

A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation

Felix Bieker¹(✉), Michael Friedewald², Marit Hansen¹, Hannah Obersteller¹,
and Martin Rost¹

¹ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
(Independent Centre for Privacy Protection Schleswig-Holstein), Kiel, Germany
{fbieker,marit.hansen,hobersteller,mrost}@datenschutzzentrum.de

² Fraunhofer Institute for Systems and Innovation Research ISI,
Karlsruhe, Germany
michael.friedewald@isi.fraunhofer.de

Abstract. With the General Data Protection Regulation there will be a legal obligation for controllers to conduct a Data Protection Impact Assessment for the first time. This paper examines the new provisions in detail and examines ways for their successful implementation. It proposes a process which operationalizes established requirements ensuring the appropriate attention to fundamental rights as warranted by the GDPR, incorporates the legislation's new requirements and can be adapted to suit the controller's needs.

Keywords: Data Protection · Data Protection Impact Assessment · General Data Protection Regulation · Privacy · Privacy Impact Assessment

1 Introduction

While the proliferation of technological innovation has made the processing of personal data by automated means ubiquitous, the enforcement of the individual's rights has not been at the forefront of concern. Although the European Union's (EU) Charter of Fundamental Rights (CFR) is equipped with a new right to the protection of personal data, which accompanies the well-established right to private life, there has been a disconnect between the debate of rights protection and the implementation of new technologies. Carrying out a Data Protection Impact Assessment, while keeping in mind its purpose of ensuring the protection of individual rights, is able to bridge this divide. In order to help organizations and enterprises to assess the data protection impact of their processing of data, the new EU General Data Protection Regulation (GDPR), under the conditions of its Article 35, prescribes the execution of a Data Protection Impact Assessment (DPIA). A DPIA is an instrument to identify and analyze risks for individuals, which exist due to the use of a certain technology or system by an organization in their various roles (as citizens, customers, patients,

etc.). On the basis of the outcome of the analysis, the appropriate measures to remedy the risks should be chosen and implemented. Since the inception of impact assessments there have also been approaches to adapt a model for the area of privacy and data protection. However, as there was no obligation to carry out such an assessment, these attempts had a wide range. This will change once the GDPR comes into force. Data protection authorities are the logical proponents of a comprehensive and operational model for these assessments.

In the following, previous models for Privacy Impact Assessment (PIA) will be briefly introduced (Sect. 2), the legal requirements of the GDPR will be analyzed (Sect. 3) and a methodology, in a broad sense, based on operational models outlined (Sect. 4). It is concluded that the process outlined in this paper realizes the full potential of DPIA with regard to the protection of fundamental rights as envisaged by the GDPR and provides a convenient instrument, built on established for controllers to comply with legal requirements (Sect. 5).

2 Related Work

Even though the current EU data protection regime, the Data Protection Directive 95/46/EC, does not foresee a DPIA, the concept has been discussed within the EU before. In response to recommendations by the European Commission [1, 2], the Article 29 Working Party set out general requirements for PIAs [3, 4]: any process had to contain provisions on the evaluation of data protection risks and incorporate the concept of data protection targets. In conformity with Article 8 Data Protection Directive 95/46/EC the process had to include requirements for the processing of special kinds of data, such as ethnicity, political or religious beliefs as well as health data. While parts of the concept of risk assessment could be incorporated in a PIA, the Working Party stressed that regarding legal requirements compliance could not be optional and that no discretion could be awarded to the organization under any circumstances. These demands can be seen as minimum requirements.

In parallel, there have been conceptualizations in academia based on methodologies developed *inter alia* in the UK, Canada, Australia and the USA [5] and industry [6], which follow their own respective methodologies based on the varying interests. Furthermore, the data protection authorities of the UK and France developed their own approaches to PIA. However, as these procedures were developed well before a legal obligation to conduct a DPIA, they are largely phrased as mere recommendations and the UK Information Commissioner's Office (ICO) Code of Practice is explicitly issued in order to promote good practices under Article 51 of the UK Data Protection Act, which does not impose a legal obligation to conduct a PIA. Further, ICO and to some extent also the French Commission Nationale de l'Informatique et des Libertés (CNIL) follow a checklist approach. While this makes it easy for organizations to carry out an assessment, it also entails the risk of overly focusing on the points set out instead of adapting the process to the specific risks and requirements of an individual data processing operation.

2.1 The UK Information Commissioner’s Office Privacy Impact Assessment Code of Practice

The generic PIA model [7] developed by ICO defines PIA as a process to assess and reduce the risks of a given project for privacy. In order to systematically assess these risks an organization should apply PIA throughout the entire life-cycle of a project, from development to implementation. It defines six phases for assessment

1. Firstly, the necessity for an assessment and its scope should be examined. This may depend on the sensitivity of the data processed as well as the personnel and resources allocated to the project.
2. An assessment of data flows during all phases of processing, including access rights follows.
3. This information is then used to identify the risks for privacy and possible solutions.
4. The Code of Practice explains that the surveillance of users or loss of data are not only liable to affect users’ rights, but also pose financial risks for the organization itself.
5. It refers to data minimization, training of employees in handling personal data and the implementation of technical security measures to protect the data. Although ICO takes a tiered approach to risks – ranking from elimination to acceptance of a risk – it emphasizes that legal obligations have to be fulfilled.
6. Lastly, the results should be secured and implemented in the project plan. During each phase, internal and external consultations should accompany the assessment and involve stakeholders whose rights may be affected.

2.2 The Privacy Impact Assessment Developed by the French Commission Nationale de l’Informatique et des Libertés

The CNIL’s [8] methodology was developed to respond to risks for data protection, especially with regard to the rights of the individuals concerned. According to CNIL PIAs are aimed at finding technical and organizational measures to counter risks for rights of the data subjects. It emphasizes that these rights have to be upheld. Therefore, PIA is a continuous cycle, which starts with the definition of the data processed, including particularly the purposes of the processing and the persons concerned as well as the proportionality of the operation. This further extends to existing or planned control mechanisms.

In a further step the data protection risks have to be identified and assessed to ensure they are addressed appropriately. For this, it has to be ascertained how seriously any acts, omissions or circumstances which may occur as well as the use of certain (technical) tools, would interfere with the individuals’ rights. These consequences are then ranked depending on their gravity and likeliness of occurrence. Lastly, it has to be decided whether the results of the assessment are satisfactory or whether the assessment has to be repeated. In addition, a report, detailing the assessment of risks and the findings, should be prepared and submitted to the data protection authority by request.

3 Legal Requirements

As it has been published in the EU's Official Journal, the GDPR according to its Articles 88(1) and 91(2) will be applicable from 25 May 2018 and replace the current Data Protection Directive 95/46/EC. It will be directly effective in the Member States as prescribed by Article 288(2) TFEU. The obligation to carry out a DPIA, as well as its minimum requirements are provided in Article 35 GDPR.

3.1 Conducting a Data Protection Impact Assessment

When a high risk for the rights of individual concerned is likely to emanate from the nature, scope, context or purposes of data processing, a DPIA has to be carried out according to Article 35(1) GDPR. Paragraph 3 lists examples of when such a high risk is likely to occur

- (a) When data are systematically and extensively evaluated to analyze the personality of a natural person based on automated processing, including profiling, and decisions which have legal or similarly serious consequences for those concerned,
- (b) when sensitive data or data on criminal convictions or penalties are processed in large scale, or
- (c) when public areas are monitored systematically on a large scale.

With the new provision, the EU legislator demands the identification of risks: The controller has to assess whether there is a risk in order to determine whether a DPIA has to be conducted. However, this approach is not to be confused with the general procedure of risk management. The latter usually addresses risks for an organization and its activities. This is not the case in Article 35(1) GDPR, which concerns the risk for the rights and freedoms of individuals. Thus, unlike in risk management, there is no acceptable residual risk and every processing of personal data is an interference with the individual rights and freedoms and has to be justified.

Where necessary, the controller has to review whether the processing is still compliant with the findings of the DPIA according to Article 35(11) GDPR. According to the provision this is the case at least when there is a change in the risk posed by the processing of data. The European Parliament's proposal included an obligatory biannual review of the compliance with data protection provisions to demonstrate that the processing of personal data is compliant to the DPIA. While this was not adopted in the final version, it is clear that a change in the risk is merely one of the options for a review of the DPIA. Such a necessity however, is also brought about by changes in technology (i.e. when new technologies allowing for data minimization) or when the modes of data processing are changed.

Further, the data protection authorities are authorized to enumerate cases of data processing which do and do not require a DPIA under Article 35(4)

and (5) GDPR in specific lists. Even though Article 35(3) GDPR already lists categories where a high risk is likely to occur, it can be useful to enumerate further instances that clearly demonstrate a high level of interference with the rights of individuals, such as big data or processing of any special categories of personal data as enumerated in Article 9(1) GDPR. However, as the compilation of a list under Article 35(5) – cases where the necessity of a DPIA can be rejected under all circumstances – is not obligatory, this should not be pursued by data protection authorities. Article 35(1) GDPR already requires a high risk for the rights of individuals in order to require a DPIA. The high level of protection of fundamental rights such as the right to private life according to Article 7 CFR and data protection under Article 8 CFR envisaged by Recitals 1 through 4 and 10 as well as Article 1(1) and (2) GDPR mandates that any high risk for the rights of an individual be subject to all relevant safeguards, including a DPIA.

According to Article 35(10) GDPR the obligation to conduct a DPIA is limited when it comes to public authorities relying on legal bases of EU or national law, the law regulates the specific processing operations and a DPIA has already been carried out as part of the legislative procedure. However, this incurs a risk with regard to the actual processing of personal data in a specific case. Although the specific processing operations are to be regulated in the relevant law, this has necessarily to be achieved in a general manner and cannot cover the specific setting of data processing in every instance regulated. Thus, risks that are realized at the implementation stage are not assessed. A further concern in this regard is that privacy-enhancing technologies may not yet be available at the time of the legislation. Accordingly, while a general DPIA in the course of the legislative process is welcome, each individual implementation calls for a separate specific DPIA to assess its own specific risks. Of course, these specific assessments can be built on top of the general DPIA and thereby would consume significantly less resources.

3.2 Requirements for a Data Protection Impact Assessment

The GDPR itself merely provides a minimum standard for carrying out a DPIA, as stipulated by Article 35(7) GDPR. The starting point is a systematic description of the envisaged data processing and its purposes, including, where applicable, the legitimate interests of the controller under Article 35(7)(a) GDPR. In order to facilitate the considerations as to the nature, sources and seriousness of the risk, the controller must involve data subjects in the process where appropriate and give the persons concerned a chance to express their views on the intended processing (Article 35(9) GDPR). With this information the necessity and proportionality of the processing in relation to its purposes as well as the risks for the rights of the persons concerned can be assessed according to Article 35(7)(b) and (c) GDPR. Lastly, any DPIA has to contain measures to remedy the risks identified, including safeguards, security mechanisms and measures to protect personal data and to demonstrate compliance with the GDPR as a whole (Article 35(7)(d) GDPR). An example of this last category is the measures to be taken in case of a breach of personal data under Articles 33 and 34 GDPR,

i.e. the notification of the data protection authority and – where the breach is likely to result in a high risk for the individuals – a communication to the data subject.

Article 35(8) GDPR provides that compliance with codes of conduct according to Article 40 GDPR is a factor which must be taken into account when assessing the impact of the processing operations. However, this step must also take into consideration the rights and legitimate interests of data subjects and other persons concerned by the processing.

A DPIA report can also be helpful with regard to the certification process as envisaged under Article 42 GDPR. With regard to the certification mechanisms and data protection seals and marks, which are to be developed by the Member States, the data protection authorities and the European Data Protection Board, Article 42(1) GDPR employs the same phrase of demonstrating compliance with this Regulation as Article 35(7)(d) GDPR. A DPIA report may thus facilitate the certification process: It contains several elements, such as data flows or actors and their roles in the processing, which are also of interest for this evaluation. However, in order to realize the common, high standard of protection within the entire EU as set out in the GDPR, the mere compliance with legal obligations should not give way to a guaranteed certification within the sense of Article 42 GDPR. As the GDPR incorporates general data protection principles, for instance data protection by design and default in Article 25 GDPR, an organization striving to be certified should incorporate processes and technologies which further these principles in order to demonstrate full compliance.

Regarding the documentation or presentation of results, the GDPR does not include any explicit provisions. Article 36(1) GDPR requires that the competent data protection authority has to be consulted in cases where the absence of the measures taken by the controller in accordance with the results of the DPIA would lead to a high risk for individual rights. However, as Article 36(3)(e) GDPR merely states that the DPIA is to be provided to the data protection authority by the controller it does not stipulate any further requirements for the DPIA itself.

4 Elements of a Data Protection Impact Assessment

The process outlined below (Fig. 1) is the basis of the suggested DPIA process [9]. It has been derived from the extensive analysis of existing processes [5] and combines procedural as well as evaluation elements, which were tested and approved in practice in the EU projects PIAF and SAPIENT in an extensive empirical assessment of existing PIA schemes that the authors carried out in collaboration with Trilateral Research [10–12]. The process developed ensures that results can be reproduced and verified, enabling inter alia the competent data protection authorities to check whether all legal obligations have been satisfied. The process allows for comparison of different solutions and is technology-neutral.

The process consists of three stages, which are described in the following.

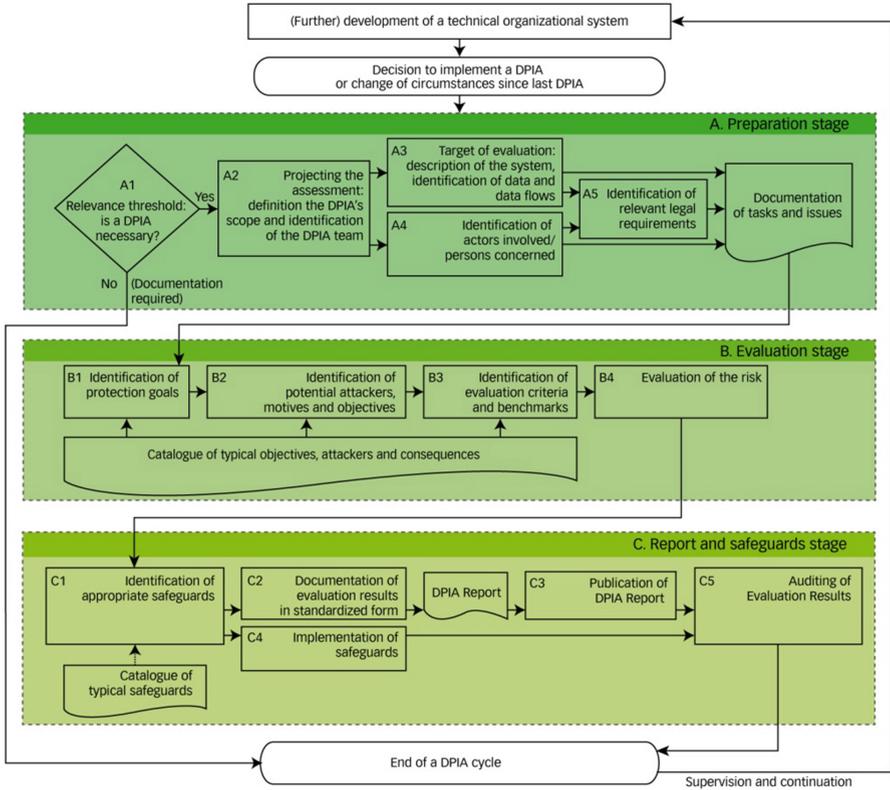


Fig. 1. DPIA process

4.1 Preparation Stage

Firstly, the controller should consider whether there is a legal obligation to carry out a DPIA. As described above, this is the case under the conditions of Article 35(1) GDPR, when a high risk for the rights of individuals is likely, especially in the cases expressly mentioned in Article 35(3) GDPR, i.e. profiling, sensitive data or systematic surveillance of public places are concerned. Further, in order to assess whether a DPIA has to be conducted, the lists concerning cases when a DPIA has to be carried out and which kinds of data processing are exempt, which are to be published by the data protection authorities under Article 35(4) and (5) GDPR have to be consulted.

Projecting the Assessment. If a DPIA is to be carried out, the goals and scope of the assessment should first be laid out. The personnel assigned to carry out the assessment has to have sufficient resources and competence available to achieve an objective analysis. Ideally, the person responsible for the development and implementation should be responsible for carrying out the DPIA.

They should be assisted by a neutral party, such as quality assurance. Where a Data Protection Officer is assigned, he or she has to be consulted according to Article 35(2) GDPR.

Standard Data Protection Model. The Standard Data Protection Model [13] is useful to implement the assessment as envisaged by the European legislator in order to demonstrate that a specific system for data processing is in compliance with the requirements of data protection and identify appropriate safeguards. In order to enable data protection authorities and the public to trace the assessment's results recourse to a predefined list of evaluation criteria and benchmarks, and safeguards can be taken. However, the primary purpose is to ensure transparency as warranted by Article 35(9) GDPR, rather than enable controllers to check off a list instead of assessing the risks for the rights of the individuals in a specific scenario, as will be described in further detail in the evaluation stage below.

Target of Evaluation. The target of evaluation defines the scope of the DPIA. In order to evaluate whether a high risk is likely, the controller has to have an overview of the data processing in question. At this point, the systematic description of the data processing and its purposes, as well as the legitimate interests of the controller according to Article 35(7)(a) GDPR thus has to be prepared. It is paramount that the controller is aware of the extent of the processing operations in order to determine how these may affect the rights of the individual. This includes in particular the data and their formats for storage and transfer (protocols), the information technology (IT) systems used and their interfaces as well as processes, procedures, and functional roles. A DPIA as required by Article 35 GDPR may not be limited to a single component or function, but must describe the predefined object of evaluation in its entirety, including its technical as well as the organizational implementation at the controller level. This concerns any use cases that are to be implemented and should pay particular regard to the purposes of the data processing. Further, it is necessary to comply with data protection principles such as purpose limitation (Article 5(1)(b) GDPR) and data minimization (Article 5(1)(c) GDPR) and, where necessary, competing interests have to be balanced in order to ensure the protection of fundamental rights.

Identification of Actors Involved/Persons Concerned. Equally important as the proper identification of the target of evaluation in this phase is the proper identification of actors involved and persons concerned. Aside from organizations and persons participating in the development or implementation (and thereby potential attackers), all persons affected by the use should be involved, such as

- the manufacturer of the test object,
- operators e.g. as processors (data centers, internet service providers),
- the controller employees,

- the persons concerned in their respective roles as citizens, patients, customers, employees, etc.,
- third parties who take note of personal data, either by chance (persons randomly present) or by intent (security services).

Identification of Relevant Legal Requirements. While the GDPR has a wide scope of application – i.e. whenever an establishment within the EU processes personal data or personal data of data subjects who are in the EU are processed according to Article 3 GDPR – it does not regulate all legal aspects exhaustively. There are provisions which leave the Member States a certain degree of discretion in the implementation of the measures, e.g. for the public sector under Article 2(2) GDPR or the health and social security sector in Article 9(2)(h) GDPR. Furthermore, there may be sector specific national legislation inter alia for the areas of telecommunications, social security, rules on professional secrecy or the protection of minors. However, as a DPIA deals with processes and technical operations, these rules are only of concern if they are implemented directly in the process.

Documentation of Tasks and Issues. The results of the preparation stage have to be documented. This should be done following a standardized procedure in the form of a scoping report.

4.2 Evaluation Stage

Identification of Protection Goals. The requirements of data protection are prescribed by law and can be operationalized as protection goals (as developed in [14–18]) which have proven very effective in IT and information security. This provides a methodology fit to elucidate risks that have to be covered by appropriate measures and safeguards.

Six protection goals have been established (Fig. 2): The classical risks of IT security are incorporated with the first three protection goals (1) availability, (2) integrity and (3) confidentiality.¹ Building on this framework, three additional data protection specific protection goals were formulated: (4) unlinkability, (5) transparency, (6) intervenability.

Availability is the requirement to have data accessible, comprehensible and processable in a timely fashion for authorized entities. Integrity represents the need for reliability and non-repudiation concerning information, i.e. unmodified, authentic and correct data. Confidentiality concerns the need for secrecy, viz. the non-disclosure of certain entities within the IT system in question. Unlinkability ensures data cannot be linked across different domains and/or be used for purposes differing from the original intent. Transparency means that the data

¹ Note that Article 32(1)(b) GDPR, in addition to the classical security goals confidentiality, integrity, and availability, also stipulates the resilience of systems and services processing personal data as an objective.

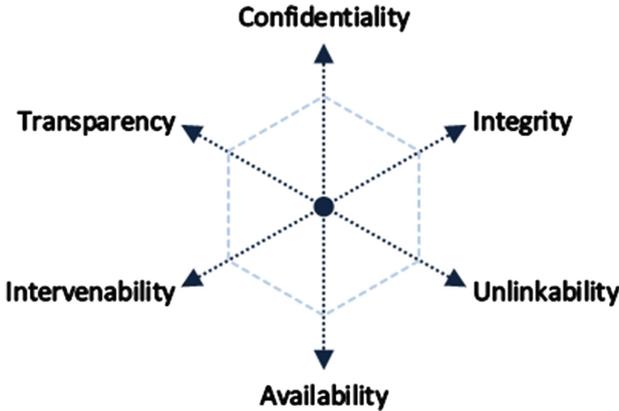


Fig. 2. Protection Goals

subjects have knowledge of all relevant circumstances and factors regarding the processing of their personal data. Lastly, intervenability entails the control of the data subjects, as well as the controller or supervisory authority over the personal data.

Note that the protection goals are meant to represent the perspective of the data subject whose rights are at stake. If, e.g., transparency is violated because the controller does not inform the data subject appropriately as required by law, this has to be tackled in the DPIA: not knowing who processes data for which purpose and being deprived of possibilities to intervene – even if the personal data is kept safe and secure – infringes the data subject’s rights and thus constitutes a risk.

Each protection goal incorporates further, derived protection goals, each of which can be deduced from legal provisions in the GDPR. Alternatively the central principles of data protection law can be assigned to a specific protection goal. However, there are certain legal provisions which cannot be accommodated within the concept, especially the check for lawfulness of processing, which has to be done prior to any Data Protection Impact Assessment.

The protection goals are in a state of dual interplay. This leads to a tension, as usually the strengthening of one protection goal leads to the detriment of its counterpart. The evaluation therefore has to achieve the proper balance between the protection goals. For instance, a system that processes highly confidential data will restrict the access to the data as much as possible, thereby limiting the availability. Still authorized entities should be able to access the data, but depending on the implemented safeguards they may need to undergo a cumbersome process, e.g. applying a four-eye principle and demanding necessary paperwork before access is granted, requiring specific hardware for access of the clear text etc.

Identification of Potential Attackers, Motives and Objectives. While in IT security threats are usually assessed from an organizational point of view, in a DPIA the perspective is that of the persons concerned. Consequently, attackers are not limited to third parties, but can also be rule-abiding internal users of the organization itself, e.g. employees or contractors gaining access to personal data. The goal of a DPIA is, correspondingly, not the protection of business processes but of the rights and interests of an organization's customers, employees, etc. Thus, it has to be ascertained whether the following organizations pose a risk to the rights and interests of the individual

- Public authorities, e.g.
 - Security services: Department of State, police, intelligence services, military, etc.
 - Public benefit administration, i.e. social security services
 - Statistics agencies
 - Failing authorities, which open spaces for illegal activities
- Enterprises, e.g.
 - Technology companies, system integrators, IT providers (access, content, etc.)
 - Banks, insurance companies
 - Credit agencies, address and data trading companies
 - Advertising agencies
 - Advocacy groups and lobbyists
 - Employers
- Health care, e.g.
 - Hospitals, doctors
 - Public and private health insurers
- Research, e.g.
 - Medical, social research
 - Universities

There is, of course, a conflict of interest when the organization conducting the DPIA is also seen as a serious risk for data protection. In order to avoid any blind spots in the risk evaluation, there should at least be retroactive external supervision. Further, an organization's data protection officer, where one is appointed, is by definition expected to take the point of view of the persons affected by the processing.

Identification of Evaluation Criteria and Benchmarks. Every processing of data, even if it is entirely in compliance with the legal requirements, is an interference with the individual's rights to private life and data protection as guaranteed by Articles 7 and 8 CFR. Therefore, while the IT-Grundschutz methodology [19] developed by the German Federal Office for Information Security (BSI) has demonstrated its value in practice, the standard of protection cannot be simply measured in severity of damage and likelihood of occurrence categories when it comes to data protection. As every processing interferes with

fundamental rights and thus has to be justified and assessed under the conditions of Articles 8(2) and 52(1) CFR in order to be in accordance with the law, it follows that the level of protection has to be normal by default, as detailed below. Due to the pivotal nature of fundamental rights and the fact that their protection is the very basis of data protection law, a lower level must not be considered. However, depending on the use of specific data or kinds of processing, the intensity of interference can rise to a high or very high level. The three protection standards are thus

- Normal: personal data are processed and there are no scenarios in which the nature of the processing shows potential for a high intensity of interference.
- High: special categories of personal data according to Article 9 GDPR are processed and thus require a high protection standard by law and/or the persons concerned depend on the decisions/services of the organization, if
 - the high intensity of interference of the data processing can lead to serious consequences for the persons concerned and/or
 - there are no effective safeguards, methods of intervention for the persons concerned (including the availability of judicial redress).
- Very high: personal data requiring a high protection standard are processed and the person concerned depends on the decisions/services of the organization to an existential level and there are additional risks posed by insufficient data security or illegitimate changes of the purposes of processing, which the persons concerned cannot become aware of and/or correct by themselves.

Additionally, a high protection standard may be required when there is a cumulative effect of various aspects of the data processing, which by themselves do not demand a high level. This may be the case where data from a large group of persons are collected or when data from fewer persons are collected for various purposes and persons concerned are affected in various roles.

Evaluation of the Risk. At the core of the evaluation is the comparison of the controller’s envisaged measures or those determined in the course of the assessment with a catalogue of reference measures (Fig. 3). Currently, the technical working group of the conference of German data protection authorities (AK Technik) is developing a catalogue of such data protection measures [20].

Table 1 contains selected measures which – when implemented correctly – can ensure the safeguarding of the protection goals as detailed above in Fig. 2. While this list is generic, the measures taken may have to be updated in line with the advance of the state of the art, as referred to in Recitals 78 and 83 and Articles 25(1) and 32 GDPR. Additionally, due to its generic nature the list cannot be used as a mere checklist. The mere implementation of a listed measure does not satisfy the risk evaluation. For instance, a system, to ensure confidentiality, may implement a rights and roles concept. However, this alone cannot satisfy the requirement of confidentiality. If the rights are granted overly generous and roles are not clearly separated, the concept is not effective. Therefore, the controller will have to explain how the rights and roles concept of the specific system in question ensures confidentiality of the data processed.

Table 1. Examples of generic protection measures

Protection goal	Component	Measure
Ensuring availability	Data, systems, processes	Redundancy, protection, repair strategies
Ensuring integrity	Data	Comparing hash values
	Systems	Limitation of write permissions, regular integrity checks
	Processes	Setting references values (min/max), control of regulation
Ensuring confidentiality	Data, systems	Encryption
	Processes	Rights and roles concepts
Ensuring unlinkability through definitions of purposes	Data	Anonymity, pseudonymity, attribute-based credentials
	Systems	Separation (isolation) of stored data, systems and processes
	Processes	Identity management, anonymity infrastructures, audits
Ensuring unlinkability through definitions of purposes	Data	Documentation, logging
	Systems	System documentation, logging of configuration changes
	Processes	Documentation of procedures, logging
Ensuring intervenability through anchor points	Data	Access of persons concerned to their data (information, rectification, blocking, deletion)
	Systems	Off-switch
	Processes	Helpdesk/single point of contact for modification/deletion, change management

In the course of the risk evaluation any deviances from the reference measures have to be assessed in the light of their gravity and in how far they compromise the protection goals. Turning back to the example of the rights and roles concept, this means that if the controller did not even implement such a basic measure, it is *prima facie* doubtful whether the system can satisfy the requirement of confidentiality. Where the analysis demonstrates such failures to comply with protection goals, such a finding – from the viewpoint of a data protection authority – leads to an assumption of deficiencies in data protection and has to be redressed. The data protection authority in its consultancy role may provide advice on remedies.

In practice it can easily be ascertained if criteria and benchmarks have not been satisfied through recourse to this model, as the envisaged measures and the quality of the implementation according to the protection standard will be missing. If different measures are chosen, the assessment may be more complex

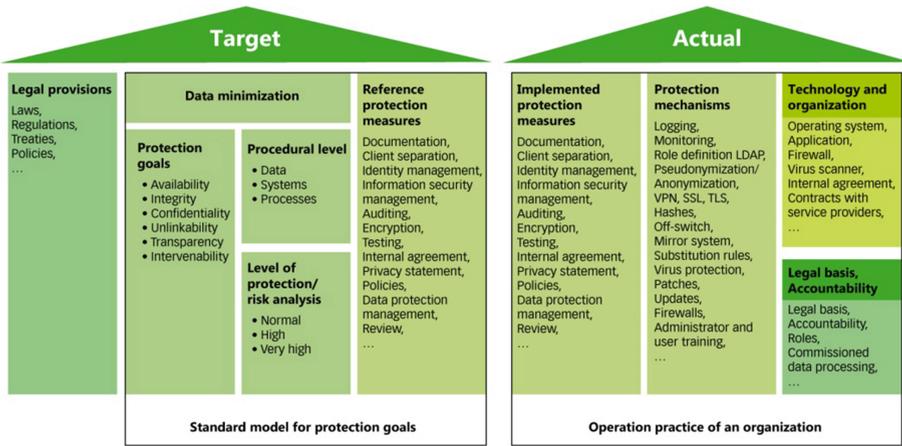


Fig. 3. Risk-assessment through target/actual comparison

and a proof of appropriateness and at least equivalence to the reference measure will have to be provided.

Taking into account the proper measures identified at this stage, the necessity and proportionality of the data processing envisaged by the controller can be assessed, as prescribed by Article 35(7)(b) and (c).

4.3 Report and Safeguards Stage

Identification and Implementation of Appropriate Safeguards. Based on the results of the evaluation, a plan for risk management has to be prepared. According to Article 35(7)(d) GDPR the DPIA must contain measures to remedy the risks identified including safeguards, security mechanisms and measures to protect the personal data, as detailed above with regard to the reference measures, and demonstrate compliance with the GDPR as a whole. Particularly with regard to the rights of individuals it is not acceptable to follow a de minimis approach and rank risks for these rights as acceptable when only few persons are concerned. However, there is the possibility to prioritize risks and take those measures with the highest benefit for the persons concerned in compliance with legal requirements. The action plan should explicitly detail

- which safeguards are taken to reduce the gravity of or avoid interference with fundamental rights or specific harm for the persons concerned,
- who is responsible to implement the safeguards and the persons to be consulted,
- by when these safeguards are to be implemented and which resources are available,
- the criteria to measure the results of the safeguards, and
- who is responsible to evaluate and document these criteria.

The selection of appropriate safeguards is facilitated by the list of generic safeguards as provided above for risk assessment (Sect. 4.2).

Documentation and Publication of a Report on Evaluation Results.

In order to achieve the intended effects of a DPIA it is necessary to comprehensively document and publish a report on the findings. Like the scoping report it should follow a standardized form to facilitate evaluation and comparison by data protection authorities, enterprises and the public. For the latter, a special version of the report, excluding any business secrets, may be created. Nonetheless, such a shortened version must not be used to conceal negative findings, but should be subject to legitimate and documented grounds.

Auditing of Evaluation Results. In order to ensure that the DPIA has been duly conducted, the DPIA report should be evaluated by an independent third party – where appropriate also the competent data protection authority. This includes especially an appropriate handling of conflicts of interest, taking due regard of the rights and interests of the persons concerned when selecting safeguards, adequate information of the public and ensuring that the envisaged safeguards are actually implemented.

Supervision and Continuation. A DPIA is not a singular and linear process, but rather has to be repeated to ensure continuous supervision over the lifetime of a project. Accordingly, Article 35(11) GDPR calls for a review at least when there are changes in the risks posed by the processing of data. Such changes may occur whenever organizational or legal conditions change or new risks for data protection in general are identified. It then has to be ensured that the safeguards chosen are able to adapt to these changes.

5 Conclusions

Although DPIA is a relatively new instrument in most of the Member States, it can be extremely helpful to identify risks for the rights of persons concerned by the use of new data processing technology. It can be regarded as an early warning system enabling all actors to systematically address potential deficiencies in a process. Controllers can foresee risks and their causes and are thus enabled to distribute responsibilities and competences accordingly in order to implement data protection at the core of the operations. A DPIA allows for better decision-making at the implementation stage and avoids the need for costly subsequent improvements or potential leaks of personal data. Thus, for controllers it is an important instrument to demonstrate the compliance with legal requirements and can build trust between the controller and its customers, who are empowered to make informed decision when using the controller's services. A standardized DPIA procedure also helps data protection authorities to find weaknesses and

legal infringements, but also allows for a better overview on best practices which is important to advise controllers on how to improve their products or processes.

Once the legal obligation to carry out a DPIA comes into force in 2018, a standard will be required to ensure an effective implementation of this legislation. With the interdisciplinary methodology proposed in this paper, which is based on and expands components that have been implemented successfully in practice, the full potential of DPIA can be realized. This is particularly true with regard to the importance of fundamental rights protection as the *raison d'être* of data protection legislation, as can be seen *inter alia* from Recitals 1–4, 10, 47, 51–53, 102 and Article 1(2) GDPR, which is achieved by the incorporation of the data protection goals in the process. Through their operationalization with regard to the new data protection framework, this methodology provides a convenient instrument for controllers to assess risks and enables them to offer better services and improves their ability to compete in a market for privacy-friendly solutions, which also incorporates the requirements imposed by the upcoming EU legislation.

Acknowledgement. This paper was partially funded by the European Commission under the 7th Framework Programme, grant agreement no. 261698 (SAPIENT project) and the Bundesministerium für Bildung und Forschung (German Federal Ministry of Education and Research) for the project Forum Privatheit – Selbstbestimmtes Leben in der Digitalen Welt (Privacy-Forum), www.forum-privatheit.de.

References

1. European Commission: Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. OJ L 122/47 of 16 May 2009. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009H0387&from=EN>
2. European Commission: Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems. OJ L 73/9 of 13 March 2012. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012H0148&from=EN>
3. Article 29 Working Party: Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. WP 175 (2010). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp175_en.pdf
4. Article 29 Working Party: Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force. WP 209 (2013). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf
5. Wright, D., De Hert, P. (eds.): Privacy Impact Assessment. Springer, Heidelberg (2012)
6. ISO/IEC 29134: Information technology – Security techniques – Privacy impact assessment – Guidelines. ISO/IEC, International Organization for Standardization (2016)

7. ICO (Information Commissioner's Office): Conducting privacy impact assessments code of practice. ICO (2014). <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>
8. CNIL (Commission Nationale de l'Informatique et des Libertés): Privacy Impact Assessment: Methodology (how to carry out a PIA). CNIL (2015). <http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf>
9. Friedewald, M., Bieker, F., Nebel, M., Obersteller, H., Rost, M.: Datenschutz-Folgenabschätzung - Ein Werkzeug für einen besseren Datenschutz. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe (2016). <https://www.forum-privatheit.de>
10. Wright, D., Gellert, R., Bellanova, R., Gutwirth, S., Langheinrich, M., Friedewald, M., Hallinan, D., Venier, S., Mordini, E.: Privacy Impact Assessment and Smart Surveillance: A State of the Art Report, Deliverable 3.1 SAPIENT Project (2013). <http://www.sapient-project.eu>
11. Wadhwa, K., Rodrigues, R.: Evaluating privacy impact assessments. *Innov. Eur. J. Soc. Sci. Res.* **26**(1–2), 161–180 (2013)
12. Wright, D., Friedewald, M., Gellert, R.: Developing and testing a surveillance impact assessment methodology. *Int. Data Priv. Law* **5**(1), 40–53 (2015)
13. AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Schulz, G., Rost, M.: Das Standard-Datenschutzmodell – der Weg vom Recht zur Technik: Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen (2015). https://www.datenschutzzentrum.de/uploads/sdm/SDM_Tagungsband2015_Hannover.pdf
14. Hansen, M., Jensen, M., Rost, M.: Protection goals for privacy engineering. In: 2015 International Workshop on Privacy Engineering (IWPE), Security and Privacy Workshops (SPW), pp. 159–166. IEEE (2015)
15. Rost, M., Pfitzmann, A.: Datenschutz-Schutzziele - revisited. *DuD - Datenschutz und Datensicherheit* **33**, 353–358 (2009)
16. Rost, M., Bock, K.: Privacy by Design and the New Protection Goals, EuroPriSe Whitepaper (2011). <https://www.european-privacy-seal.eu/AppFile/GetFile/ca6cdc46-d4dd-477d-9172-48ed5f54a99c>
17. Hansen, M.: Top 10 mistakes in system design from a privacy perspective and privacy protection goals. In: Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., Russello, G. (eds.) *Privacy and Identity 2011*. IFIP AICT, vol. 375, pp. 14–31. Springer, Heidelberg (2012)
18. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Le Métayer, D., Tirtea, R., Schiffner, S.: Privacy and Data Protection by Design - from policy to engineering, ENISA (2014). https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/at_download/fullReport
19. Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security): BSI-Standard 100-2, IT-Grundschutz Methodology (2008). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard.100-2_e.pdf.pdf
20. Probst, T.: Generische Schutzmaßnahmen für Datenschutz-Schutzziele. *DuD - Datenschutz und Datensicherheit* **36**, 439–444 (2012)



<http://www.springer.com/978-3-319-44759-9>

Privacy Technologies and Policy

4th Annual Privacy Forum, APF 2016, Frankfurt/Main,
Germany, September 7-8, 2016, Proceedings

Schiffner, S.; Serna, J.; Ikonomou, D.; Rannenber, K.
(Eds.)

2016, XIV, 203 p. 38 illus., Softcover

ISBN: 978-3-319-44759-9