internal market, especially by public - private driven innovation.
- The Right to Privacy is not an absolute right, but a fundamental right amongst other rights.

"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

- Conclusion: no business as usual, but also no disruption of research.
- GDPR is a game changer, and we have to shift to the new paradigm

Code: What, How and Who

October 2017

25 May 2018

What & How

Who

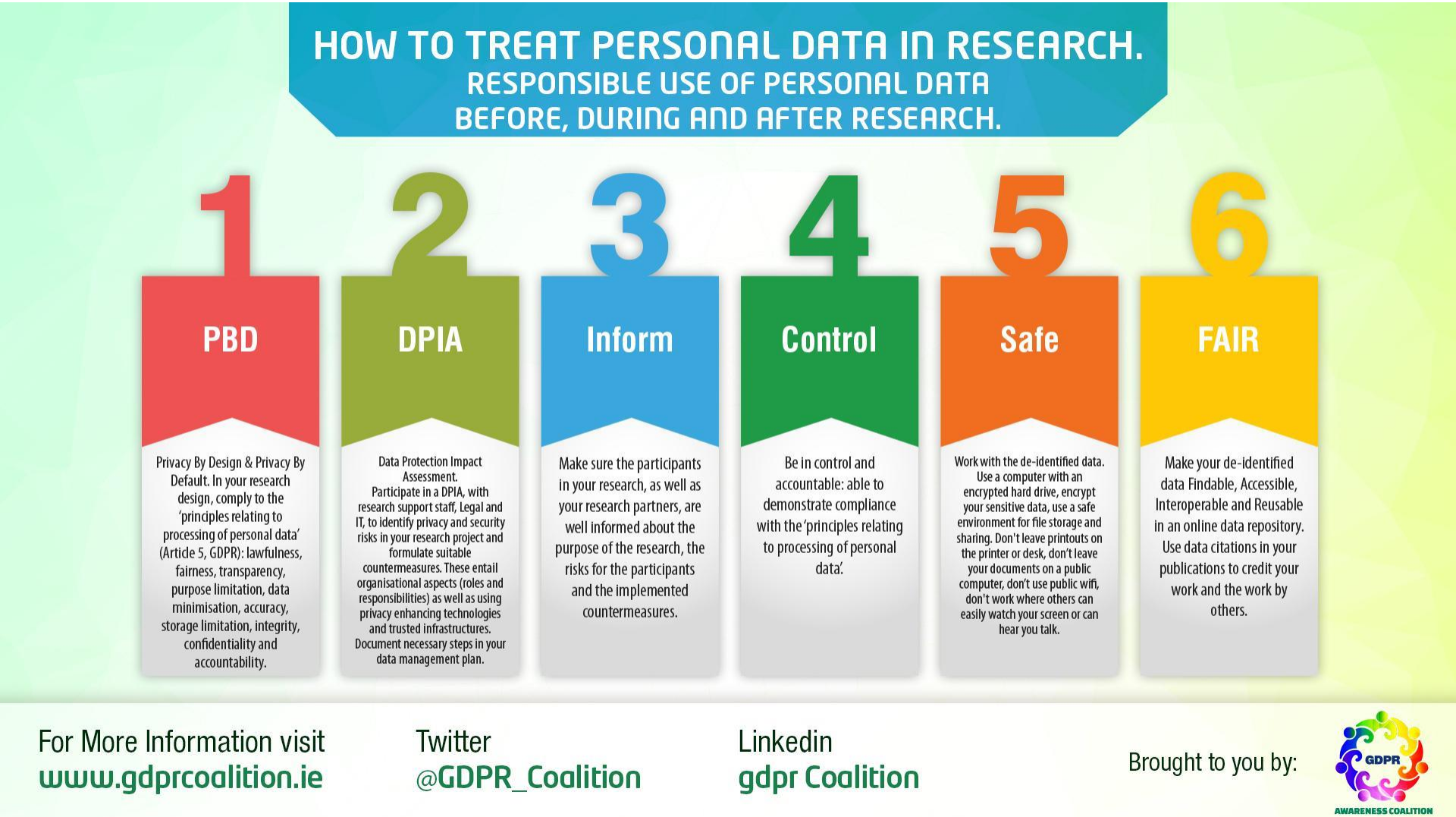
University: necessary general conditions to enable researchers to demonstrate compliance; policy, guidelines, infrastructure and skilled and available research support staff.

Dean: 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 policy, guidelines, infrastructure and skilled and available research support staff.

2. The EU General Data Protection Regulation:

Privacy Before, During and After Research



For More Information visit
www.gdprcoalition.ie

Twitter
@GDPR_Coalition

Linkedin
gdpr Coalition

Brought to you by:

GDPR AWARENESS COALITION

Created in collaboration with the GDPR Coalition

1. The EU General Data Protection Regulation:

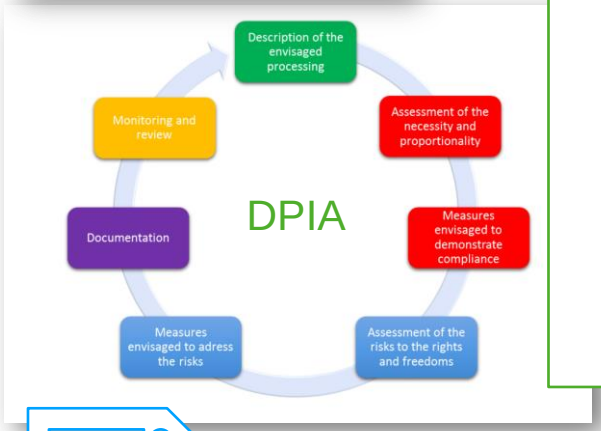
Article 5 GDPR: Principles Relating to Processing of Personal Data

Source: http://gdprcoalition.ie/infographics/

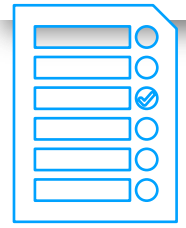
Privacy Before Research: Data Management Plan

Privacy Principles

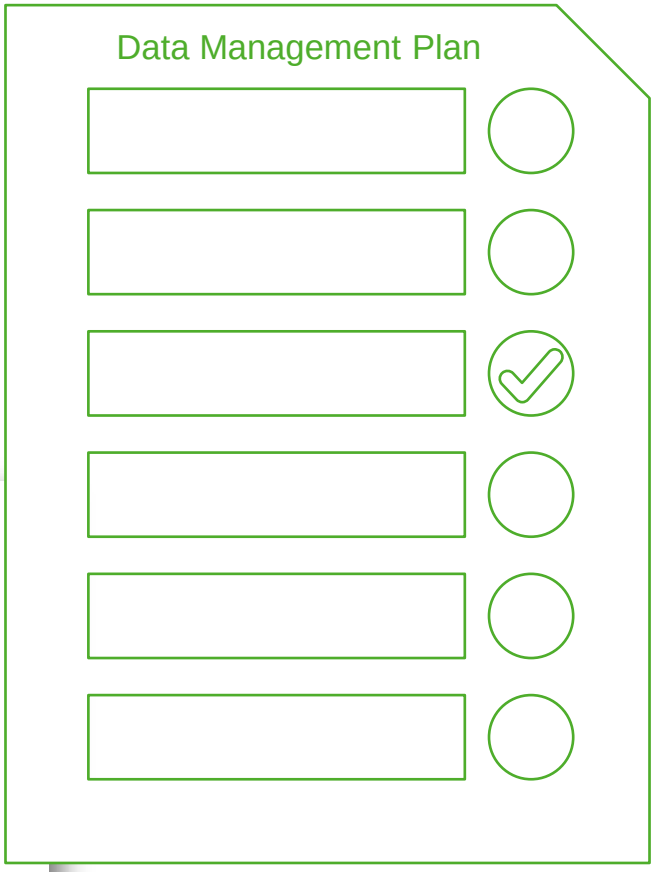
1



2



Risks, Appropriate Organisational and Technical Measures, Ethical Self Assessment



ICON	ESSENTIAL INFORMATION
	No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing
	No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing
	No personal data are **processed** for purposes other than the purposes for which they were collected
	No personal data are **disseminated** to commercial third parties
	No personal data are **sold or rented out**
	No personal data are retained in **unencrypted** form

Two Models of Governance

Command & Control

- Fixed norm
- Actor
- Sanction
- Example: METC

Reflexive regulation

- Situated norm
- Multiple Actors
- Learn
- Example: intervision

Source: Prof. Dr. Antoinette de Bont, Erasmus School of Health Policy & Management (ESHPM): *The Governance of re-use of data.* Summerschool 9-12 July 2017 @ Erasmus MC.

Reprise: Two Models of Governance

Reflexive regulation

- Situated norm (in context)
- Multiple Actors
- Learn

Focus Points:

- Nature of the Data
- Nature of the Consortium
- Nature of the Dataflow
- Appropriate Measures

Balancing the legitimate interests of the research 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

Source: Brendan Van Alsenoy (Belgian Privacy Commission), *Balancing the interests of controllers and the rights of the data subject.* Brussels Privacy Hub, VUB Brussel, June 30 2017.

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

Article 8 - Protection of personal data

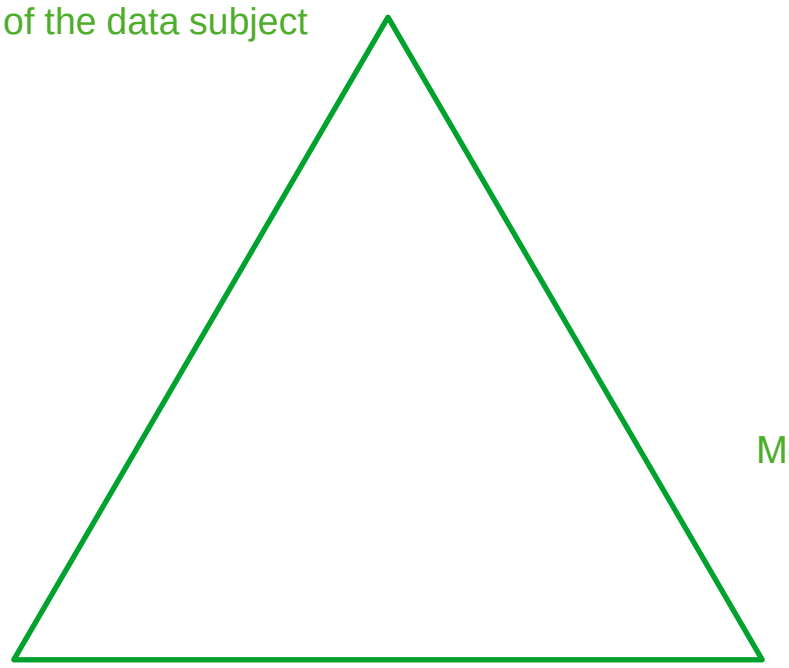
1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Source: **Charter of Fundamental Rights of the European Union (2012/C 326/02).**
Online: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN .

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



GDPR

Member States' Implementation Legislation

(Inter)National Codes of Conduct

- ISO Standards
- NEN Norms

WP29 Opinions

- Discipline Specific
- Good Practices

Source: **Prof. Dr. Gloria González Fuster***: Recent jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union*. Brussels Privacy Hub, VUB Brussel, June 30 2017.

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

Source: Article 29 Data Protection Working Party. Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC". Adopted on 9 April 2014. Online: **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf**

Research Scenarios and the General Data Protection Regulation: Privacy Principles and Corresponding Actions

Met de huidige stand van de techniek (anno 2016) worden de volgende maatregelen doorgaans als passend gezien:

1. Authenticatie op een vertrouwde locatie, zoals een werkplek[24] binnen een beveiligd kantoor en op een beveiligd netwerk[25], vindt minimaal op basis van een kenniskenmerk (wachtwoord) plaats.
2. Authenticatie op een niet-vertrouwde locatie, zoals een werkplek thuis of in een openbare ruimte, of via een niet vertrouwd netwerk[26], vereist naast het kenniskenmerk ook een bezitskenmerk.
3. Persoonsgegevens die worden verstuurd over het bedrijfseigen beveiligde netwerk worden bij voorkeur versleuteld; buiten het eigen beveiligde netwerk, zoals Internet, worden ze altijd versleuteld. Dit geldt ook op draagbare media.
4. Services[27] die persoonsgegevens verwerken of aanbieden zijn niet te benaderen zonder autorisatie en authenticatie, bijvoorbeeld door het gebruik van certificaten.
5. Fysieke en logische maatregelen schermen de verwerking van de persoonsgegevens af, bijvoorbeeld door servers in afgesloten ruimtes te plaatsen en systemen/componenten te 'hardenen'[28].
6. De toegang tot persoonsgegevens door systeembeheerders wordt vastgelegd (tijd en raadpleger worden gelogd).
7. De toegang en het gebruik wordt vastgelegd (tijd, raadpleger, proces, en resultaat worden gelogd).

In aanvulling op de maatregelen voor de 'gewone' persoonsgegevens worden de volgende maatregelen voor bijzondere persoonsgegevens doorgaans als passend gezien:

8. Authenticatie vindt naast het kenniskenmerk altijd ook op basis van een bezitskenmerk plaats.
9. Bijzondere persoonsgegevens worden, ook als ze verstuurd worden over het bedrijfseigen beveiligde netwerk, versleuteld.

Source: *Centrum voor Informatiebeveiliging en Privacybescherming (CIP): Handleiding Privacy by Design, 7 mei 2017.* https://www.cip-overheid.nl/wp-content/uploads/2017/05/20170507%20Handleiding%20Privacy%20by%20Design%20v3.0.pdf

What we don't want; Data Breaches 2017:

3	Entity	alternative name	story	YEAR	records lost	ORGANISATION	METHOD OF LEAK
4	**CEX**		A misconfigured spambot leaked full contact info & financial details, although the newest financial data dates to 2009.	14	2000000	retail	accidentally published
5	**Instagram**		A bug exposed user's contact information. Instagram initially said it affected only verified accounts, but has now admitted non-verified users were also affected. Instagram hasn't confirmed numbers, but hackers say they have info from 6m accounts.	14	6000000	web	hacked
6	**Equifax**		If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.	14	143000000	financial	hacked
7	**Nival**	Videogame maker	A teen hacker has randomly hacked several Russian websites. In a statement, he claims the hack was revenge for the MH17 crash. The companies affected have not commented, however Troy Hunt, a security researcher, has confirmed its legit. Nival and KM.ru were both hacked.	14	1500000	web	hacked
8	**KM.ru**	News site and email provider	A teen hacker has randomly hacked several Russian websites. In a statement, he claims the hack was revenge for the MH17 crash. The companies affected have not commented, however Troy Hunt, a security researcher, has confirmed its legit. Nival and KM.ru were both hacked.	14	1500000	web	hacked
9	**Waterly**	App for paying water bills	Jan 2017. Israel-based app contained a vulnerability in the sign-in process that could potentially expose user account details. The problem was fixed within 2 weeks of being identifiied.	14	1000000	app	poor security

1	name	alternativename	notes	primaryval	subcategory	category	type
2	**Ohio State University**			6	760,000	academic	hacked
3	**Stanford University**		Tens of thousands of past and current Stanford University employees had personal information - including their dates of birth, Social Security numbers and home addresses - stored on the hard drive of a stolen university laptop.	4	72,000	academic	lost / stolen computer
4	**University of California Berkeley**	details on students, alumni and others		5	160,000	academic	hacked
5	**University of Miami**		Thieves stole a briefcase containing data tapes out of a vehicle used by a private off-site storage company. Anyone who had been a patient of a University of Miami physician or visited a UM facility since 1999 is likely included on the tapes. The data included names, addresses, Social Security numbers and health information. 47,000 of these records may have included credit card or other financial information regarding bill payment.	4	2,100,000	academic	lost / stolen computer
6	**University of Utah Hospitals & Clinics**	stolen data tapes	The data tapes were stolen by petty thieves from an employee's car. According to police reports the thieves tried - and failed - to view the tapes using a VHS player.	4	2,200,000	academic	lost / stolen media
7	**University of Wisconsin - Milwaukee**			7	73,000	academic	hacked
8	**Yale University**			6	43,000	academic	accidentally published

Source: Information is Beautiful: Data Breaches (public), bit.ly/bigdatabreaches

Privacy Before Research:
Privacy by Design Strategy ('traditional 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.

Source: ENISA report (2015): Privacy By Design In Big Data. Online: https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport

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

	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	Anoymisation techniques. Data quality, data provenance.
5	All phases	ENFORCE/ DEMONSTRATE	Automated policy definition, enforcement, accountability and compliance tools.

Source: ENISA report (2015): Privacy By Design In Big Data. Online: https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport

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

Source: ENISA report (2015): Privacy By Design In Big Data. Online: https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport

Research Scenarios

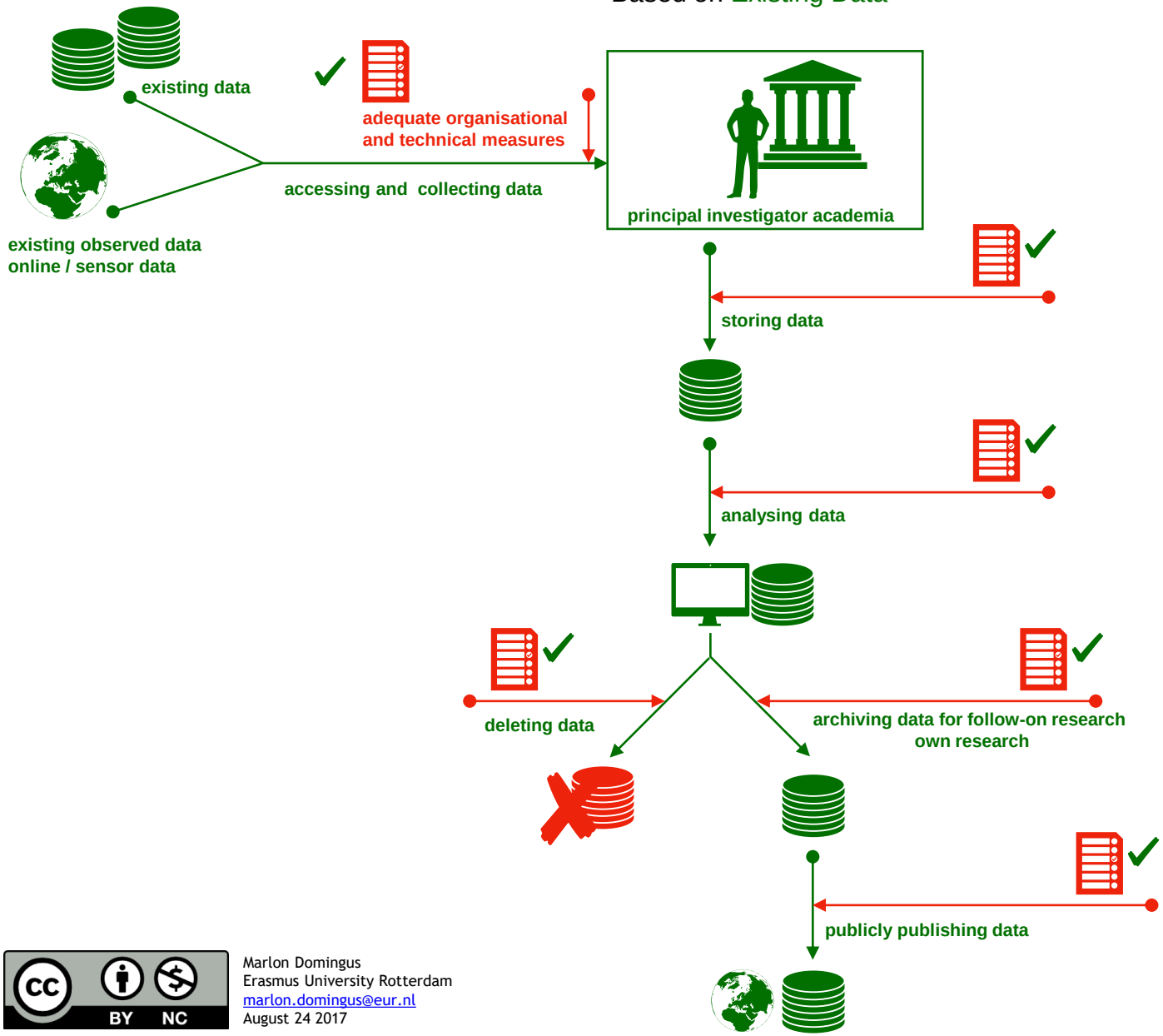
ODISSEI workshop, Utrecht, October 26 2017

Marlon Domingus

Erasmus University Rotterdam

Research Scenarios and the General Data Protection Regulation:

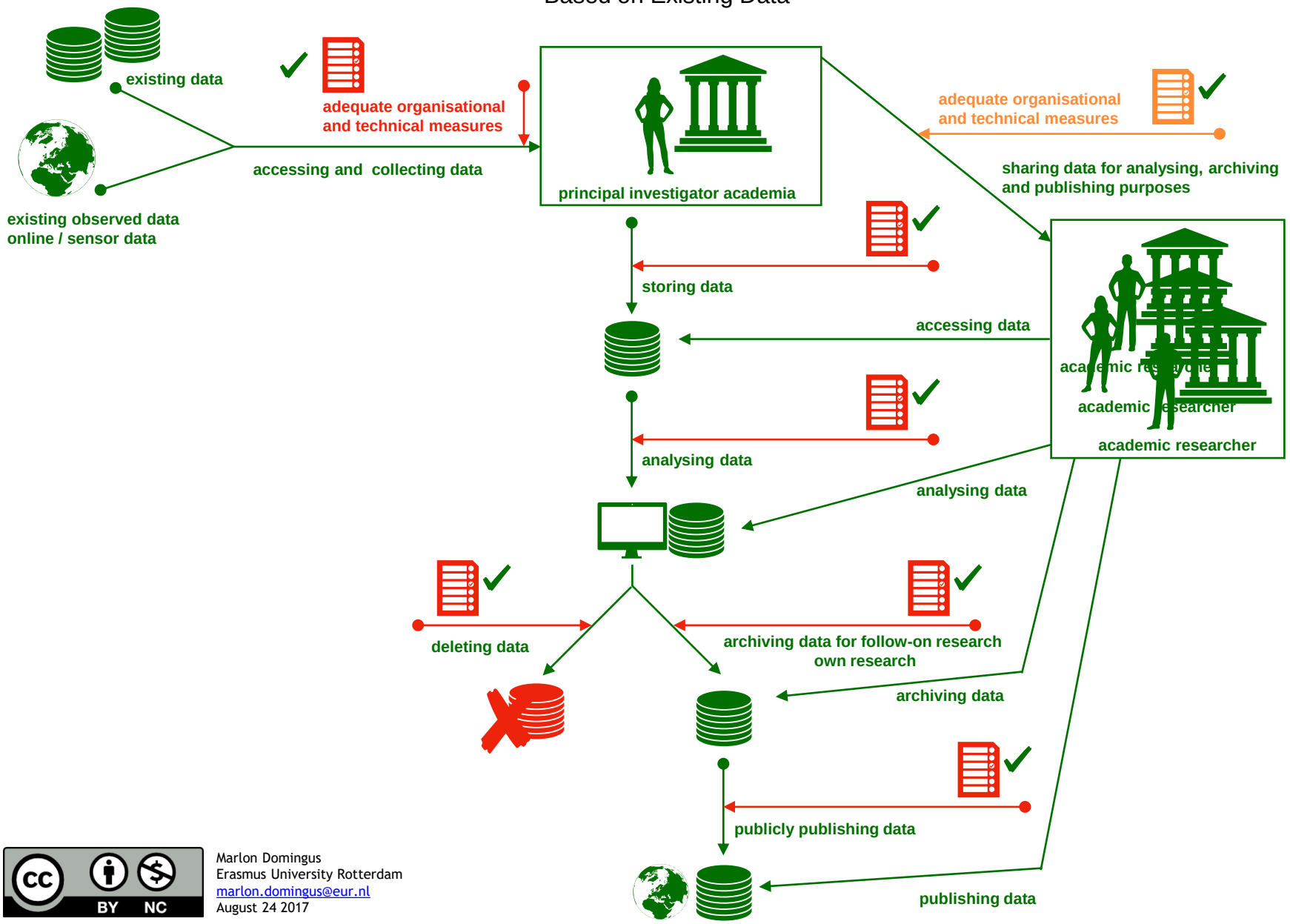
1. Individual Academic Research
Based on Existing Data



Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

Research Scenarios and the General Data Protection Regulation:

2. Academic Research by an International Research Group Based on Existing Data

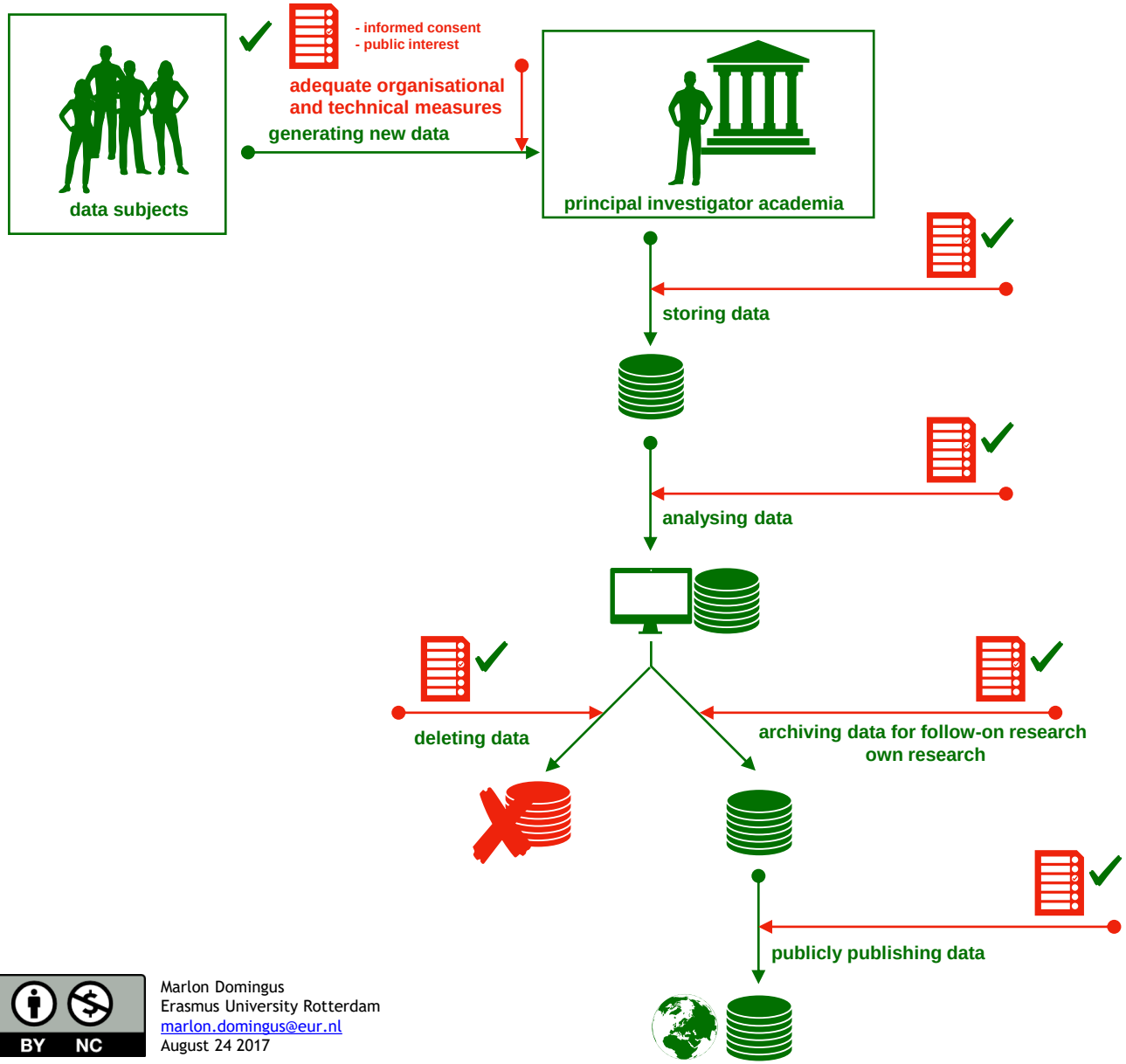


Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

Research Scenarios and the General Data Protection Regulation:

3. Individual Academic Research

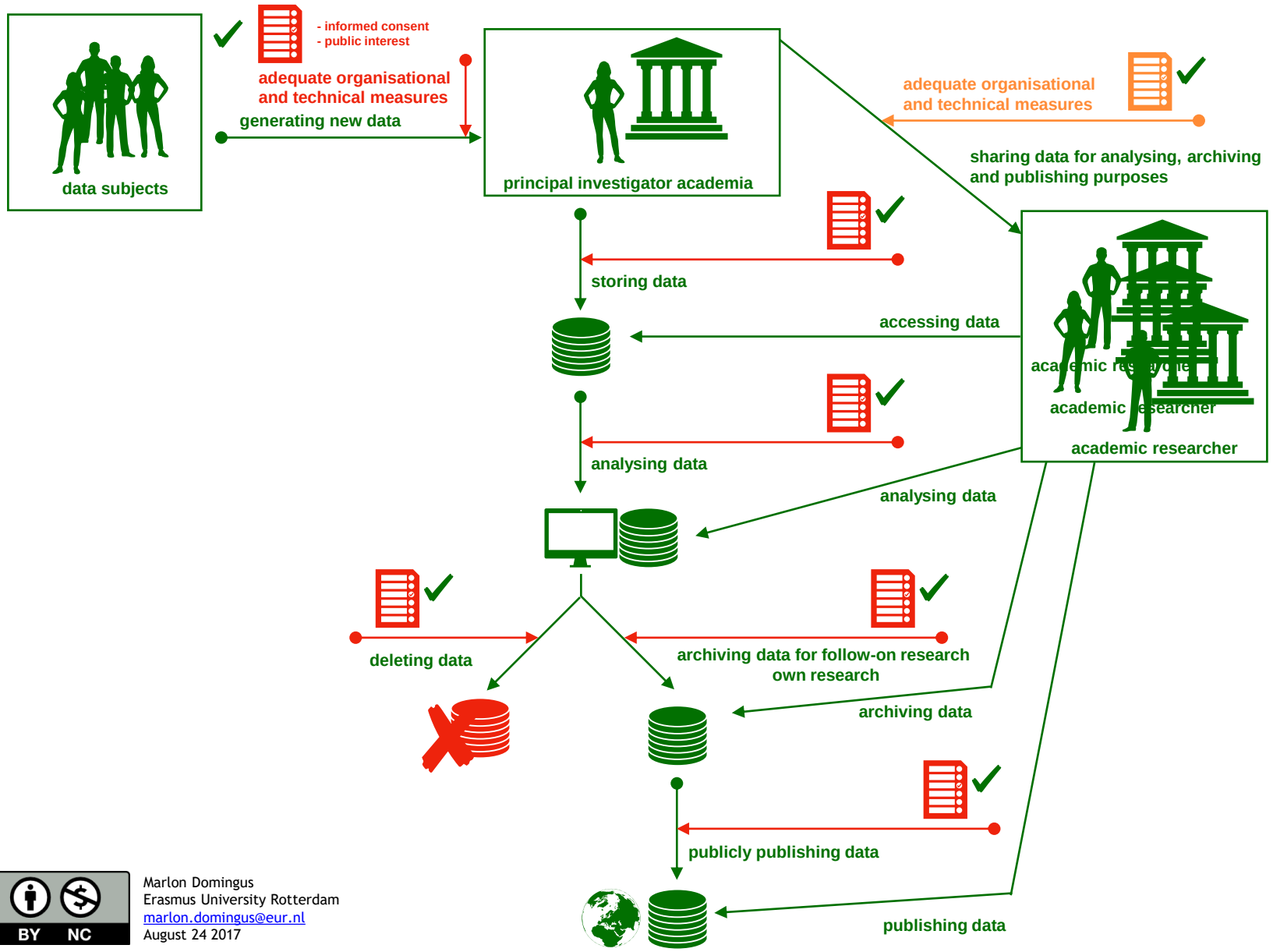
Based on Generated Data from Data Subjects



Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

Research Scenarios and the General Data Protection Regulation:

4. Academic Research by an International Research Group Based on Generated Data from Data Subjects

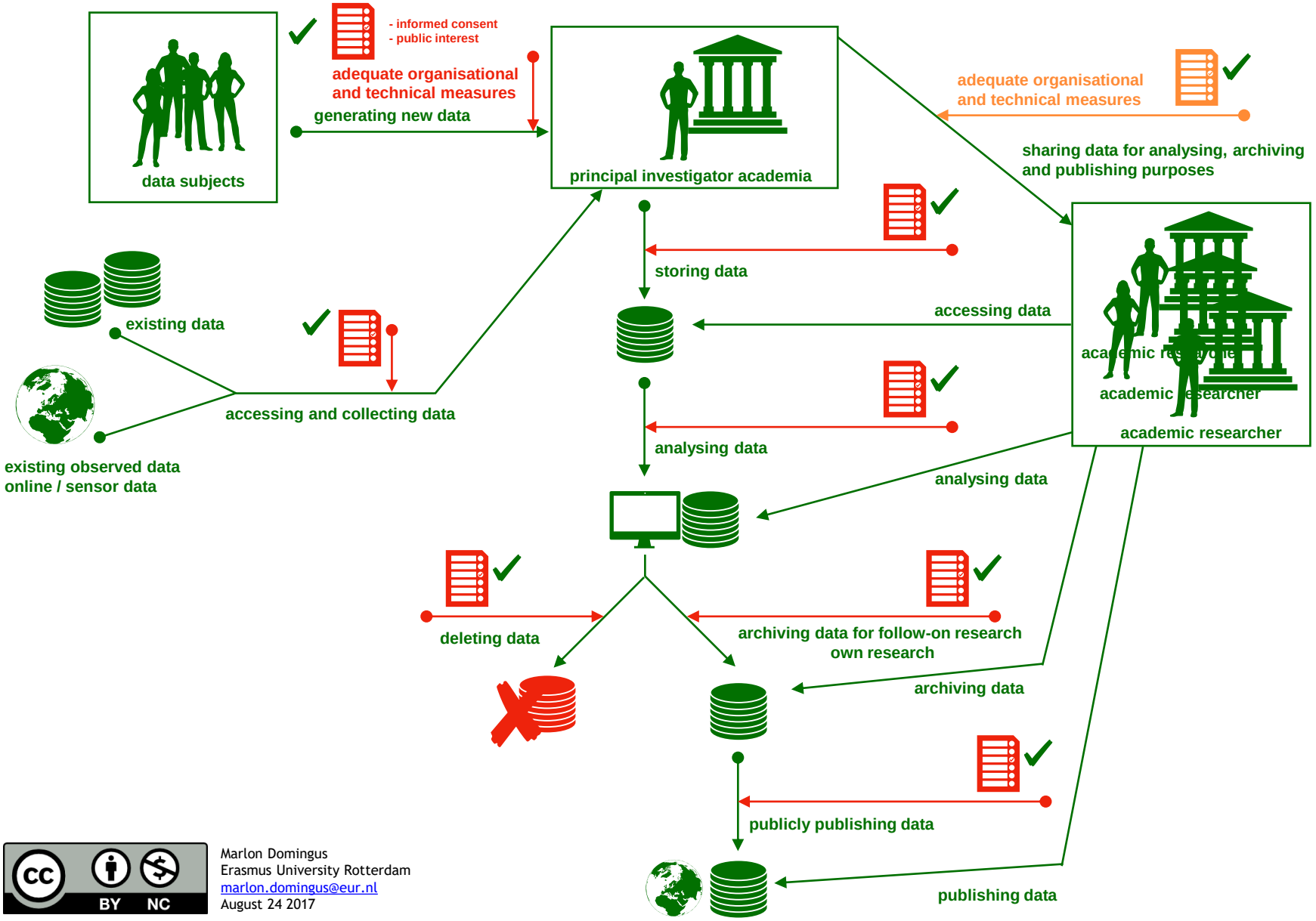


Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

Research Scenarios and the General Data Protection Regulation:

5. Academic Research by an International Research Group

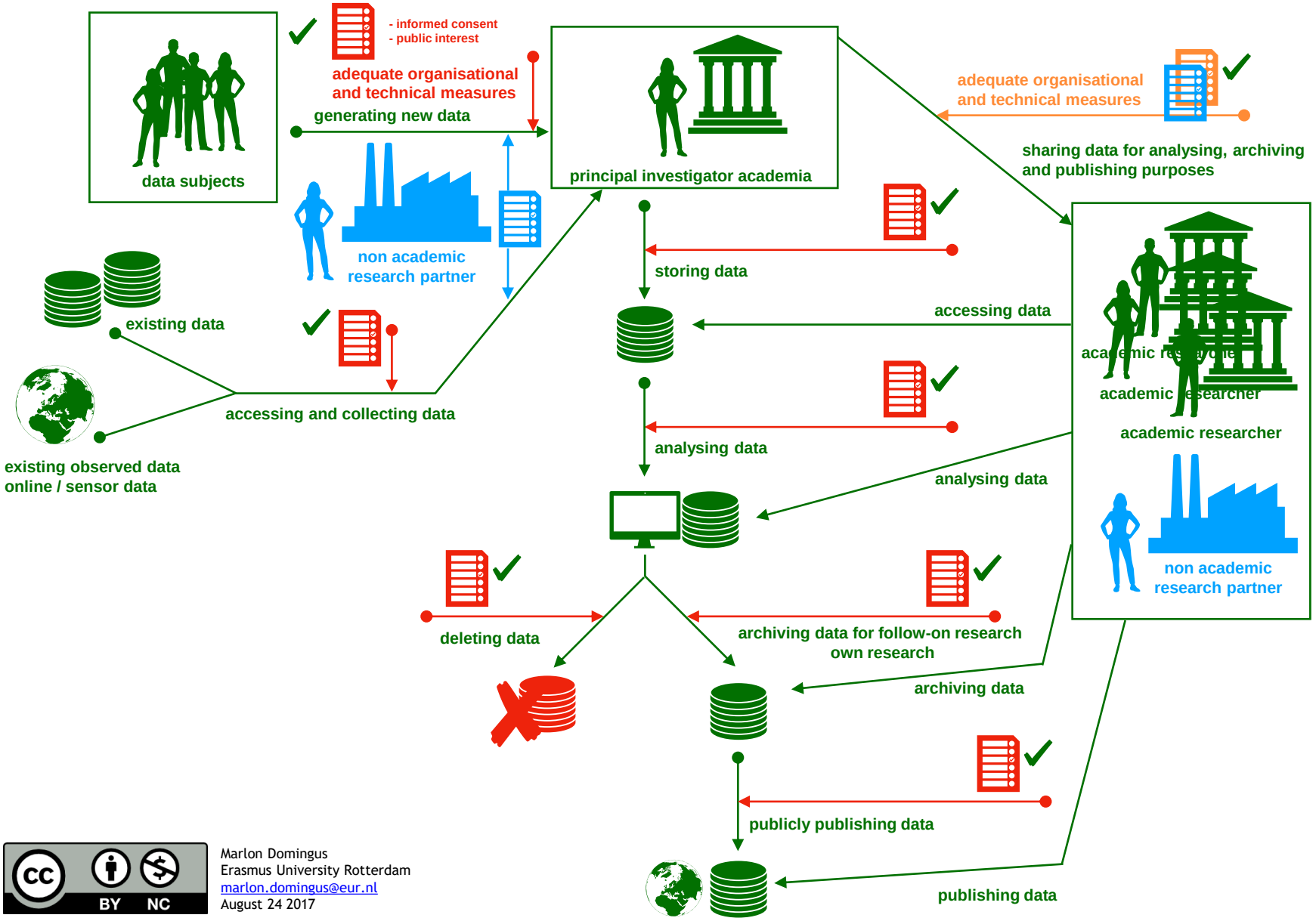
Based on Generated Data from Data Subjects Combined With Existing Data



Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

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

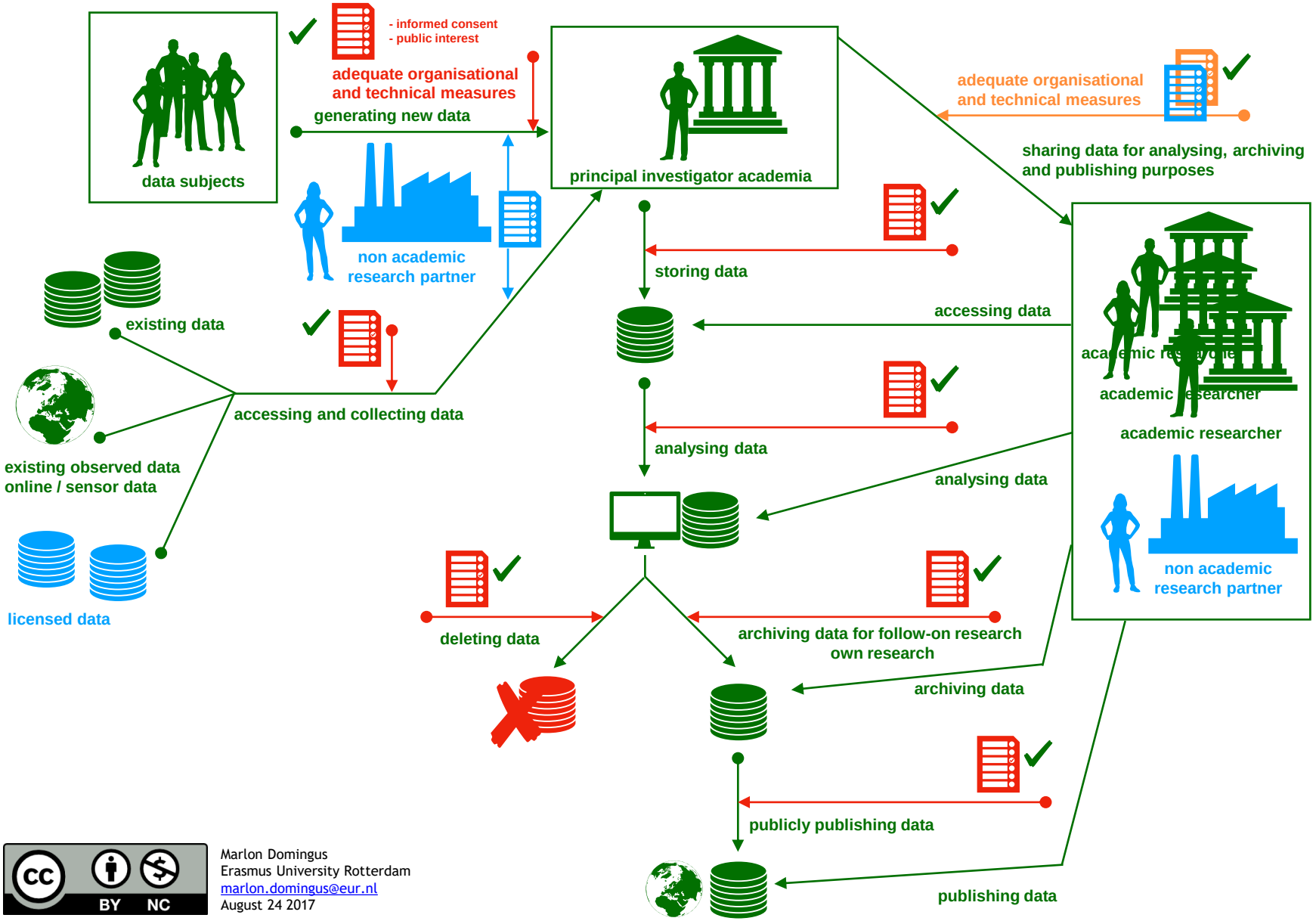


Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

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

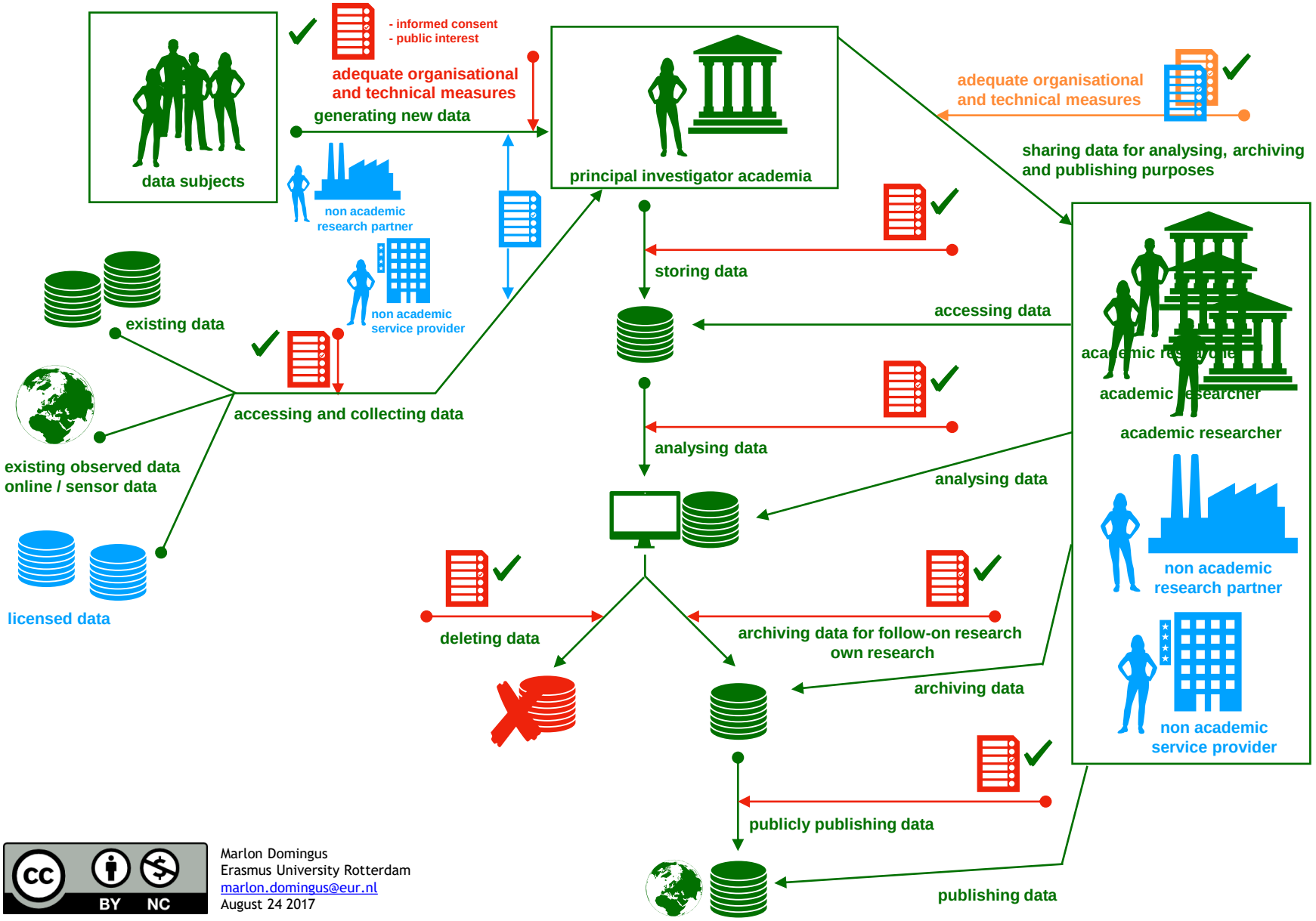


Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

Research Scenarios and the General Data Protection Regulation:

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

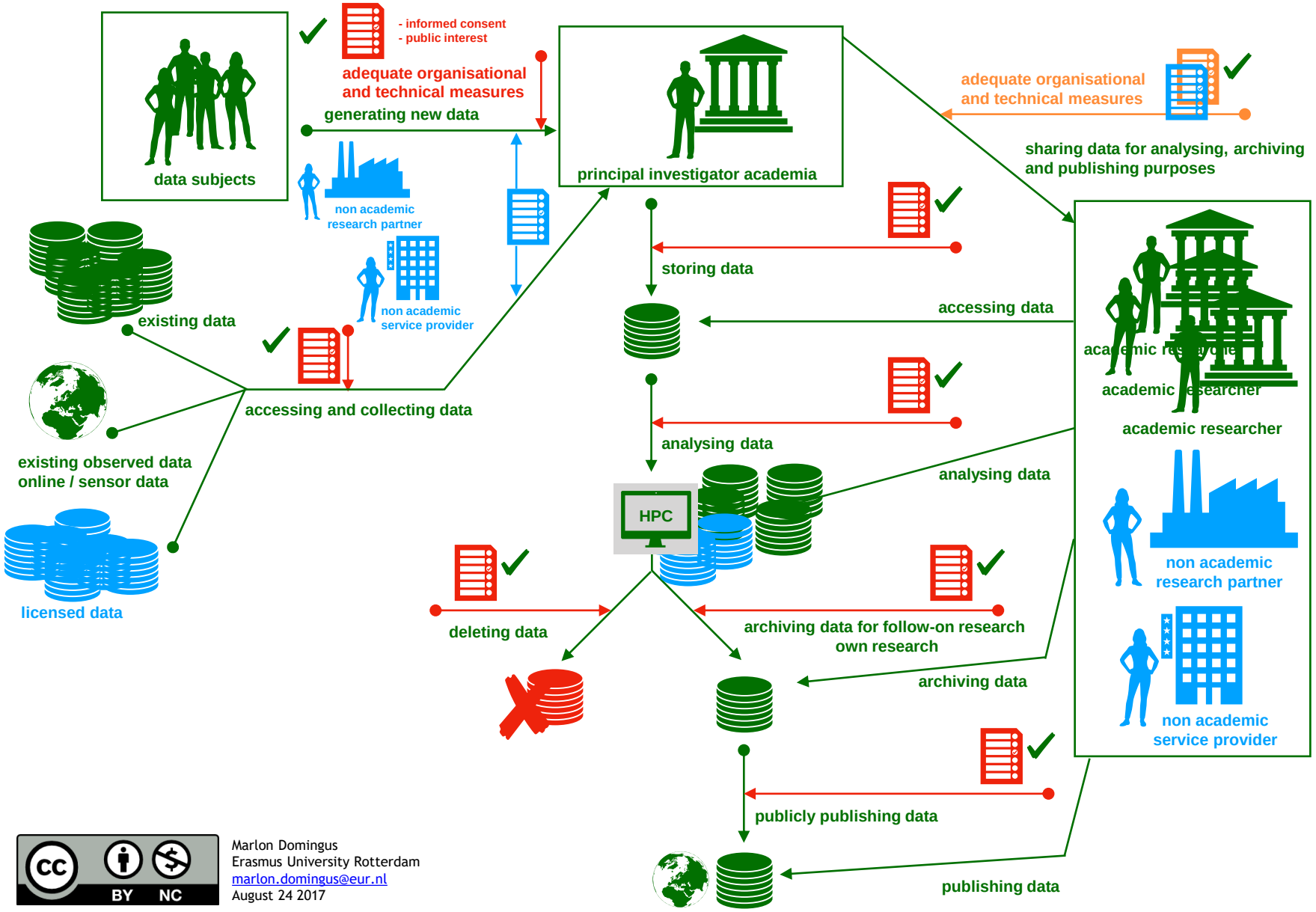
Based on Generated Data from Data Subjects Combined With Existing Data and Commercial Data



Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

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



Marlon Domingus
Erasmus University Rotterdam
marlon.domingus@eur.nl
August 24 2017

Research Scenario 1: Individual Academic Research Based on Existing CBS MicroData: Privacy Principles and Corresponding Specific Actions

action	description	generic actions	corresponding actions
further processing of existing personal data	Further processing for archiving purposes in the public interest, scientific or historical research purposes.	access control, permission control, logging and monitoring of mutations	- The microdata are to be used solely for statistical purposes, i.e. not for administrative, judicial or fiscal purposes, nor for control purposes against individuals, companies or institutions. - Permission: only you via personal token and username / password - Access: only you via Remote Access terminal and a CBS register phone (for RA SMS code) or on site (CBS) - No public wifi
storing personal data	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	de-identify data, access control, permission control, logging and monitoring of mutations, encryption of data, storage and communication	- You may not take information outside the Remote Access environment by overwriting the data, taking photos or using the function button 'printscreen'. - Always use the export folder in your account to export information from the Remote Access environment so employees of CBS can check it for disclosure risks. - In case of disclosure: delete export folder.
analysing personal data	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	de-identify data, access control, permission control, logging and monitoring of mutations, encryption of data, storage and communication	Minimum number of observations: All tabular and similar output should have at least 10 units (unweighted) underlying any cell or data point presented. Models: all modelled output should have at least 10 degrees of freedom and at least 10 units have been used to produce the model. Degrees of freedom = (number of observations) -/- (number of parameters) -/- (other restrictions of the model). Rules for frequency tables: Group disclosure: In all tabular and similar output no cell can contain more than 90 % of the total number of units in its row or column to prevent group disclosure. Rules for magnitude tables: Dominance: In alle magnitude tables and similar quantitative data, the largest contributor to a cell should not contribute more than 50 % to the total amount in the cell.
archiving personal data	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	de-identify data, access control, permission control, logging and monitoring of mutations, encryption of data, storage and communication	It is prohibited to offer microdata as output. This also means that: - The (SPSS) command LIST cases may not be used in the output. - No individual linking variables, such as RIN, RINADRES, BEID, BRIN, can be included in the output.

Research Scenario 1: Individual Academic Research Based on Existing CBS MicroData: Privacy Principles and Corresponding Specific Actions

Microdata Services – Remote Access Sanctioning Policy

	Description	Sanction[1]
Minor breach	If an action by the Remote Access (RA) user leads to an incident, this is a minor breach. An ***incident*** is a disturbing event or circumstance that may cause disruption of Statistics Netherlands' (hereinafter CBS) processes. The following is considered an incident in any case: 1. Failure to report the missing, loss or theft of: a. RA username and/or password; b. a phone that has been registered with CBS for the RA SMS code; c. RA token provided by CBS. 2. Lending of the RA token.	Warning letter to the supervisor of the researcher(s) and revocation of the privilege to post-check for the entire project for a period of up to six months. The breach shall be recorded for 3 years. If a new incident is reported within one year after the first incident in a project, these breaches shall be considered severe.
Severe breach	*A **security incident** is an incident which possibly violates the confidentiality, integrity or availability of data available within CBS.* The following breaches are considered severe in any case: 1. Bypassing the output control by copying, photographing etc. of RA aggregated data from the monitor. 2. Working in a public space. 3. Working on a computer which connects to the Remote Access via a public WiFi network (for example on trains, in cafes etc.). 4. Letting an unauthorised person work in the RA environment. 5. Otherwise violating the confidentiality of the data provided.	Revocation of login rights of the researcher involved for a period of up to one month as well as revocation of the privilege to post-check for the entire project for a period of up to six months, depending on the severeness of the breach and the intensity of the use of RA facilities. The organisation of the researcher(s) must take measures to prevent recurrence. The breach shall be recorded for 3 years. If more than one severe breach is reported within one year after completion or within 3 years during the project, these shall be considered very severe.
Very severe breach	A ***data leak*** is a security incident in which *personal or business data* have been lost or in which it cannot reasonably be ruled out that personal or business data were processed unlawfully (a full definition can be found on the website of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens). The following breaches are considered very severe in any case: 1. Bypassing the output control by copying, photographing etc. of RA *personal or business data* from the monitor. 2. Not destroying the output if post-checks indicate that the output still is not safe. Or: 3. Otherwise causing or contributing to a data leak.	Suspension of the project agreement for <u>all</u> researchers involved for a period of at least 6 months up to 1 year, depending on the severeness of the breach and the intensity of the use of RA facilities. All tokens of researchers involved are deactivated during the suspension period. After the suspension period, the organisation may re-submit a request with CBS for restarting the project. Whether the project agreement is restarted by CBS also depends on the measures taken by the organisation to prevent recurrence. The breach shall be recorded for 3 years.

Typical Issues

ODISSEI workshop, Utrecht, October 26 2017

Marlon Domingus

Erasmus University Rotterdam

Typical Issues

1. Legal Ground

2. Further Processing

3. Informed Consent

Source: Article 29 Data Protection Working Party. Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC". Adopted on 9 April 2014. Online: **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf**

Legal Ground:
Article 6 EU GDPR "Lawfulness of processing"

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
=> Article: 9

(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
=> Article: 7
=> Recital: 42, 171

(b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for **compliance with a legal obligation** to which the controller is subject;

(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;

(f) 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 which require protection of personal data, in particular where the data subject is a child.
=> Article: 13, 21
=> Recital: 113, 47

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

1. The EU General Data Protection Regulation:

Article 9 GDPR: 2. Paragraph 1 shall *not apply* if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care

Further Processing

1.3.2. De grondslag verdere verwerking voor onderzoek

De hoofdregel voor een rechtmatige verwerking is dat organisaties die persoonsgegevens verwerken een rechtmatige grondslag moeten hebben voor de verwerkingsactiviteit. Artikel 6 van de verordening geeft aan welke grondslagen mogelijk zijn. Artikel 41 van de Wet op het Centraal bureau voor de statistiek is een belangrijk voorbeeld voor een wettelijke grondslag voor verwerking van persoonsgegevens voor onderzoek. Het CBS is bevoegd om -mits er voldaan is aan maatregelen bij het CBS en de verzoeker- persoonsgegevens te verstrekken of toegankelijk te maken aan universiteiten in de zin van de WHW of andere bij wet ingestelde instellingen voor het doel van statistisch of wetenschappelijk onderzoek. Daarnaast is een verwerking bijvoorbeeld toegestaan als er toestemming van de betrokkene is of als de verwerking noodzakelijk is voor het gerechtvaardigde belang van de verantwoordelijke of een derde. De verantwoordelijke mag dan een afweging maken of verdere verwerking voor een ander doel toegestaan is. De nationale wetgever kan daarnaast in een specifieke wettelijke bepaling verdere verwerking toestaan als noodzakelijk en evenredige maatregel voor een zwaarwegend algemeen belang, zoals uitgewerkt in artikel 23 lid 1 AVG. Daarbuiten is de verdere verwerking slechts rechtmatig indien en voorzover de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is (artikel 6 (1) (f) AVG). Het verkrijgen van een nieuwe rechtmatige grondslag op grond van deze afweging mag overigens niet als de aanvankelijke grondslag berust op toestemming van betrokkenen.

Artikel 5 (1) b AVG noemt nadrukkelijk de mogelijkheid van verdere verwerking voor het doel van wetenschappelijk onderzoek.

...de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd.

Source: *Addendum 1, pg 36.* VSNU Code of conduct for using personal data in research. To appear online: http://www.vsnu.nl/en_GB/code-personal-data

Bij de grondslag verdere verwerking is het daarom geen obstakel dat het wetenschappelijk onderzoek gericht kan zijn op een ander doel. De overige criteria voor de

Informed Consent

Standaard EUR Informed Consent Formulier

versie 0.1 M. Nariman and M. Domingus, Juni 2017.
Met dank aan Daphne van de Bongardt voor praktische voorbeelden.

Vrijwilligheid	Deelname aan dit onderzoek is geheel vrijwillig. Je kunt als deelnemer jouw medewerking aan het onderzoek te allen tijde stoppen, of weigeren dat jouw gegevens voor het onderzoek mogen worden gebruikt, zonder opgaaf van redenen. Dit betekent dat als je voorafgaand aan het onderzoek besluit om af te zien van deelname aan dit onderzoek, dit dit op geen enkele wijze gevolgen voor jou zal hebben. Tevens kun je tot 5 werkdagen (bedenktijd) na het interview alsnog de toestemming intrekken die je hebt gegeven om gebruik te maken van jouw gegevens. In deze gevallen zullen jouw gegevens uit onze bestanden worden verwijderd en vernietigd. Het stopzetten van deelname heeft geen nadelige gevolgen voor jou of de eventueel reeds ontvangen vergoeding. Als je tijdens het onderzoek, na de bedenktijd van 5 werkdagen, besluit om jouw medewerking te staken, zal dat eveneens op geen enkele wijze gevolgen voor je hebben. Echter: de gegevens die u hebt verstrekt tot aan het moment waarop uw deelname stopt, zal in het onderzoek gebruikt worden, inclusief de bescherming van uw privacy zoals hierboven beschreven. Er worden uiteraard geen nieuwe gegevens verzameld of gebruikt. Als u besluit om te stoppen met deelname aan het onderzoek, of als u vragen of klachten heeft, of uw bezorgdheid kenbaar wilt maken, of een vorm van schade of ongemak vanwege het onderzoek, neemt u dan aub contact op met de onderzoeksleider: [Contactgegevens in te vullen door de onderzoeksleider]

Source: EUR Legal RDM Services- templates and guideline: https://www.eur.nl/researchmatters/research_data_management/services/rdm_legal_services/

Next Steps

ODISSEI workshop, Utrecht, October 26 2017

Marlon Domingus

Erasmus University Rotterdam

Privacy: Maturity Model

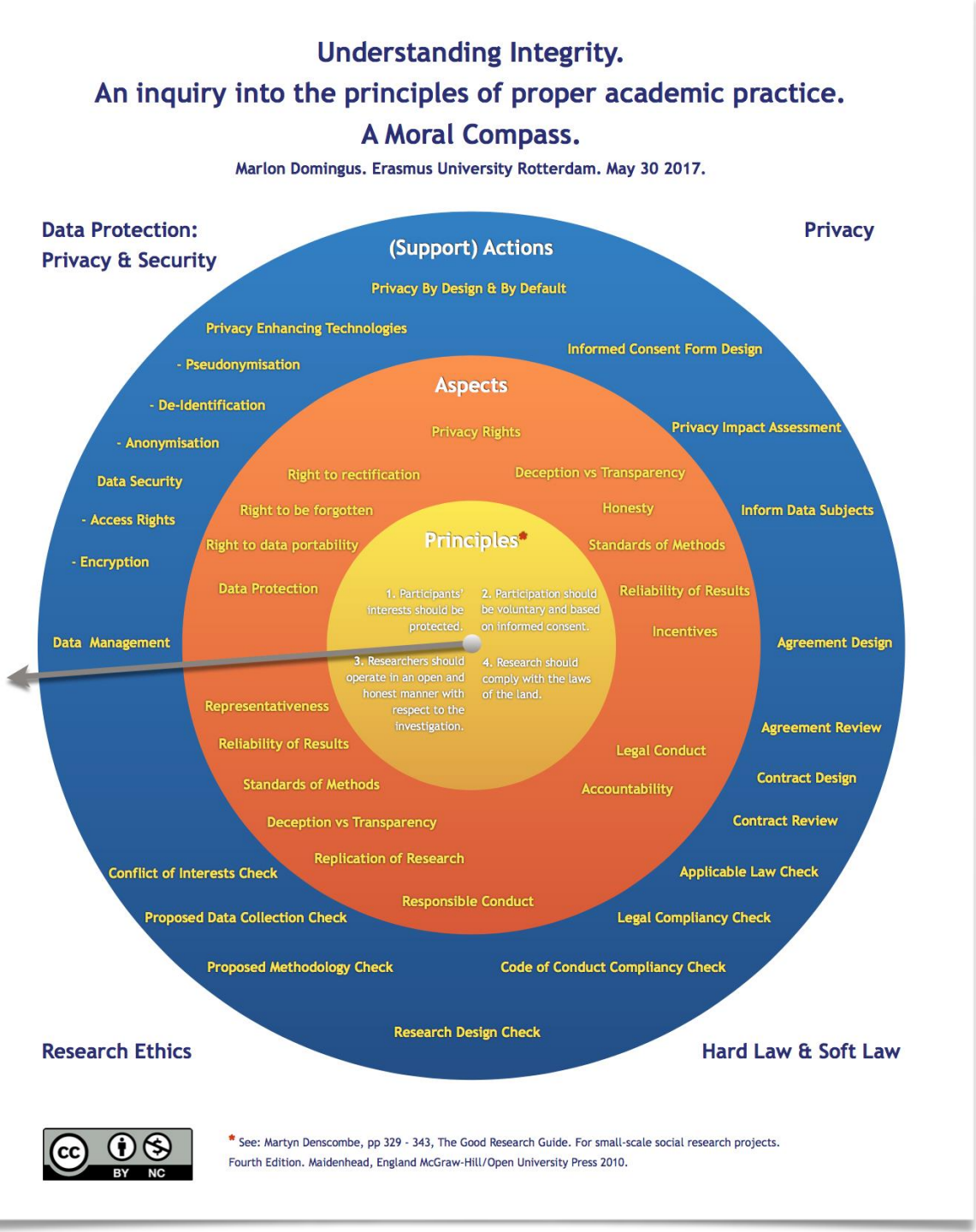
Capability Maturity Model for Safeguarding Privacy in Academic Research or: *The GDPR* Readiness Levels*

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	'What is this acronym: "GDPR" everyone is talking about?' 'I'm afraid we have to do something related to this, but don't know what, why and how.' University appoints a *Data Protection Officer* (DPO).	People across the university are meeting on a regular basis to share their practices, based on application of the *Privacy Impact Assessment* (PIA). A common language and understanding emerges on how to safeguard the privacy of data subjects in the collection, processing and sharing of personal data.	A *standard data protection process* 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.	Typical research scenarios are fully supported, GDPR compliant, as a standard service. Ongoing evaluation is in place for improving the quality of the GDPR compliancy support. Tailored support is in place for specific (new / complex) aspects in research scenarios.	GDPR is considered a starting point for the University to develop its own distinctive position. This position is *above par and* reflected in the University's policy, guidelines, principles of ethics committees, and as such recognisable both in research and research support.
Faculty	Faculty dealing with sensitive data have a heterogeneous understanding of *privacy* and *data protection*. What appropriate behaviour is, is a matter of opinions. In general 'privacy' is considered relevant, but a black box.	Faculty are discussing data protection practices from within their discipline. Faculty develop a strategy (with or without central support) to comply to various (external) data protection requirements by, e.g. research funders.	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. Solutions for generic research scenarios are available for faculty.	Faculty routinely design their research in terms of PBD and have access to a library of relevant and tailored documents to support them. Privacy is no longer considered an *external threat*, or burden, but the obvious way to be transparent on how to treat the rights of data subjects / citizens.	GDPR is considered the baseline from a research professionalism perspective. Privacy is seen as an *important strength*. By ensuring *trust* in transparant and responsible research, privacy is an enabler of societal relevance and impact of research.. Regular checks are built in, to check what to improve and how.
Legal	Legal staff is getting acquainted with the GDPR. Examining the rights, responsibilities, roles and responsibilities. Discussing available relevant (best and worst) practices.	Relevant examples, practices, instruments and relevant legal expertise are combined. Templates and model provisions are drafted to cover the relevant area. The first Register draft is created. PIA strategies are explored.	All GDPR concepts, rights and roles are clear, defined and documented in the context of academic research. Legal staff pro actively contribute to research support with *Privacy By Design and by Default* (PBD) implementations.	All roles, instruments, contracts and template wordings are in place for GDPR compliant support in various research scenarios. Legal staff act as embedded research supporters, in cooperation with the DPO and the ethical committee(s).	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.
CIO	Privacy is discussed in the context of governance and e-strategy. Privacy principles are discussed in the context of Higher Education Reference Architecture.	Privacy is included in the Business Function Model, Information Model, Business Process Model, Application Model & Platform. A privacy policy is drafted.	A privacy policy enters into force. Guidelines are distributed. An updated information security policy is implemented. CIO designs PBD strategies.	All relevant GDPR aspects are addressed in the privacy-, information security policy and governance. CIO appoints privacy officers in collaboration with Legal.	CIO is at all times willing and able to demonstrate the GDPR compliancy of information processing within the university. Checks and balances are in place to stimulate responsible behaviour.
IT	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.	Relevant *Privacy Enhancing Technologies* (PETS) 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.	A chain of PETS is implemented as basic services for research. Selection and prioritisation in collaboration with Faculty, Legal and CIO.	The baseline PETS are embedded in the working environment of researchers and supported (both individually and in workshops for faculty).	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 PET solutions.

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

Source: LCRDM. https://www1.edugroepen.nl/sites/RDM_platform/RDM_Blog/Lists/Posts/Post.aspx?ID=12



How to use the compass

In the core, the four Denscombe principles, serve as a starting point.
In the next layer, the aspects related to these principles are listed.
In the outer layer, the actions for faculty and/or research support staff are listed.

The arrow aligns the principles with the corresponding aspects and actions

Thus four quadrants appear, with a focus on the distinct aspects of research integrity. Traditionally ethics committees look at the aspects of the lower left quadrant. How to address the aspects in the rest of the compass? Suggestion: work together with the Data Protection Officer and the Legal Department for a new governing approach to assessing proper academic practices.

Questions?

drs. Marlon Domingus
Research Services
coordinator Community Research Data Management

T +31 10 4088006
E researchsupport@eur.nl
W https://www.eur.nl/researchmatters/research_data_management/ (services and templates)

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