Platform Privacy - Research for a
self-determined life in the digital world

Plattform Privatheit

Michael Friedewald, Alexander Roßnagel, Christian L. Geminn and Barbara Ferrarese

INNOVATION, COMPETITION AND VALUE ORIENTATION

A European approach to data protection and digital innovation

Policy Paper

Edited by Michael Friedewald, Alexander Roßnagel, Christian Geminn and Murat Karaboga

Publisher's information

Research papers of the Platform Privacy, No. 11-en

Published by

Plattform Privatheit (Platform Privacy)
Michael Friedewald[1], Alexander Roßnagel[2,3], Christian Geminn[2], Murat Karaboga[1]
(1) Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe
(2) University of Kassel, Project Group: Constitutionally Compatible Technology Design (provet) in the Research Centre for Information Systems Design (ITeG)
(3) Hessian Commissioner for Data Protection and Freedom of Information, Wiesbaden

Authors

Michael Friedewald[1], Alexander Roßnagel[2,3], Christian Geminn[2], Barbara Ferrarese[1]

(1) Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe
(2) University of Kassel, Project Group: Constitutionally Compatible Technology Design (provet) in the Research Centre for Information Systems Design (ITeG)
(3) Hessian Commissioner for Data Protection and Freedom of Information, Wiesbaden

Acknowledgements

A draft version of this policy paper was submitted to the Advisory Board of Plattform Privatheit for consultation. The authors thank the members of the Advisory Board for their detailed comments, critical observations and suggestions, which informed the revision.
Special thanks are due to Professor Thomas Hess and Fynn Kunter of Ludwig Maximilian University of Munich for additional research and expert comments.

Series

ISSN (Print)	2199-8906
ISSN (Online)	2199-8914
DOI	10.24406/publica-10016

Publication

October 2026, 1st Edition
Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe

Recommended citation

Friedewald, M. et al. (2026): Innovation, Competition and Value Orientation: A European Approach to Data Protection and Digital Innovation. Policy Paper. Research paper of the Platform Privacy, No. 11-en. Karlsruhe: Fraunhofer ISI.

Notes

This work is licensed under a Creative Commons Attribution - NonCommercial-NoDerivatives 4.0 International license.
The information has been compiled to the best of the authors' knowledge and beliefs in accordance with the principles of good scientific practice. The authors assume that the information in this report is accurate, complete and up to date, but do not accept liability for any errors, explicit or implied. The opinions expressed in this document do not necessarily reflect those of the client.

1 Introduction

Germany and Europe are at a crossroads: In terms of future-oriented digital technologies such as artificial intelligence (AI), cloud infrastructures, and quantum computing, there is a risk of falling behind China and the U.S., with consequences for competitiveness, prosperity and geopolitical capacity to act. Some sectors of the business community and the political sphere are calling for a change of course, less regulation, less bureaucracy, and more entrepreneurial freedom. In particular, the General Data Protection Regulation (GDPR) is often depicted as "putting the brakes on innovation". Given this situation, how can we shape policies in Germany and Europe that do not pit data protection against economic innovation, but rather combine them in a values-based approach?

This policy paper demonstrates that such a policy is necessary, advisable and feasible. It is based on key empirical findings but does not claim to provide a comprehensive scientific assessment.[1] The conclusion is that value orientation should not ignore economic interests; real conflicts of interest between data protection and economic performance must be openly acknowledged and weighed up in the policymaking process.

2 What We Know: Framework Conditions for Successful Digital Innovations in Germany and Europe

Freedom of research and data protection: What are the conflicts of interest?

Research and development and the innovations they drive are prerequisites for economic and social development. Key technologies such as AI determine the success of entire economies. Germany and Europe need to actively shape this development and are dependent on the broadest possible access to data, because data-driven knowledge generation relies on extensive and diverse data sets. Yet this is precisely where a conflict of interest arises: When it comes to personal data, data protection safeguards individual and collective informational self-determination and deliberately limits the use of personal data. Both positions are enshrined as fundamental rights and must be balanced in a way that does equal justice to both the freedom of research and the protection of personality rights.

While data protection regulations are often perceived as an obstacle to the freedom of research, scientific studies paint a more nuanced picture of the effects of data protection on research, particularly in medicine and AI. An international research team led by data protection experts from the University of Leuven in Belgium conducted a broad-based survey of clinical research stakeholders from 25 EU countries, including data protection officers, physicians, and ethics committees. It found that the greatest challenge for medical research is not the GDPR itself, but the lack of harmonization in its interpretation by national authorities and institutions. A group of Finnish researchers reached a similar conclusion. They analysed the number of approved research permits over a period of nearly ten years and found that the introduction of the GDPR in 2018 had no measurable negative effect on register-based medical research. It was a 2020 national follow-up law on the secondary use of health data, which entailed significantly more bureaucracy, that led to a 47% drop in the number of approved data permits.

[1] For a detailed discussion, empirical evidence and the sources used, see Friedewald, Michael, Alexander Roßnagel, and Christian L. Geminn. 2026. *Innovation, Wettbewerb und Werteorientierung: Datenschutz- und Digitalregulierung zwischen Innovationshemmnis und Standortvorteil*. Forschungsberichte der Plattform Privatheit No. 9. Plattform Privatheit. https://doi.org/10.24406/publica-9910.

One finding often overlooked in the debate concerns researchers' reluctance to share their own data or to use data shared by others, even where the political will and technical infrastructure to do so exist. Whether this reluctance stems primarily from data protection requirements or is due to deeper-rooted cultural and structural factors cannot be conclusively determined empirically. Anyone identifying data protection law as the sole barrier to insufficient data sharing is therefore overestimating what legal reforms alone can achieve.

The GDPR already offers considerable leeway through its research privileges—it facilitates changes in purpose, allows for the processing of particularly sensitive data, and limits information and deletion obligations for research purposes. The key challenges lie in harmonizing procedures for cross-border collaborations and establishing practical rules for international data transfers.

It should be noted that the problem regarding data transfers to the U.S. arising from the European Union's Court of Justice's Schrems II ruling has (for the time being) been largely resolved since 2023 by the EU-U.S. Data Privacy Framework, although recent developments in the U.S. are raising new questions about its validity. There are adequacy decisions in place for other key research partner countries and standard contractual clauses are available for others. The legal hurdles to international research data transfers are thus lower than is often suggested in the debate.

Data maximization as a driver of innovation: promises and limitations

Modern AI systems and data-intensive business models promise efficiency gains across all sectors by analysing vast quantities of data. Underlying this is the widespread belief that more is better: more data mean a better basis on which to work. Many view the data protection requirement of data minimization as a structural contradiction to innovation.

Upon closer examination, this sweeping assertion needs to be differentiated. The marginal returns from simply adding large amounts of uncurated data decline systematically; erroneous or distorted data on a large scale produce incorrect results. What matters far more is the quality, accuracy and exclusivity of training data. This is also confirmed by an American study that surveyed 325 AI startups worldwide: Startups with proprietary training data, i.e., data they collected themselves and that are not publicly available, receive significantly more venture capital than those that rely entirely on publicly available datasets. This finding calls into question the political argument that less strictly regulated data access would automatically benefit AI startups, because if all companies had access to the same data pools, there would be no innovation advantage to distinguish them. Furthermore, at present, AI development is increasingly moving toward more data-efficient methods, driven not primarily by data protection, but by economic factors such as computing power requirements and energy consumption. These methods, including federated learning, synthetic data, and transfer learning, enable high-performance applications even with limited datasets.

Unintended technology impacts: A call to action, not an excuse

Those opposed to regulation often argue that innovation impacts are unpredictable anyway, so it should be left up to the market to decide. However, experiences with data-based business models show the opposite: A lack of regulation does not maximize benefits; it shifts the risks onto the shoulders of less well-protected groups and leads to discrimination, data misuse and market concentration. The underlying regulatory dilemma is real: Early regulation is difficult to justify due to a lack of knowledge about its impacts; late regulation is costly and time-consuming. However, this is not an argument against regulation, but rather one in favour of adaptive approaches.

Research therefore recommends risk-based tools that integrate foresight into the innovation process. Regulatory sandboxes allow innovations to be tested under supervision before the final rules are put in place. Impact assessments of data protection and fundamental rights oblige organiza-

tions to evaluate the risks to fundamental rights *before* deploying a technology, not after the damage has already been done. The principle of values-based technology design turns this design mandate into product development. Data protection requirements are incorporated into the system architecture before development begins. This prevents structural vulnerabilities and reduces long-term modification costs. Regulation thus shifts from being a reactive intervention to a proactive design framework.

Is the GDPR putting the brakes on innovation? An empirical assessment

Whether the GDPR substantially hinders the innovative capacity of the German and European economies cannot be clearly determined based on the available empirical evidence. The survey data from Bitkom paint an alarming picture at first glance: In 2024, just under two-thirds of the companies surveyed had either discontinued or failed to launch at least one innovation project due to GDPR requirements, and this is especially common in the field of artificial intelligence. Scientific studies based on the Mannheim Innovation Panel arrive at a more moderate conclusion: While nearly all companies are affected by the GDPR, only 36.4% report direct impacts on their innovation activities—primarily in the ICT sector and knowledge-intensive services. [2] The share of revenue from product innovations remained constant at these companies following the introduction of the GDPR. However, there was a shift from radical to incremental innovations—companies prioritized adapting existing products to GDPR requirements at the expense of new ones. Whether this effect is temporary is still an open empirical question. As long as radical innovations continue to decline, long-term competitiveness is at risk, especially in AI. Policymakers must design legal certainty in a way that still makes radical innovations possible.

Looking beyond the German economy, international evidence points to even more pronounced effects. Analyses of app marketplaces and venture capital flows reveal a noticeable decline in new market entries as well as declining international investments in European digital companies in the years following the introduction of the GDPR. Such effects tend to favour large, data-rich platform companies rather than smaller and younger providers. Larger companies were able to adapt without compromising on radical innovations. The fact that small and young enterprises are more severely affected by the GDPR in terms of their ability to innovate points to the need for reform. The EU Commission's omnibus reform proposal of November 19, 2025, addresses this issue.

Bureaucracy and financial penalties: How much does the GDPR cost?

In the Bitkom survey, nearly all companies (97%) report a high bureaucratic burden due to data protection requirements. However, the argument frequently made in the debate - that European companies bear the compliance costs unilaterally compared to non-European competitors - misses the point regarding the legal situation, since the GDPR applies without distinction to all companies operating in the European market, regardless of whether their headquarters are in Europe or elsewhere. No specific competitive disadvantage for European companies can be inferred from this. The crucial dividing line is not based on company size, but on the actual processing risk involved. Any company processing sensitive data on a large scale or for high-risk purposes must comply with stricter requirements, regardless of its size. Smaller companies therefore face a disproportionate burden because the GDPR makes little distinction based on risk, and compliance costs weigh more heavily on them relative to their resource base. An analysis of cloud computing usage data reveals that the additional costs of data use resulting from the GDPR rise significantly as company size decreases, even if this has only a minor impact on total production costs. This is where the real need for reform lies.

[2] These two findings are not mutually exclusive: Company surveys measure subjective perceptions of burden and project decisions; the Mannheim Panel measures objective changes in output. Both perspectives are valid and complement each other.

Another point of criticism concerns the significantly higher range of fines permitted under the GDPR. Once again, it is evident that the pattern of costs depends on company size, albeit in the opposite direction. The median of the 3,000 fines imposed since 2018 is approximately 6,000 euros. The highest penalties, exceeding 200 million euros, have been exclusively directed at large international digital corporations. This does not indicate a systematic threat to economic viability. The stricter sanctions are a response to real threats in digitalized markets posed by large, primarily non-European providers, who do not consider themselves bound by European law. They are not an expression of hostility toward innovation by European providers.

3 What We Want: Values as a Benchmark for Innovation

Who decides which innovations are desirable?

Not every innovation is conducive to social cohesion. Innovations can have a disruptive effect in a negative sense and cause harm to society as a whole. What matters is not the innovation itself, but its effects.

Innovations must be desirable for society. Their acceptability requires compatibility with the existing value system: human dignity, self-determination, democratic control, and the rule of law, including the protection of personal data and respect for privacy. This requires a normative framework within which technology is developed. Innovations will only strengthen the foundation of values if this is taken into account in the innovation process in the form of sector-specific design principles. Letting markets decide on their own is a normative position, not a law of nature. Those who let the markets decide, leave the distribution of risk to those stakeholders with the greatest power in terms of capital and data.

Entrepreneurial success itself has a connection to the common good: It creates jobs, ensures tax revenue, and strengthens the national economy as a whole; this is the fundamental mechanism of market economies. Problems arise if profit becomes the *sole* benchmark for evaluation and other values, such as the protection of fundamental rights, fair competition, and social cohesion, are systematically sidelined. It is incompatible with a values-based approach if innovation is geared exclusively toward profit. This becomes particularly clear in the case of services that are based on the unrestricted use of all data freely available on the internet and that dominate the market in Europe, even though the conditions under which they were created would not be legally permissible here. In times when an economy is weak, governments often try to stimulate the market through radical deregulation. The danger is that this will lead to new problems in the medium term. However, the goal cannot be to replace problematic non-European social media platforms with equally problematic European counterparts. The goal should be to develop genuine European alternatives that are guided by European values through transparency, interoperability, user autonomy, and responsible data handling, but are still competitive.

Technology impact assessment makes uncertainty manageable by showing which combinations of technologies and business models lead to which effects. The data protection and fundamental rights impact assessments required by the GDPR and the AI Act for high-risk processing ensure that organizations examine whether fundamental rights are at risk before deploying a technology, rather than waiting until afterward. This precautionary principle enables action to be taken even in the face of uncertainty when serious harm is imminent. This does not mean a blanket ban on innovation, but rather clear boundaries when fundamental rights are at stake. The principle of "data protection and protection of fundamental rights by design," required by the GDPR and the AI Act, makes this protective function a design requirement from the very beginning. This results in technical solutions that combine data protection and the protection of fundamental rights with economic benefits, rather than treating them as opposites.

Freedom of research: A privilege, but not an unconditional one

Freedom of research is part of the canon of European values. Research is in the public interest; the conditions necessary for its success must be ensured. However, this right to freedom does not permit the research process to infringe upon the fundamental rights of others. Research must respect trade secrets and must not violate the dignity or informational self-determination of the individuals concerned. The Charter of Fundamental Rights of the European Union stipulates that personal data may only be processed with consent or on a legal basis.

In this context, the differences between research and innovation must be taken into account. Scientific research requires considerable freedom for experimentation. The research process rarely leads to irreversible effects. The GDPR takes this into account by granting research purposes greater privileges than any other purposes, including making it easier to change purpose, providing exemptions from information obligations, erasure obligations, and the right to object, as well as exceptions to the data minimization principle. The term "research" is deliberately defined very broadly and also encompasses applied research, technological development, and privately funded research. Even if a company pursues economic goals, its research does not lose this special status, provided that it also benefits society.

Research is therefore the most highly privileged processing activity in the entire field of data protection law. The fact that this privileged status is nevertheless insufficient in practice is not due to substantive law, but rather its implementation. Lack of harmonization among Member States, and a shortage of local legal expertise result in an overcautious reluctance to engage in research projects, as well as bureaucratic hurdles in cross-border cooperation. The need for action is therefore not directed at lowering the level of protection, but rather at providing legal certainty, standardization, and practical procedures.

Digital sovereignty: Data protection as the foundation of German and European self-determination

Digital sovereignty and resilience are essential for security, competitiveness, democracy and the protection of fundamental rights. Which values are important to Europe and how these are implemented can only be determined by constitutional bodies through democratic processes. Neither foreign governments nor global digital corporations should be allowed to exert decisive influence here.

Data protection is both the goal and the tool in this regard. The law on basic rights obliges the EU to protect citizens against any unauthorized interference, even if their data are processed in third countries. Digital self-determination does not mean isolation. On the contrary. Europe deliberately relies on cooperation with partners who guarantee comparable standards of protection. The protection of data subjects does not stop at Europe's external borders but is upheld even in international data transfers.

If the Union wants to keep its promise of protection, it must insist that anyone operating on the European market complies with the applicable protection requirements. A lower level of protection in other countries must not be transferred to the EU. If, however, European SMEs are disproportionately affected by regulation while large, resource-rich companies are in a better position to adapt to new rules and exploit legal loopholes to their own advantage, this indicates the need for action. As empirical evidence shows, while larger companies are affected to a greater extent by sanctions, it is primarily the innovative activities of younger and smaller companies that are constrained by the GDPR. This suggests that large, resource-rich companies are better able to mitigate the legal and financial risks of non-compliance than smaller ones; a structural advantage that exists regardless of whether there is a deliberate strategy of non-compliance with the law.

Trust as a competitive advantage: Opportunities and limits

Values-based design can become a competitive factor in its own right. The European Commission based the justification for the GDPR on the argument that stricter data protection would strengthen trust and foster growth. But is there any empirical evidence of this correlation?

The evidence is not conclusive: Data protection strengthens trust only under certain conditions: rules have to be comprehensible, data subjects need genuine choices, laws must be credibly enforced, and the requirements must be aligned to the respective risk.

The attitude of citizens is contradictory. Many express strong concerns about data protection, but still use data-intensive services, a phenomenon known as the 'privacy paradox'. There is little empirical evidence that the GDPR has actually strengthened user trust. A Eurobarometer survey showed that 81% of Europeans said they have no or only partial control over their online data. According to studies, even the limited gain in trust has so far mainly benefited non-European providers. In areas where the perceived risk is high, such as health and finance, credible data protection is practically a prerequisite for acceptance. In other contexts, such as social media and search engines, convenient and cost-free services prevail despite weak data protection.

For businesses, a study by the German Economic Institute (IW) shows that innovative companies assess the GDPR as a competitive advantage much more frequently than non-innovative ones. In the business-to-business (B2B) sector, data protection compliance is increasingly regarded as an indicator of professional risk management.

An innovation policy guided by social values must consider these differences. In risk-sensitive areas, such as health, finances and public-sector data processing, policymakers should prioritize the credible enforcement of high data protection standards - as this has proven to result in a trust dividend. In areas with lower data sensitivity, on the other hand, requirements should be simplified based on risk. A low processing risk should also mean less bureaucratic effort. It is not enough to make the sweeping claim that data protection creates trust and then use this to justify every regulation and bureaucratic burden.

However, it is also true that data protection is not a cost-free competitive advantage. It generates real compliance costs, ties up development resources and can, especially in young and small enterprises, temporarily constrain innovation capacities. This trade-off between protection goals and economic performance cannot be ignored; it must be made transparent at the policy level and consciously weighed up. This is precisely what a credible argument in favor of values-oriented innovation requires: clearly identify the conflicting goals and then show why the selected regulation framework is still justified and how it can be shaped.

4 What Should We Do? Combine Innovation and Value Orientation in a Practical Way

Europe needs a coherent strategy that does not treat innovation support and value orientation as opposites but rather as complementary elements of a European approach to digital policy. The following strategic steps are particularly important:

Ease the burden on SMEs using a risk-based approach: Producer responsibility instead of user obligation

As the majority of SMEs process low-risk data but are still subject to the same documentation and burden of proof requirements as high-risk processing, in future, the scope of these obligations should be oriented to a greater extent on the actual processing risk involved and not on company

size. Following the example of the Cyber Resilience Act and the AI Act, it is the manufacturers and providers of standard IT solutions that should be made responsible. They are best placed to integrate data protection requirements into their products in a cost-effective way and to provide users with proof of compliance such as sample processing inventories or templates for data protection impact assessments. This would ease the burden on the vast majority of SMEs without lowering the level of protection where this remains objectively necessary.

Actively correct distributional effects: From the 'Brussels effect' to economic advantage

European data protection standards function as an international benchmark (the so-called 'Brussels effect'), but so far European companies have not automatically benefited from this. The GDPR has triggered new markets for privacy-enhancing technologies (PETs) and compliance software, but the GDPR's innovation-promoting effect has not been proven empirically. The EU must therefore actively strengthen the additional support for technology transfer and scale up the support for PET providers, combined with critically reviewing the strategic takeovers of European start-ups by non-European players with deep pockets.

Scale-up data-efficient AI and data protection technology as a European growth area

Because Article 25 of the GDPR and Article 27 of the AI Act make the protection of data and fundamental rights a design requirement from the outset, structural weak points can be avoided from the start and the costs for subsequent reworking and corrections can be reduced. Europe should make greater use of this advantage because it and, Germany, in particular, have international research strengths in cryptography, formal methods and IT security that so far have rarely been turned into marketable products.

Instead of trying to catch up with large, data-maximizing AI models, Europe should target data-efficient methods that comply with fundamental rights, supported by a public procurement policy that prioritizes products with proven data protection and security design and in this way help European providers to become more visible internationally. As data protection and IT security complement and do not fundamentally contradict each other here, "Made in Europe" could become an internationally recognized mark of quality on this basis.

Consistent use and practical expansion of the research privilege

Since the GDPR already grants research numerous exemptions, this legal leeway should be leveraged more consistently rather than demanding ever more privileges. The guidelines at the 2024 German Data Protection Conference and those of the European Data Protection Board from April 2026 clearly outline which types of research - including industrial research - benefit from privileges. The planned Digital Omnibus will bring additional simplifications and legal certainty for research.

In addition, regulatory sandboxes should be expanded more consistently and used to test which risks are associated with innovations and how these can be minimized or avoided. However, they must be linked to clear conditions such as public transparency and independent oversight and explicitly exclude high-risk areas such as biometric surveillance.

Develop impact-based regulation that is capable of learning

Data protection should not be treated as a one-off compliance project, but rather as a continuous process that is able to learn. Regular evaluation of the GDPR (Article 97) should therefore explicitly look at innovation impacts and distributional effects - who pays and who benefits – rather than being limited to formal implementation. Which innovation risks a society is prepared to take remains a democratic decision that must not be left to those stakeholders wielding the greatest power in terms of capital and data.

5 Conclusions

The claim that less data protection regulation leads to more innovation is too simplistic. The GDPR is neither a general obstacle to innovation nor does it offer an automatic competitive advantage. Its effects depend on company size, sector and type of innovation, and have not yet been conclusively determined by scientific research. Data quality and exclusivity are what matter for the success of data-driven innovations, not data maximization.

Innovation is not an end in itself, but must serve the common good, not just a select few. If it does not, in the long term, the risks include declining social acceptance and increasing concentration of economic and political power, risks that forward-looking policymakers should avoid. Innovation must be compatible with Europe's fundamental values. A European approach that is viable for the future requires:

1) Consistent use and targeted expansion of research privileges.
2) Embedding data protection as a design and innovation principle and offering strategic support to PETs and data-efficient AI.
3) Establishing data protection governance as a management responsibility and easing the burden on SMEs using risk-based differentiation.
4) Designing industry policy so that Europe not only makes the rules but also benefits economically from its own standards.
5) Effectively enforcing regulations such as the General Data Protection Regulation (GDPR) and the AI Act across all market participants to enable genuine and fair competition within the EU; and
6) Understanding regulation as an adaptive process whose impacts on innovation and whose distributional effects are regularly reviewed and revised.

This will enable an approach to innovation that regards compliance with fundamental rights as a mark of quality.

Plattform Privatheit

With funding from the:

Federal Ministry of Research, Technology and Space

Participating institutions

Fraunhofer ISI

Natur Technik Kultur Gesellschaft UNIKASSEL VERSITÄT