ATHENE
National Research Center for Applied Cybersecurity

Position Paper on the Second GDPR Evaluation (2024)

More Legal Certainty for Researchers: On the Need for a New Instrument in Data Protection Law

AUTHORS

Dr. iur. Annika Selzer
Fraunhofer SIT | ATHENE

Sarah Stummer, LL.M.
Fraunhofer SIT | ATHENE

Dipl. Jur. Alina Boll
Fraunhofer SIT | ATHENE

Position Paper on the Second GDPR Evaluation (2024)

More Legal Certainty for Researchers: On the Need for a New Instrument in Data Protection Law

Authors

Dr. iur. Annika Selzer
Fraunhofer SIT | ATHENE

Sarah Stummer, LL.M.
Fraunhofer SIT | ATHENE

Dipl. Jur. Alina Boll
Fraunhofer SIT | ATHENE

Translation

Joanne Lyons
Fraunhofer SIT | ATHENE

Legal Notice

Contact
National Research Center for Applied Cybersecurity ATHENE
c/o Fraunhofer-Institute for Secure Information Technology SIT
Rheinstraße 75
64295, Darmstadt

Notes
This paper received support from the Federal Ministry of Education and Research (BMBF) and the Hessian Ministry of Higher Education, Research, Science and the Arts (HMWK) as part of their joint funding for the National Research Center for Applied Cybersecurity ATHENE.

The paper reflects the authors' personal opinion.

Abstract

When conducting applied research to investigate or defend against cyberattacks, unplanned processing of personal data may occur. The data protection legislation in force in the European Union does not provide for the possibility of structuring such cases in a legally compliant manner – i.e. in which it is neither possible to plan whether a research activity will involve personal data processing, nor which categories of personal data will be processed by which data subjects and in what quantity. As a result, the implementation of applicable data protection law often encounters limits in this area, which hinders research, meaning that benefits cannot be achieved, e.g. to protect critical infrastructures from cyberattacks.

In light of this, ATHENE researchers proposed the new instrument "data protection preventive assessment"[1] in 2023 and developed it further.[2] This newly proposed instrument is intended to enable unplannable and unpredictable, but reasonably probable, personal data processing with legal certainty. Any imminent personal data processing is to be prepared by means of the newly proposed instrument for a data protection preventive assessment by first making assumptions about the possible imminent personal data processing, which shall be regarded as probable. The assumptions should be based on previous experience of similar research activities among other things. Based on this, core aspects of data protection law (including the identification of a relevant legal basis), which reflect the previously made assumptions, should be implemented before the planned research activity is commenced.

The data protection preventive assessment is thus intended to ensure data protection compliant and legally secure processing if personal data processing should occur in the course of the research activity. To ensure that core aspects of data protection law are implemented appropriately, personal data processing that is assumed to be improbable to occur (hereinafter referred to as "improbable personal data processing") should not be considered in the context of the data protection preventive assessment.[3] Should improbable personal data processing occur nonetheless, this should not be subject to fines. In the future, the applicability of the data protection preventive assessment beyond the field of research is generally conceivable and we see a significant need for this.

This position paper therefore proposes anchoring the instrument "data protection preventive assessment" in the European General Data Protection Regulation. Only then can the data protection preventive assessment ensure that applicable law and technical progress interlock sensibly and thus improve protection for society. If the data protection preventive assessment were to become part of the European data protection legal system, it would

- provide clarity for data controllers in order to be able to implement unpredictable and unplannable personal data processing in a legally secure manner on the one hand and
- provide adequate protection for the rights and freedoms of data subjects as provided for in the GDPR on the other hand.

[1] Boll, Selzer, Spiecker gen. Döhmann, *Tagesspiegel Online*.
[2] Boll, Selzer (2024) *DuD*; Boll, Stummer (2024) *DuD*; Boll, Stummer, Selzer (2024) *DuD*; Boll (2024), *DuD*.
[3] For the first three paragraphs see Boll/Selzer, *DuD* 2024.

1. Introduction

The General Data Protection Regulation – GDPR in short – will undergo its second evaluation in 2024. As part of this evaluation, the European Commission submits a report to the European Parliament and the Council of the European Union on the evaluation and review of the GDPR, in which, among other things, appropriate proposals are made to amend, adapt and/or supplement the GDPR, taking into account developments in information technology and progress in the information society (Article 97 GDPR).

We would like to take this evaluation as an opportunity to highlight what we consider a required amendment to the GDPR.

2. Problem statement

By means of the GDPR, the European legislator provides a regulatory framework for almost every conceivable form of personal data processing – i.e. the processing of people's personal information, such as their name, address, or profession. Thereby, the European legislator assumes that all personal data processing can be predicted and planned in detail before the processing takes place. However, this no longer coincides with the actual circumstances – especially in cyber security research – since personal data processing mostly isn't intended in the research in question, but the occurrence of such data processing cannot be ruled out entirely and therefore cannot always be planned.[4]

The motivation to address this topic emerged while looking at an example, in which a cyber security researcher conducts research on new attack methods on the dark web in order to develop necessary countermeasures. During his research, he may unintentionally come across lists containing stolen personal data from cyberattacks. To avoid worse, he informs the people on the list so that they can take appropriate countermeasures (e.g. resetting their password).

As the cyber security researcher is not aware of the processing as such or the amount and type of personal data and data subjects (and therefore their need for protection) before processing, it is generally impossible to plan the implementation of data protection requirements in advance in such cases. If personal data processing is not predictable or plannable, it cannot be carried out in accordance with applicable data protection law. Thus, researchers are faced with the dilemma of possibly violating applicable data protection law during their research.

Despite the significant benefits that cybersecurity researchers can achieve by carrying out such work, they operate in a legal gray area. Knowledge of this legal gray area may lead to refraining from such research activities for fear of legal consequences, regardless of the added value.[5]

To facilitate such research in the future, the applicable law must therefore be adapted to the actual circumstances of research and must respond to its needs. Specifically, a clear and legally secure instrument for unpredictable and unplannable personal data processing must be created, which renders this data processing legally compliant on the one hand, without unduly restricting the rights and freedoms of data subjects on the other.

Though the requirement – as described here – was derived from cybersecurity research, it is important to emphasize that the need to enable unpredictable and unplannable data processing in a legally compliant manner exists beyond this and other research.

[4] Boll, Selzer (2024), *DuD*.
[5] Boll, Selzer, Spiecker gen. Döhmann, *Tagesspiegel Online*.

3. Proposed solution

Based on this, we believe that a new instrument is required in European data protection law to enable unpredictable and unplannable personal data processing without unduly restricting the rights and freedoms of data subjects in the process. We refer to this instrument as the "data protection preventive assessment" or "DP-PA" for short.

The purpose of the DP-PA is to prepare for any imminent – unpredictable and unplannable – personal data processing by first making assumptions about the possible imminent personal data processing, which can be regarded as reasonably probable. In the case of research, assumptions can be based on previous experience of similar research activities or on knowledge of the medium used for the research activity ("which data of which data subjects could usually be found on the dark web as a result of data theft?"). On this basis, core aspects of data protection law (including the identification of a relevant legal basis, the implementation of technical and organizational measures as well as the implementation of information obligations) that are appropriate in relation to the previously made assumptions should then be implemented before any personal data processing takes place.

If personal data processing occurs that was not identified as reasonably probable during the precautionary data protection measures, the fact that this specific data processing occurred without precautionary data protection measures should not be subject to a fine.

The GDPR currently consists of a total of 99 individual Articles, with each Article regulating a separate legal area (e.g. the conditions for consent). Specifically, we propose adding a new Article to the GDPR to make this new instrument legally binding. As the individual Articles of the GDPR are divided into superordinate chapters (e.g. the conditions for consent are specified within the "Principles" chapter), such a new Article should not be added as the 100th Article but should rather be added as a new Article within a suitable chapter. In the most appropriate, logical order of the Articles within this chapter the Article number should be followed by an "a". We therefore propose the legal anchoring of the DP-PA as a new Article 36a[6] GDPR.

The proposed Article 36a GDPR pursues two equally important objectives:

1) It is intended to provide data controllers with certainty that unpredictable and unplannable personal data processing operations can be implemented in a legally secure manner.
2) It is intended to obligate the data controller in the context of unpredictable and unplannable personal data processing to implement measures to ensure adequate protection of the rights and freedoms of data subjects affected by any personal data processing that may be carried out.

To implement this, Article 36a GDPR would first have to regulate when an organization that is responsible for personal data processing (from a data protection perspective "the controller") is obligated to carry out a DP-PA. This should be the case if personal data processing is not predictable, cannot be planned but is reasonably probable.

In strictly exceptional cases, in which personal data processing could cause very serious harm to data subjects (e.g. potential processing of information on persons under witness protection), the DP-PA should be carried out even if data processing is improbable.

This may be regulated in the GDPR as follows:[7]

Proposal for Article 36a paragraph 1 GDPR
(1) If personal data processing is
a) not predictable and
b) not plannable and
c) reasonably probable

[6] This placement appears ideal, as the DP-PA would thus succeed the instrument for the data protection impact assessment – an instrument that has certain similarities to the DP-PA.
[7] To adopt the GDPR wording as accurately as possible within the framework of the proposed amendment, this proposed amendment is based on the existing wording of Article 35 GDPR and adopts some of it verbatim, provided it can be applied to the DP-PA.

the controller must implement a data protection preventive assessment.
In exceptional cases, the controller must implement a data protection preventive assessment, even if the personal data processing is not predictable, not plannable, nor probable, but if it may result in a high risk to the rights and freedoms of natural persons. A single process of a data protection preventive assessment can be implemented for several similar processing operations with the same purposes.

Within a responsible organization, the implementation of data protection requirements is often delegated to those employees who have been appointed to execute the specific processing of personal data. For example, the implementation of data protection requirements within the application process is often delegated to employees in the HR department. However, these employees do not always have in-depth expertise in data protection law.

Since both the decision on whether the implementation of the DP-PA is obligatory as well as the execution of the DP-PA require sound knowledge of data protection law, it must be stipulated that the data protection officer – i.e. the employee who makes recommendations on data protection implementation within the respective organization and monitors data protection requirements internally – be involved in this process.

This may be regulated in the GDPR as follows:

Proposal for Article 36a paragraph 2 GDPR
(2) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection preventive assessment.

Data protection authorities are responsible, among other things, for specifying in which cases (or for which processes involving personal data processing) certain obligations of the GDPR apply. This is particularly important if the decision on the obligation to implement is complex and may therefore present the responsible organizations with (undue) difficulties.[8] Since this may occur with the DP-PA, the responsible data protection authorities should support the respective organizations with a list of typical processing operations for which the implementation of a DP-PA is obligatory.

As there are several data protection authorities within the European Union, they must ensure the uniform application and enforcement of the GDPR – and therefore a uniform application of the obligatory implementation of the DP-PA. This is done in the so-called consistency mechanism.

This may be regulated in the GDPR as follows:

Proposal for Article 36a paragraph 3 GDPR
(3) The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection preventive assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68. If applicable, this shall be done in accordance with the consistency mechanism pursuant to Article 63.

The challenge outlined above regarding the decision on the obligation to implement a DP-PA by the responsible organization may be supported by a list from the responsible data protection authorities containing typical operations for which the implementation of a DP-PA is not obligatory.[9]

This may be regulated in the GDPR as follows:

Proposal for Article 36a paragraph 4 GDPR
(4) The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection preventive assessment is

[8] Based on this, data protection authorities have already published lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment. The data protection impact assessment is an instrument of data protection law already regulated in the GDPR for particularly high-risk personal data processing operations.
[9] Again, these lists are regulated within the data protection impact assessment (see footnote 8). In contrast to the lists containing typical operations for which the implementation of a data protection impact assessment is obligatory, the publication of a list of operations for which the implementation is not obligatory is not mandatory. It is at the supervisory authorities' discretion whether they wish to publish such a list. We follow this approach as part of our proposal to regulate the instrument of the GDPR.

required. The supervisory authority shall communicate those lists to the Board referred to in Article 68. If applicable, this shall be done in accordance with the consistency mechanism pursuant to Article 63.

In addition, it would be necessary to regulate which specific obligations exist in the context of the DP-PA implementation. As explained in Article 36a(1) GDPR, in principle only those personal data processing operations that are unplannable and unpredictable, but reasonably probable, should be considered in a DP-PA. Consequently, a DP-PA should first describe the activities in which personal data processing is to be expected and why it is to be expected (e.g. because similar personal data processing has occurred in comparable research activities before). Then, important core aspects of data protection law must be implemented in preparation for these probable data processing activities in order to be prepared from a data protection perspective for the eventuality that personal data processing will occur at a later stage.

Implementation is based on assumptions that may result from previous experience with similar contexts, among other things. For example, appropriate technical and organizational measures would have to be implemented based on these assumptions.

This may be regulated in the GDPR as follows:

Proposal for Article 36a paragraph 5 GDPR

(5) The data protection preventive assessment shall contain at least:

a) a comprehensive and systematic description of the envisaged operations, in particular with regard to the purpose of the operation and its necessity;

b) the identification of relevant legal bases pursuant to Articles 6 to 10 as well as, if applicable, the implementation of contracts pursuant to Articles 26(1) and 28(3) and the implementation of the requirements of Articles 44 to 50;

c) the identification and, if applicable, the implementation of information requirements pursuant to Article 13 or Article 14;

d) the identification and, if applicable, the implementation of technical and organizational measures pursuant to Article 25 and 32;

e) if required, data protection supervision during operation, which includes in particular

- the monitoring of the actual data collection, a comparison with the predicted data collection and, if necessary, the documentation of unexpected data processing pursuant to Article 5(2),

- the monitoring of the applicability and, if necessary, the compliance with the rights of the data subject pursuant to Articles 12 and 15–22,

- the monitoring of the compliance with the Articles 13 and 14, the compliance to erasure periods as well as the implementation and, if necessary, adaptation of technical and organizational measures pursuant to Articles 25 and 32,

- the monitoring of the applicability and, if necessary, the compliance to Articles 33 and 34, in case of personal data breaches.

f) documentation of the steps referred to in paragraph 5 points (a)–(e) pursuant to Article 5(2).

To adequately address the risks to the rights and freedoms of data subjects (potentially) affected by personal data processing, a small number of potential data subjects (or their representatives) should be involved in the DP-PA in order to obtain their views on any forthcoming data processing and take them into account in the further course of the DP-PA implementation. However, this is only possible if the group of potential data subjects can be narrowed down. For instance, if an unplanned and unpredictable data processing operation could generally only affect the users of a particular social network. In this case, some social network users' point of view could be obtained.

This may be regulated in the GDPR as follows:

Proposal for Article 36a paragraph 6 GDPR

(6) Insofar as the group of potential data subjects can be narrowed down, the controller shall, where appropriate, seek the views of potential data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

In Article 30, the GDPR regulates an obligation to implement comprehensive documentation, which is generally impossible to implement or can only be implemented partially in the case of unplanned and unpredictable data processing. Thus, an exception to this obligation is required for unplanned and unpredictable data processing.

This may be regulated in the GDPR as follows:

Proposal for Article 36a paragraph 7 GDPR
(7) Article 30 paragraphs 1 and 2 shall apply with the proviso that the information contained in the record of processing activities by the controller and, where applicable, by the processor shall only be listed to the extent already known.

The proposed amendment of Article 36a GDPR would be accompanied by further minor amendments to the GDPR, including adding the new Article 36a GDPR to Article 83(5) GDPR, which covers the scope of administrative fines for certain infringements of the GDPR. Then fines of up to EUR 20,000,000 or, in the case of a company, up to 4% of its total annual global turnover in the preceding financial year could be imposed if a DP-PA (provided the new proposed article is applicable) is not carried out. It should be noted that there should be no obligation to implement a DP-PA for unpredictable, unplannable, and not reasonably probable personal data processing. Should such processing occur unexpectedly, this should not be subject to a fine.

Further additions required include a legal definition for unpredictable and unplannable data processing (Article 4 GDPR), the addition of the tasks of the data protection officer (Article 39(1) point (c) GDPR) and the addition of the tasks of the supervisory authorities (Article 57(1) point (k) GDPR).[10]

4. Significance beyond research

Only by rethinking data protection law towards the DP-PA, as described here, it can ultimately be ensured that (relevant) scientific research is conducted in a legally secure manner and that our society can benefit from the advantages of this research in the long term.

Although cybersecurity research is the initiator of the DP-PA, as outlined above, the instrument may become relevant not only for scientific research. Especially considering technological progress, potential applications involving anonymized data sets that have already been partially de-anonymized or involving artificial intelligence are conceivable among other things.

5. Conclusion

The data protection legislation in force in the European Union does not provide for the possibility of carrying out unpredictable and unplannable but reasonably probable personal data processing in a legally secure manner. However, this is urgently needed in order to conduct cybersecurity research in a legally secure manner and thus maintain the significant social benefit of this research.

The data protection preventive assessment would provide a solution to this issue: The legally binding anchoring of the data protection preventive assessment in the GDPR would resolve the legal gray area for such data processing and create legal certainty. At the same time, the rights and freedoms of data subjects would be adequately protected.

[10] See Boll, Stummer, Selzer (2024), *DuD* on this and on the proposal of Art. 36a GDPR in detail.

6. Further readings

For a detailed overview of the proposed instrument, please refer to the following papers (in chronological order):

Alina Boll, Annika Selzer, Indra Spiecker gen. Döhmann (2023), *Datenschutz in der offensiven Cybersicherheitsforschung*, https://background.tagesspiegel.de/cybersecurity/datenschutz-in-der-offensiven-cybersicherheitsforschung.

Annika Selzer (2023), *Umbruch im Datenschutz – Datenschutzvorsorge in der Cybersicherheitsforschung, Verifizierung von Anonymität und Berücksichtigung der Nutzerbedürfnisse*, *GI Informatik*, p. 705–713.

Annika Selzer, Indra Spiecker gen. Döhmann, Alina Boll (2023), *Datenschutzvorsorge in der offensiven Cybersicherheitsforschung – Datenschutzkonforme Verarbeitung in Fällen unvorhersehbarer Datenverarbeitungen*, *DuD*, p. 785–789.

Boll, Annika Selzer (2024), *Die Datenschutz-Vorsorge (DS-V) – Systematisierung eines neuen Instruments für das Datenschutzrecht*, *DuD*, p. 44–48.

Boll, Stummer (2024), *Erste Schritte im Rahmen der Datenschutz-Vorsorge – Beschreibung und Rechtsgrundlagen*, *DuD* (in print).

Boll, Stummer, Annika Selzer (2024), *Datenschutz-Vorsorge – Anwendbarkeit jenseits der Forschung und Einbettung in das geltende Datenschutzrecht*, *DuD* (in print).

Boll (2024), *Weitere Schritte im Rahmen der Datenschutz-Vorsorge – Informationspflichten, TOMs, Dokumentation und Betreuung* (Schritte 3-6 der DS-V), *DuD* (in print).

Boll, *Die Datenschutz-Vorsorge in der offensiven Cybersicherheitsforschung – Eine erste exemplarische Umsetzung in Form eines Planspiels* (under review).

ATHENE

National Research Center
for Applied Cybersecurity