# Control the Risks, Not the Processing

DANIEL GUAGNIN*, Institut für Kooperationsmanagement und interdisziplinäre Forschung, Germany
JÖRG POHLE*, Alexander von Humboldt Institute for Internet and Society, Germany

## 1 Introduction

It's long been evident that the world of consent and control is in crisis. When the call for position papers poses its first two questions – how to understand the "context of privacy decisions" and what is "all the relevant information to a decision" – it overlooks that there is an even more fundamental one lurking beneath: what do users, or data subjects in the context of applicable law, need to understand when making a decision, for the decision to be reasonably called 'informed'? What information has to be provided or communicated to evoke such understanding, is then only the second question. Thus, our first claim is: **We must distinguish between the understanding that is to be evoked and the information or communications that are to evoke this understanding.** Our position paper takes this distinction as its starting point, then presents the understanding that should be generated or evoked, and makes a proposal as to how it can be empirically determined whether sufficient understanding has actually been achieved.

## 2 Informed About What?

When addressing the question what data subjects need to understand for being able to make an 'informed' decision in accordance with the EU General Data Protection Regulation (GDPR), we must bear in mind that the GDPR only makes explicit statements about the understanding that is to be achieved in very few places. In many more places, the GDPR merely stipulates what information a controller must provide and in what manner. This imbalance is also reflected in research and public debate.

Across Articles 12–14 GDPR, information duties are predominantly framed as obligations to disclose facts about processing activities and their characteristics, such as actors, purposes, categories of data, retention periods or legal bases. Only in exceptional cases, such as where the controller intends to transfer personal data to a third country or international organisation but there exist no adequacy decision by the EU Commission (cf. Article 45(3) GDPR) nor appropriate safeguards (cf. Article 46 GDPR), the controller has to provide information on "possible risks of such transfers for the data subject" (Article 49(1)(a) GDPR).

More detailed information about what the European legislator and the GDPR expect data subjects to understand after they have been informed can only be found in the non-binding part of the GDPR, namely in the recitals. In Recital 65, the legislator argues for the necessity of the rights to rectification and to erasure and explains their particular importance using the example of children who grow up: "That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing." This means that the understanding to be elicited from data subjects relates to the risks associated with data processing. This is

*Both authors contributed equally to this research.

Authors' Contact Information: Daniel Guagnin, guagnin@nexusinstitut.de, Institut für Kooperationsmanagement und interdisziplinäre Forschung, Berlin, Germany; Jörg Pohle, joerg.pohle@hiig.de, Alexander von Humboldt Institute for Internet and Society, Berlin, Germany.

consistent with the explicit objective pursued by the GDPR, which is set out in Article 1: to protect people and all their fundamental rights and freedoms when processing their personal data.

Thus, our second claim is: **The understanding that must be conveyed, generated, or elicited concerns the risks to fundamental rights and freedoms — and the benefits — in connection with data processing.**

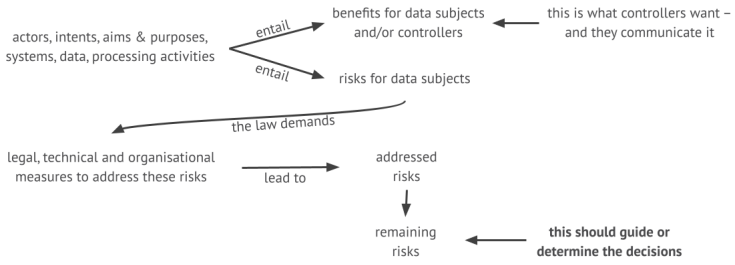
What matters for users' decision-making is not whether they can reconstruct how data is being processed, but whether they can anticipate and evaluate potential consequences of that processing for their fundamental rights and freedoms, interests as well as benefits.

Based on our distinction between the information that is provided and the understanding that is thereby elicited, we can now distinguish between two cases: 1) If data subjects are informed only about the characteristics of the data processing, they must independently infer the risks associated with it. 2) If data subjects are informed directly about the risks, they only need to understand the information that has been provided.

It is obvious that the first approach places significantly higher demands on the prior knowledge and competencies of data subjects than the second approach. This also allows the question raised in the call to be formulated more clearly: necessary and sufficient are those pieces of information that either directly convey an understanding of the risks or ensure that the risks can be easily inferred.

These considerations directly challenge the widespread belief that more information, or more detailed information, necessarily lead to better decisions.

As a side note, we would like to add that, with regard to the risks to fundamental rights and freedoms associated with data processing, a further distinction must be made between (1) the original risks that exist prior to the application of appropriate safeguards and to which many academic and public debates refer, and (2) the residual risks that remain even after the effective implementation of appropriate safeguards. We consider it self-evident that it is primarily the remaining risks that do and should guide or determine the decisions.




We will now make a proposal as to how empirically determine whether sufficient understanding has actually been achieved – or in terms of the GDPR: whether the information was provided in an effective manner (cf. Article 25(1) GDPR – data protection by design).

## 3 How to Assess 'Effectively Informed'?

Existing approaches to determining comprehensibility rely primarily on objectified metrics and assessments. These empirically measure and evaluate aspects such as word choice, the number of technical terms, text length, and similar features, with the EU digital accessibility standard EN 301 549 being an example. While this makes it possible to determine whether the information provided is formulated in clear and plain language (cf. Article 12(1) GDPR), these

approaches do not allow us to determine – and subsequently assess – whether and what the recipients of the information, i.e. the data subjects, have actually understood after reading it.

Instead, we propose a comparative approach that conceives the effectiveness of information as a matter of alignment rather than completeness. We assume that there are experts who have a substantial understanding of the risks to fundamental rights and freedoms arising from a specific processing activity when they are provided with information about that processing. This includes the ability to infer from the information not only the original risks, but also those addressed by safeguards as well as the remaining risks. If we compare the understanding generated by such experts with that of laypeople who were exposed to the same information, we can empirically determine the understanding of laypeople, i.e. data subjects.

Thus, our third claim is: **Informing is effective to the extent that lay users' risk assessments approximate expert judgments under comparable conditions.**

This shifts the challenges from determining understanding to organizing and conducting appropriate user studies with both an expert and a layperson panel and, most importantly, to the composition of the expert panel. The expert panel must be appointed based on two criteria: expertise and representation of interests. The first criterion is simple and straightforward, though far from trivial in practice: all expertise, knowledge regimes, scientific disciplines, and competencies in research areas relevant to the specific data processing activity must be covered. The second criterion stems from the recognition that data processing is characterized by conflicting interests, primarily between controllers on the one hand and data subjects on the other. Hence, we require that each dimension of expertise be represented by an equal number of experts representing conflicting interests.

## 4 What Are the Consequences?

Our proposal has significant implications not only for informed consent and the information that must be provided in that context, but also for the rights of data subjects, the exercise of those rights, and what it requires of controllers when they are to facilitate the exercise of those rights (cf. Article 12(2) GDPR): It is evident that the exercise of data subject rights is not merely about controlling data processing or intervening in data processing. Rather, the core of these rights is that, by intervening in the data processing, data subjects are able to exercise control over the risks. **This requires nothing less than a complete revolution in thinking about and designing control mechanisms and tools.**

## 5 Brief Author Biographies and Areas of Expertise and Interests

Daniel is a sociologist, with a background in computer science. Since 2010 he has done research on security, privacy and data protection. Since 2022, he is head of the research area Network and Society at nexus institute Berlin. His research interests include the interplay between technology and society, and value-sensitive design.

Jörg is a computer scientist by training, with a background in law, political science, and sociology. The last thirteen years, Jörg was a researcher at the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin, most recently as head of a research programme. His research interests include modellification, governance, and data protection by design. Since December 2025, he is an associated researcher at HIIG.

## Acknowledgments

Daniel Guagnin has received research support from the German Federal Ministry for Research, Technology and Space (BMFTR) (Grant number 16KIS1967K). Jörg Pohle has received research support from the German Federal Ministry for Research, Technology and Space (BMFTR) (Grant number 16KIS1968).