PRIVACY

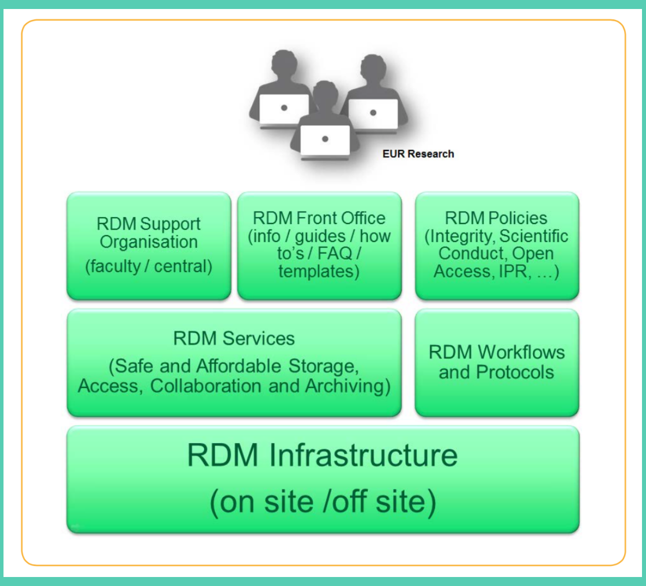
For Academic Research

COOKBOOK

a case study: Erasmus University Rotterdam

* images are clickable links *

1


EUR Research
RDM Support Organisation (faculty / central)
RDM Front Office (info / guides / how to's / FAQ / templates)
RDM Policies (Integrity, Scientific Conduct, Open Access, IPR, …)
RDM Services (Safe and Affordable Storage, Access, Collaboration and Archiving)
RDM Workflows and Protocols
RDM Infrastructure (on site /off site)

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.

2

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.

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 be held liable for the entire damage. Furthermore, penalties including administrative fines are to be 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.

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?

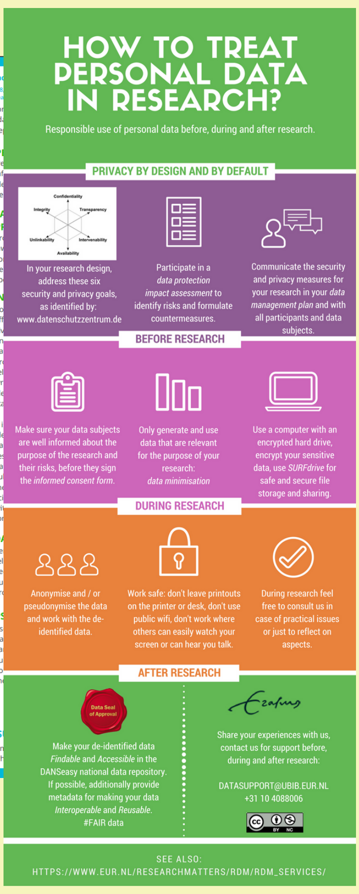
INFORMATIONAL PRIVACY
Protection of personal data
Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned.

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.

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

Confidentiality
Transparency
Intervenability
Availability
Unlinkability
Integrity

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.

BEFORE 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.

DURING 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.

AFTER RESEARCH

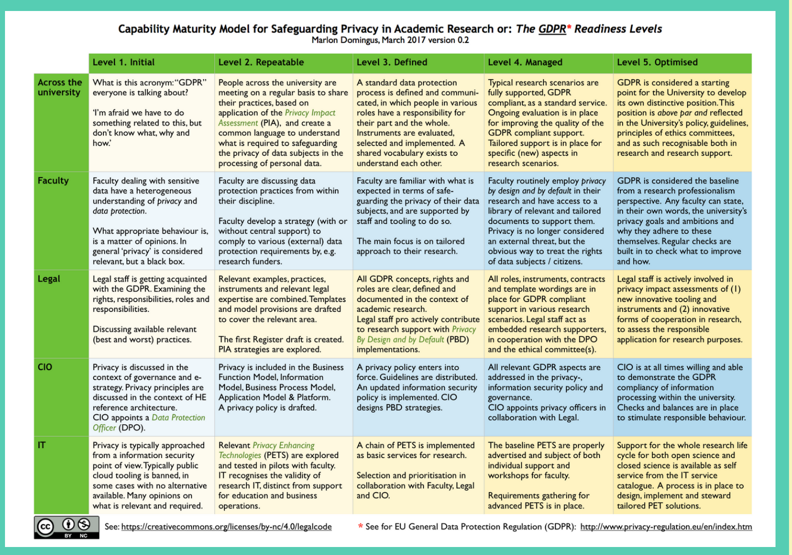
Make your de-identified data *Findable* and *Accessible* in the DANSeasy national data repository. If possible, additionally provide metadata for making your data *Interoperable* and *Reusable*. #FAIR data

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/

3



Capability Maturity Model for Safeguarding Privacy in Academic Research or: *The GDPR* Readiness Levels*
Marlon Domingus, March 2017 version 0.2

	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.'	People across the university are meeting on a regular basis to share their practices, based on application of the *Privacy Impact Assessment* (PIA), and create a common language to understand what is required to safeguarding the privacy of data subjects in the processing 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 the whole. Instruments are evaluated, selected and implemented. A shared vocabulary exists to understand each other.	Typical research scenarios are fully supported, GDPR compliant, as a standard service. Ongoing evaluation is in place for improving the quality of the GDPR compliant support. Tailored support is in place for specific (new) 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 in terms of safeguarding the privacy of their data subjects, and are supported by staff and tooling to do so. The main focus is on tailored approach to their research.	Faculty routinely employ *privacy by design and by default* in their research and have access to a library of relevant and tailored documents to support them. Privacy is no longer considered an external threat, but the obvious way to treat the rights of data subjects / citizens.	GDPR is considered the baseline from a research professionalism perspective. Any faculty can state, in their own words, the university's privacy goals and ambitions and why they adhere to these themselves. 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 HE reference architecture. CIO appoints a *Data Protection Officer* (DPO).	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, in some cases 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 IT, 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 properly advertised and subject of both individual support and workshops for faculty. Requirements gathering for advanced PETS is in place.	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: 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

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.

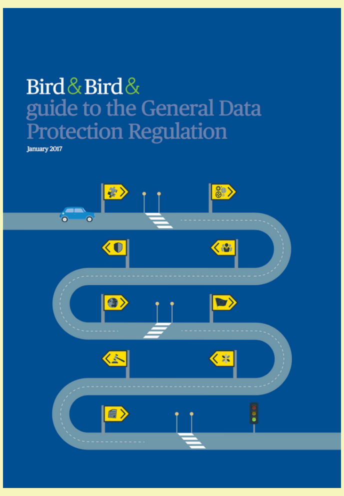
4

Define and implement a privacy strategy. Many great starting points are available.

Data protection

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

ico.



Bird & Bird & guide to the General Data Protection Regulation

January 2017

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