The Order of Protection Goals

Martin Rost (martin.rost@maroki.de)

2018

Abstract

This article presents different arrangements of data protection objectives, which may be of often surprising importance for operational data protection.[1]

1 Introduction

Protection goals or guarantee goals anchor the standard data protection model (SDM)[2] in the General Data Protection Regulation (GDPR).

Three questions on the genesis and structure of protection goals have been waiting for a long time to be answered:

1. What is the "generative principle" for new protection goals and which instance may legitimately proclaim them as "bindingly applicable"?
2. Can a presumption be made as to the completeness of protection goals?
3. What is the relationship between protection objectives?

These three questions were asked by Andreas Pfitzmann, Professor for Technical Data Protection and Data Security at the Technical University of Dresden, in 2008 in an internal working paper.[3] In the meantime, initial answers can be given.

2 First attempts at answers

Question 1 concerning the generative principle for protection goals and the instance which may legitimately declare protection goals can now be answered relatively easily.

[1] This article corresponds to a translation of the article: Rost, Martin, 2018: Die Ordnung der Schutzziele; in: DuD - Datenschutz und Datensicherheit, 42. Jahrgang, Heft 1: 13-18.

[2] SDM, english version available at https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

[3] Andreas Pfitzmann died in September 2010; these questions probably arose during his deliberations at the Federal Constitutional Court in the run-up to the drafting of the confidentiality and integrity ruling (see BVerfG 2008).

For Pfitzmann, protection goals were still a regulatory instrument specifically for IT security. Protection goals were formulated in 1983 in the "Orange Book" for the evaluation and certification of the security of computer systems, which was transferred to the Common Criteria (now ISO/IEC 15408) in 1996. In the meantime, public authorities and companies in Germany are familiar with these three protection goals (securing availability, integrity, confidentiality), particularly from the context of the basic IT protection. They are used in security concepts as normative anchors. Protection goals apply if an organisation, such as the Department of Defense, for example, commits itself to them in the "Orange Book". This weak legitimation does not change even if, for example, a globally active organization such as ISO claims a certain set of protection goals as representing the state of the art. From a sociological point of view, protection goals in this sense only formulate the interests of organizations.

Organizations know the instrument of target agreements, which are then implemented both in the form of input-oriented "conditional programmes" and output-oriented "special purpose programmes" (cf. Luhmann 2000). Goals offer organizations a medium to focus the differences based on the division of labour in a normative-regulatory way, with which laws as well as self-imposed standards are connected in an understandable way within the organization. Since the turn of the millennium, protection goals have also been a component, for example, in many state data protection laws, in Article 5 of the GDPR and in Â§8a of the IT Security Act. In the meantime, the catalogue of protection goals has been expanded, adapted to data protection requirements and operationalised within the framework of the standard data protection model. The inclusion of protection goals in legal texts necessarily blurs their previously technically dominated definitions, but also leads to a broader legitimation and enforceability of protection goals in organizations.

Question 2 on the "completeness of the set of protection goals" of various (overflowing) catalogues of protection goals is naturally much more difficult to answer. Pfitzmann criticised in the internal working paper the proliferation of new protection goals proclaimed by new organizations. A first and conceptually simple attempt is to be made here, even if one can only fail with the assertion of completeness outside mathematical constructions or analytically trivial systems.[4]

The incorporation of the set of protection objectives in data protection laws makes it possible to set these objectives in relation to other existing sets of standards in a relationship secured by legal methods. In this way, the normative subordination of protection objectives to fundamental rights can be established, according to which protection objectives can only have a function to operationalize fundamental rights and are thus not an end in themselves. Two questions then arise: Do the protection objectives fully cover the fundamental rights currently covered by data protection, and does the implementation of the protection objectives lead to an equally fully effective implementation of the requirements of fundamental rights?

With regard to the operationalisation of fundamental rights requirements, it can be assumed that the six elementary protection objectives of data protection - securing the availability, integrity, confidentiality, transparency, unlinkability[5] and the

[4]Because of the open future of social developments, the set of data protection goals can only be fully asserted as "historical" or "current" (Kloepfer 2015).

[5]The normatively important requirement of data minimization is treated in this article as a subset of the protection objective of unlinkability, because data minimization must be done with regard

ability to intervene in personal proceedings - can be assumed to be complete from the perspective of the persons concerned and with reference to the EU Charter of Fundamental Rights. This assumption is based on a large number of examinations of procedures which have been carried out in the meantime and on the discovery of the fertility of the various forms of ordering protection objectives and the discussions about them. Further, specific protection goals can be developed from the already existing elementary protection goals. According to these, the protection objective "resilience" (cf. Article 32 GDPR) can be interpreted as "assured availability with integrity" and implemented with appropriately combined measures. More on this in a moment.

Before question 3 on the "order of protection goals among themselves" can also be dealt with, the sociologically essential communicative function of protection goals must be examined.

3 The communicative function of protection goals

Protection goals allow organizations to selectively relate different requirements and logics in their procedures and data processing. In the case of organizations, one thinks of companies, authorities, research institutes, medical practices and law firms, associations and parties, schools, hospitals, armies, prisons, access and content providers. In the case of logics, one thinks, for example, of legal, financial and scientific requirements and strategies. Technicians place greater emphasis on other procedural characteristics than lawyers, business economists or system architects. In the legal domain, the difference between legal conformity/non-legal conformity forms the communications. In any case, it is not the difference of engineers, who in turn act and communicate along the lines of observing whether something functions or does not function. And economists ultimately observe their environment solely on the basis of the difference of payments/non-payments.

Protection goals focus on the problems and conflicts that need to be solved, without one of the logics involved, such as the technical - or the other two logics, such as the legal or business logics, dominating in a structurally pre-determined way. Protection goals selectively link certain guiding aspects and decouple the procedural sequences of the logics and control hierarchies involved.

If one formulates this characteristic in more general terms, then it can be said that protection goals focus on communications within and between different specialist areas with their different logics, which in modern societies have developed in organizations based on the division of labour. No domain can make a promising claim to formulate the final definition for individual protection goals, which the other domains must then simply adopt. The definition of a comprehensible overall objective must be formulated in such a generalized manner that the objective can be specific to one's own domain and still point in the same direction in all other domains.[6] Protection objectives must encompass more than just repeating somewhat

to the purpose of the procedure, which legitimizes and limits the chaining of data as necessary and appropriate. This view regarding the subordinate positioning of data minimization is not shared by all colleagues participating in the discourse on protection goals.

[6] This claim to abstractly overarching validity has not yet been sufficiently fulfilled in the current definition of the protection goals, as explicitly undertaken in the standard data protection model; some definitions are legally dominated. For example, transparency is defined there as

reformulated legal standards.

It is possible to approach the question of what protection goals achieve in a different way and to sociologically deepen the justification for them, and thus also the justification for data protection. The sociological thesis is that the protection goals supplement Habermas' set of meaningful validity requirements for reasonable speech with operational requirements. By analogy, protection goals would be understood as validity requirements for "a reasonable functioning of systems". These validity requirements must be imposed on technically mediated communication infrastructures such as the Internet - and all services based on them. The organizations, procedures, services, platforms, networks and the technical components used under them must all meet the requirements formulated by the protection goals so that the reasonable validity requirements can actually be met operationally. Without the functional measures of data protection for personal procedures and communication technologies, Habermas' discourse model is obsolete for a modern society in which communications are technically transmitted. According to this model, the thesis is that protective goals have evolved because a modern society is dependent on the actual success of communications in terms of truth, normative correctness and truthfulness in the context of organizations (cf. Rost 2013).[7]

4 The order of the protection goals

How can the relationship between protection goals be determined? The thesis is that the plausibility of a sequence of protection goals is observer-dependent. For example, a technician will find a different sequence plausible than a data protection lawyer or a business economist. A general, abstract hierarchical order cannot be formulated.

If one concentrates on the three conventional protection goals - securing availability, integrity and confidentiality - then typically a triangle appears as a figure. With such a structure in mind, the question does not necessarily arise as to whether the protection objectives can also be arranged in pairs in a conflicting or hierarchical or self-referential manner.

On closer examination, it becomes apparent that a radically unilateral implementation of one of these protection goals is at the expense of the other protection goals. For example, a secured availability of a date, such as the making of backups, basically always risks securing the confidentiality of a date, because the risk of unauthorized access increases with each additional copy of a date. Conversely, intensive protection of the confidentiality of a date, implemented for example through encryption, leads to the risk of securing the availability of a date because, for example, a secret can be lost. If one takes a look at the complete set of six data protection objectives, further conflicts of a similar kind become immediately apparent: a high degree of transparency of a procedure, which is created, for example, by documentation and protocol data, risks that this data can be used unauthorized or for the purpose of

"establishing testability and assessability". As a computer scientist, of course, one understands this, so this definition is not misguided in the operationalization. However, in computer science, transparency is understood as a user's access to a system, in which the user himself does not notice the activities he triggers in the system, and the user should not be put into an inhibiting, reflective mode of testing.

[7] The present situation gives rise to suspicions that modernity is regressing.

monitoring the behavior and performance of employees.

The internal contradiction of the protection goals with their requirements, each of which is at the same time unavoidable in itself, indicates that protection goals are not dimensions. To claim dimensions, it would be necessary to require that the protection goals are independent of each other. But they are not. In practice, for example, confidentiality measures are used to ensure the integrity of the protection goals, at least for certain attacks.

Three types of the arrangement of protection targets are briefly discussed below:

1. The elementary protection targets can be arranged as three dual axes.[8] According to this, it is claimed that two simultaneously pursued protection goals that form a dual, when implemented in practice, reduce the protective effect of the other protection goal. It was this idea that led to the development of the six elementary protection goals in 2009 and ultimately to the standard data protection model. The arrangement as a dual allows a very specific intertwining of law and technology.

2. The protection objectives can be arranged in a self-referential manner. With six protection objectives, we are thus formally dealing with 36 constellations of protection objectives that can be analysed. During the development of the SDM, it has been shown that the mutual reference of protection goals is a fruitful rule for generating a complete catalogue of protection measures for high protection needs.

3. The protection goals can be arranged hierarchically. The plausibility of the order of the protection goals depends on the type of organization in which they are to be implemented. The possibility of identifying typical protection goal hierarchies would allow a large number of organizations to identify standardized data protection requirements or catalogues of protection measures.

4.1 Arrangements of protection targets as "Duals"

The arrangement of protection objectives as a dual allows a very specific intertwining of law and technology. The two spheres - functional technology and binding applicable standards - are decoupled by means of protection objectives, and any overlapping of one technical logic with the other is avoided. At the same time, protection objectives provide selective focus and contact between the two logics. The cooperation between the lawyer and the technician consists in the fact that the lawyer uses data protection law as the normative body of rules to weigh up the protection objectives, or the exposed pairs of protection objectives, and the technician then surveys the arsenal of possible protection measures which, after this normatively driven weighing up, have to be implemented in a way that is adapted to the specific procedure.

The first draft of a systematic arrangement of the elementary protection objectives of Pfitzmann and Rost had three such dual axes: Availability / Confidentiality, Integrity / Intervensibility, Transparency / Non-linkability (Rost/Pfitzmann 2009). This highlighting of three pairs makes it easier for the lawyer to fully consider the

[8] The term "Dual" comes from Pfitzmann. It is intended to indicate that two protection objectives apply to the same extent, but are contradictory.

solution space to be handled operationally. When examining the operational level of procedures, standards experts require methodological consistency in the question of which principles (protection objectives) are to be weighed up overall and against each other.

In addition to the equilibrium between three privileged dual pairs, it may prove justified for the specific procedure to identify a protection objective as leading within a dual. Thus, for example, in the rescue or defence of human lives, securing the availability of rescue measures may justifiably be considered more important than securing confidentiality. Logically, according to the 3-dual model, there can only be one dominant protection objective per dual for a procedure, which in turn can be placed in an overall ranking of all protection objectives.

4.2 Self-referential arrangement of protection targets

During the development of the SDM catalogue of measures, it became apparent that a rule was found through the self-reference of protection goals or the corresponding protection measures in order to be able to identify protection measures even for high protection needs. Protection measures taken must in turn satisfy the complete set of protection objectives. What is meant by this? In the case of a low-intensity encroachment on fundamental rights or in the case of a normal need for protection in a procedure, processes and systems must be logged, for example, in order to implement the protection objective of "transparency". If the need for protection is high, log data must also be signed in an integrity-secure manner and encrypted in a confidentiality-secure manner, a role and authorization concept for access to the log data must be available, etc.

During the discussion of the 6x6 possible assignments, it became apparent that it is possible to analyze the catalog of protective measures for completeness. It becomes clear, for example, that an integrity-protected measure to ensure transparency must be distinguished from a transparency-protected measure to ensure the integrity of a procedure. It also makes sense to relate a protection objective directly to itself - e.g. "transparency-securing transparency" - which at first seems a little strange. It refers to the fact that transparency must be created and can by no means be regarded as a system property that has always been passively given. The methodology for creating transparency must be made transparent. Creating transparency for a recipient requires the sender to have a model of the recipient horizon and its methods of specific observation. In concrete terms: Creating transparency for a data subject (data protection declaration) requires other measures than those intended to create transparency for one's own organization or for a cooperating organization, for example in the context of order processing, or for supervisory authorities. Data protection officers are interested, for example, in knowing which processes and systems are logged where and in what form in order to be able to assess the effectiveness of the protective measures taken.

It follows from the thesis of the relative completeness of the protection goals that it must be possible to formulate further specific protection goals by referring to the elementary protection goals themselves. Thus, for example, the somewhat surprisingly demanded protection goal "resilience" (Art. 32 GDPR) can be designed as "availability assured by integrity" with the means of the existing protection goals, with the corresponding protection measures to be selected accordingly. Conversely,

it makes sense to designate protection goal constellations created by self-reference as a specific protection goal. Thus, for example, secured confidential confidentiality can be described as unobservability and then implemented with special steganographic protective measures. If it should turn out that the thesis of the relative completeness of the six elementary protection objectives cannot be upheld, this would again suggest that one might not have found or constructed a new fundamental right, but a new essential facet.[9]

The rule of self-reference also makes it possible to assess and maintain the completeness and consistency of a catalogue of data protection objectives and measures. This makes it possible to check whether a protection objective that is presented as "new" to the catalogue of protection objectives cannot be reconstructed by self-referential constellations or subsumed under existing protection objectives. Proposals for new protection measures or for changes to measures in a catalog of measures can also be accepted or rejected on the basis of this examination. Furthermore, such quality assurance is a necessary condition for being able to identify measures with a consistent granularity and differentiated according to the need for protection.[10]

4.3 Hierarchical arrangement of protection goals

Protection goals can be arranged hierarchically. In the following, the thesis is plausibilised that, in principle, securing integrity has priority in every case, although the understanding of integrity depends on the respective "technical logic" organised according to the division of labour.[11]

According to this, a process can be said to have technical-functional integrity if a process comes as close as possible to the functional specification, has the desired properties and functions effectively. The efficiency and side effects are considered and kept under control. Always the same inputs lead to always the same outputs, causality is the control ideal.[12] In a tax-calculation procedure, the amount of payment is calculated automatically, the result must be correct. A distinction to be made from this would be legal integrity. This is guaranteed if a procedure meets the legal requirements. With regard to a tax procedure, this would mean that it serves, with all its components, solely and exclusively for the calculation of payout amounts and the administration of entitled recipients by authorised clerks, taking into account all relevant laws. It would also be possible to speak of business integrity if the procedure could be operated at least as cost-effectively as the tax procedures of other organizations.

If technical integrity dominates a hierarchy of protection goals in an organization based on the division of labour, the second protection goal must be in a very close relationship to it, because it must take into account the specific technical logic, in contrast to others, in operational terms.

From a technical point of view, the focus is on ensuring the functional availability

[9] On the "finding" of new basic rights see Hornung 2014.

[10] Previous catalogues of protection goals mix up principles, standards, goals, processes and rules and also compile measures as desired. They do not indicate any benchmark for the reference to legal requirements, completeness or the quality aimed for. This criticism applies, for example, to ISO 29101:2013 as well as to the CNIL catalogue of measures (see CNIL 2012).

[11] A further proposal for the arrangement can be found at Rost 2017.

[12] At this point the question can be neglected whether these characterizations also apply to neural networks or to procedures with artificial intelligence.

of a process, which includes in particular the availability of repair and backup processes. In contrast, the main problem to be solved in terms of security is to ensure the confidentiality of data processing. From a technical point of view, confidentiality protection measures must be available redundantly. Technical confidentiality protection ensures the continued existence of an organization: Data that is, for example, part of the business and procedural secrets may then only be allowed to flow under clearly controlled conditions. If the data processing of organizations is fully digitalized, the following applies: Only the control of data flows can secure the existence of an organization. The perspective of data protection law is different: According to this, the integrity of a procedure, which is specifically governed by data protection law, is enforced in the form of setting the purpose, determination of purpose, separation of purpose and earmarking of a procedure with the help of available technical measures of non-chaining. A procedure is to be operated in which the degree of external determination is reduced to the absolutely necessary extent. In business and political terms, the second protection objective should also serve to reinforce the protection objective of ensuring availability. The procedure is to exist, either for the purpose of optimum return on capital or to ensure existing power relations.

In third place in a hierarchy of objectives would then be transparency, again common to all the technical logics involved in a procedure. The function of transparency is to make it possible to check whether the technical integrity is effectively ensured.

Which protection goal comes in fourth place depends on the technical logic and the urgency with which error corrections are to be carried out. If securing availability is at the top of the list, the ability to intervene must be ensured. At the same time, intervisibility fundamentally risks integrity, because although changes should only be carried out under the control of the organization, the corresponding measures also offer convenient intervention options for external parties.[13] It is plausible to argue that the immediate correction of relevant deviations has a high technical priority, whereas legally, the correction of normative deviations may generally take longer to heal, although economically a required correction can also be classified as currently too expensive.

A discussion of a hierarchical arrangement of protection goals is obviously still in its infancy. Any elaboration should take into account the specific contradictions of dual-pair arrangements that have been identified. This means, for example, that the designation of a leading lead protection target must result in the corresponding dual protection target being at the end of the hierarchy. This is followed by the other two dual pairs, which in turn must also be arranged diametrically.

And why all this? The thesis is that for each type of organization - administration, company, scientific institute, voluntary association, total institutions with their strong control over persons (prisons, army, schools, hospitals) - a hierarchy of protection goals can be identified, with a specific arrangement of the dual pairs within the hierarchy. In terms of data protection, this would mean that for each type of organization specific information for consideration and, above all, a standard catalogue of coordinated measures would be identifiable.

[13] An example is the state Trojan, which is to be used only by security authorities, but which is suspected to be captured by program code producers and hackers.

5 Conclusion

The protection goals of data protection couple and decouple, as communication media close to organizations, the various technical logics involved in the development and maintenance of a controlled operation of a personal procedure in organizations. This characteristic is indispensable for the operation of modern personal procedures, which should not violate fundamental rights and should function effectively, in a modern "functionally differentiated world society" (Luhmann). The validity of protection goals in data protection, and to some extent in IT security, has now been legitimized by law. For the set of six elementary protection goals identified so far, one may assume a historically relativised completeness. This set of protection goals is now semantically so charged and differentiated that self-referential references can be used in practice to form a benchmark for the quality of protection measures. The attempt to show a control hierarchy of data protection goals shows that this hierarchy is different for each organization.

6 References

- BverfG, 2008: Urteil vom 27. Februar 2008 zum "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", Az. 1 BvR 595/07, 1 BvR 370/07, https://openjur.de/u/59199.html
- CNIL, 2012: Measures for the privacy risk treatment, https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf
- Hornung, Gerrit, 2014: Grundrechtsinnovationen, Tübingen, Mohr Siebeck
- Kloepfer, Michael 2015: Seminar "Neue Grundrechte - Analyse und Vorschläge", http://kloepfer.rewi.hu-berlin.de/doc/Themen_VEROEFF.pdf
- Luhmann, Niklas 2000: Organisation und Entscheidung, Opladen/ Wiesbaden, Westdeutscher Verlag
- Rost, Martin; Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele - revisited; in: DuD - Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6: 353-358
- Rost, Martin, 2012: Standardisierte Datenschutzmodellierung; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438
- Rost, Martin, 2013: Zur Soziologie des Datenschutzes; in: DuD - Datenschutz und Datensicherheit, 37. Jahrgang, Heft 2: 85-91
- Rost, Martin, 2018: Die Ordnung der Schutzziele; in: DuD - Datenschutz und Datensicherheit, 42. Jahrgang, Heft 1: 13-18.
- Rost, Martin, 2017: Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten, in: Sowa, Aleksandra, 2017: IT-Prüfung, Sicherheitsaudit und Datenschutzmodell: Neue Ansätze für die IT-Revision, 1. Auflage, Springer Vieweg, S. 23-56