

Editorial

My university has introduced a new policy requiring that all researchers' processing of personal data be registered with, and approved by, the Ethical Review Board. Although the university presents this as a GDPR-driven measure, the policy in fact has little to do with the Regulation. As such, it is emblematic of organisations' tendency, in particular among public organisations, to interpret the GDPR in an overly strict fashion. It should instead be understood as another step in the bureaucratisation of the university, and as a consequence of management's desire to oversee and control every aspect of academic work. Risk mitigation has become a defining reality in contemporary academia. The critique that the GDPR would stifle innovation and important data processing stems not from the law itself, but from the dubious interpretation by these organisations.

The policy also defeats itself by *reductio ad absurdum*. I pointed out, for instance, that any bibliography contains personal data in the form of authors' names. This prompted a confused ad hoc response: because those names are already published, they supposedly fall outside the Board's remit—an argument which, taken seriously, would imply that data scraping is acceptable under the policy. Even setting that aside, the administrative burden is striking. Researchers must now file submissions and follow protocols for routine activities such as interviewing colleagues or writing summaries of internal workshops; meanwhile, the Board is expected to process an enormous volume of applications. Predictably, the result has been delay upon delay. Some academics have decided to abandon empirical research altogether rather than endure the same experience again; others simply find they cannot complete projects on time.

The university argues that this requirement follows from the obligation to conduct Data Protection Impact Assessments (DPIAs) and to maintain a register of processing activities. That reasoning is hard to sustain. A DPIA is intended to map risks associated with *high-risk* processing. The GDPR gives three representative examples: (1) systematic and extensive evaluation of personal aspects based on automated processing, including profiling, where decisions produce legal or similarly significant effects; (2) large-scale processing of sensitive personal data; and (3) systematic monitoring of publicly accessible areas on a large scale. Researchers, by and large, do not fall under any of these (or analogous) categories. The university notes that it should verify, for *all* processing initiatives, whether a DPIA is required. While some organisations indeed use a 'pre-DPIA' to triage which projects merit a full DPIA, the university's policy effectively treats every processing activity as requiring such a preliminary assessment—an approach that again seems absurd. The same holds for the duty to keep records of processing. That obligation concerns categories of data and their general handling (eg, 'student data are processed for these purposes, stored on this infrastructure, and re-

tained for this period'; 'employee data are processed for those purposes ...'), not a granular register of every individual processing operation.

That said, a discussion about the policy raised a more interesting issue. Article 30 paragraph 5 contains an exception for the obligation to register data processes for data controllers with less than 250 employees, unless it regards high risk processing operations. A university employee could rely on this ground; the university, however, claims that it is the data controller, not individual university employees. This aligns with an older (now obsolete) Dutch universities' code of conduct, which treated the university as controller, and with the European Data Protection Board's opinion on the concepts of controller and processor. In the same spirit, the EDPB states: 'In principle, any processing of personal data by employees which takes place within the realm of activities of an organisation may be presumed to take place under that organisation's control.'¹ A footnote adds that employees with access to personal data within an organisation are generally not controllers or processors themselves, but rather 'persons acting under the authority of the controller or of the processor' within the meaning of Article 29 GDPR. The opinion acknowledges exceptions, but offers only one example: where an employee unlawfully processes personal data for their own interests. Hence, if the university is the controller, it might argue that it is only reasonable to be informed about all processing under its responsibility, even besides the formal requirements to keep a register and conduct a DPIA for sensitive operations.

Yet it is precisely here that the approach may fail—and that a genuine exception to the 'organisation as controller' principle may arise. In most organisations, there is a clear chain of hierarchy. Policies flow from senior leadership through management to teams; employees are expected to execute those policies, not to set purposes and means on their own authority. The personal data they process are stored in organisational systems and remain there if they leave. Academia has traditionally been structurally different. Academics conceive their own projects, and the ethos of scholarship is that they should be free to pursue them; heads of department or managers are not expected to monitor, let alone control, every research idea. Moreover, when academics move to another university, they typically take their datasets with them. As a researcher, I think of a topic for my scientific paper myself, I think through which literature I need to study and additional data I need to collect, such as through interviews, and thus decide both on the means and the purposes of the data processing. In addition, many researchers, myself included, have been honoured by a personal grant. These are projects that are designed and submitted by researchers themselves; although a university has to support the submission of a grant proposal, when awarded, the researcher can take their budget to any other university.

These structural distinctions have eroded somewhat over time. As research director of my institute, I have helped craft a five-year research plan. It is broad and open to in-

¹ EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (7 July 2021) <https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf> accessed 7 December 2025.

terpretation, but it nevertheless imposes some limits. Likewise, the university has—rightly, in my view—required researchers to store personal data securely using institutional infrastructure. It has also suggested that, as employer, it holds intellectual property rights over data gathered by employees in their capacity as researchers, and thus may retain those data after an employee leaves (a claim that, fortunately, has not been implemented strictly). Even with these qualifications, the inner workings of academia remain unlike those of most other organisations. We still expect academics to be free and independent, not merely executors of a plan devised by superiors.

For that reason—both because the EDPB speaks only of ‘in principle,’ and because its opinions are not legally binding—it is worth returning to the GDPR’s definition of controller. Control depends on who determines the purposes and means of processing. In the university context, that role seems to fall primarily on the individual researcher. Each academic develops their own research question and decides what data are needed to answer it. There are exceptions—such as staff hired to work on a predefined project or line of research—but even then, an academic is, and should be, free to pursue their own scholarly vision. It is also unlikely that university and researcher should be treated as joint controllers: the university generally has no practical say over the purposes and means of individual research, nor would we want a system in which it did. Perhaps, then, it is time for the EDPB to update its opinion—or issue a new one focused specifically on data processing in universities—particularly in light of the GDPR’s extensive (and not always easy to delineate) derogations for scientific research.

It is clear from everything in the GDPR that if there is a sector where the rules of the GDPR must be interpreted flexibly, it is science: an exception to the purpose limitation principle (Article 6 paragraph 1 sub b) for scientific research, an exception to the storage limitation principle (Article 6 paragraph 1 sub e), an exception to the prohibition on processing sensitive personal data (Article 9 paragraph 2 sub j), an exception to the information obligation (Article 14 paragraph 5 sub b), an exception to the right to erasure (Article 17 paragraph 3 sub d), a special arrangement for the right to object (Article 21 paragraph 6) and a general exception provision for large parts of the GDPR in the context of scientific research (Article 89 GDPR). It bears no repeating that as per Article 1 of the GDPR, data protection seeks not only to protect the personal data of citizens, but also facilitate persons and organisations in processing personal data of citizens.

When the GDPR was adopted, the hope was that sectors would design codes of conducts through which they would give detailed interpretation on the general principles contained in the GDPR for their specific domain. This hope, however, by and large, has not materialised, the code of conduct mechanism leading an almost dormant life. Instead, national supervisory authorities and the EDPB have issued guidelines on the interpretation and implementation of data protection principles in various sectors and domains. A guideline on the interpretation and implementation of the GDPR for academia could make clear that in principle, researchers are the data controller, detail if and when a DPIA is needed, if and when data processing operations need to be reg-

istered, and suggest how the various exemptions contained in the GDPR for scientific research should be interpreted in specific cases.

*Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University, the Netherlands*