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