Data Protection Impact Assessments (DPIAs) in the law enforcement sector according to Directive (EU) 2016/680 - A comparative analysis of methodologies

VERSION 1.0

Date submitted:

Dissemination Level: PU / ~~PP / RE / CO~~

DPIA framework prepared by:

- ULD (Eva Schlehahn)
- KUL (Thomas Marquenie, Els Kindt)

The research leading to these results has received funding from the European Union
Seventh Framework Programme (FP7/2007-2013) under grant agreement no FP7-IP-608142.

Programme:	FP7 Theme 10: Security
Grant Agreement No.	FP7-IP-608142
Project Acronym:	VALCRI – Visual Analytics for sense-making in Criminal Intelligence Analysis
Project Co-ordinator:	Middlesex University – Professor B.L. William Wong

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium participants (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of Contents

I. Introduction

[redacted]Context

As policing and law enforcement activities are becoming increasingly technology-based and supported by big data analytics and automated decision-making, notable concerns have been raised regarding the risks and potential negative consequences introduced by the further reliance on advanced analytical systems. It is in this light that the upcoming European Directive 2016/680 regarding data protection in the area of law enforcement and criminal justice (DPLED) requires law enforcement agencies to conduct a data protection impact assessment (hereafter referred to as a DPIA) to analyse the risks and consequences of technological advancements and personal data processing in order to implement adequate mitigation techniques. While there exist ample guidelines and templates for private, commercial and certain governmental actors to conduct such an assessment, comparatively little attention has been paid to the unique nature of law enforcement activities and how such an impact analysis can or should be performed by police actors.

As such, it is one of the goals of the European FP7 Project VALCRI (Visual Analytics for Sense-making in Criminal Intelligence Analysis) to draft an innovative methodology and overview of the impact assessment process specifically aimed at law enforcement end users of both VALCRI and other advanced analytical systems. Due to the fact that the VALCRI project concludes in the same timeframe of the DPLED entering into effect, it is expected that these guidelines are among the first to exist specifically for law enforcement under the new legislation.

This project involves the creation of a visual analytics-based sense-making capability for criminal intelligence analysis by developing and integrating a number of technologies into a coherent working environment. VALCRI is being developed as a new system for information management and evaluation by intelligence analysts in law enforcement agencies (LEAs). In order to assist law enforcement officials in their task of analysing criminal intelligence, the VALCRI system will serve as a working space which extracts meaningful information from text, documents, images and video, detects patterns and presents such data in an accessible and insightful way to its user. By coupling visualization and computation, VALCRI seeks to connect the dots and make connections often missed by humans. From data exploration to data analysis and ultimately hypothesis, the system guides and assists the user in the criminal investigation by providing an interface fit for the examination of all available information.

Within VALCRI, the Security, Ethics, Privacy and Legal (SEPL) group has been dedicated to researching how advanced analytical systems intended for law enforcement use can be developed and deployed in an ethical and legally compliant manner. This research, much of which has been disseminated and made publically available through designated White Papers, panel discussions and articles published in peer reviewed journals, has covered a number of key issues ranging from assessing compliance with police protocol and developments in legislation regarding data protection, privacy and non-discrimination, to providing concrete guidance and input on aspects of the development of the system such as transparency, accountability, security and integrity. As the knowledge gained throughout the project has resulted in valuable insights regarding the risks and potential impacts of utilizing and developing systems like VALCRI, the SEPL work will culminate in these guidelines for law enforcement actors and in particular the VALCRI end users on conducting a data protection impact assessment and achieving legal compliance with the upcoming DPLED. Due to the fact that the SEPL group has been closely involved with the development of the VALCRI system and the new legislation from its conception, a particular expertise has been formed. This provides benefits for the VALCRI project itself, as the existence of impact assessment guidelines drafted by an expert group with extensive knowledge of the system will facilitate its use and support the end users in achieving legal compliance, as well as for other actors involved in the development and use of police technologies.

[redacted]Scope and purpose of DPIA guidelines for advanced analytical systems

Under the recently reformed European data protection legislation, a data protection impact assessment (DPIA) will soon be required from private, commercial and governmental actors when they engage in certain activities processing personal data. According to the Working Party 29 Guidelines, a DPIA can be defined as the "process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data4 by assessing them and determining the measures to address them."[1] In other words, a DPIA should be considered a tool for building and demonstrating compliance with data protection laws, as well as for assisting data controllers with the processing of personal data in a lawful and accountable way.

As mentioned above, the existing DPIA templates and guidelines at the national and European level place their focus almost entirely and exclusively on the implications of the provisions of the GDPR for commercial, private and certain governmental actors. While certain aspects of these guidelines can similarly be applied in the context of law enforcement and criminal justice, high profile guidance tailored specifically to the police sector does not yet appear to exist. This report, of which this first section focuses on conducting an analysis and comparison of national approaches to DPIA's, aims to fill that gap. Its scope is therefore to first compare different methodologies of conducting a DPIA and present the findings thereof, and second to distil their core components and draft a methodology that furthers the common European approach and focuses specifically on law enforcement activities. As the first section of the document covers the analysis and comparison of national approaches to DPIA's, the second will contain a detailed overview of the requirements to be met and steps to be taken for a satisfactory and complete impact assessment to be completed. These guidelines and the overview of national methodologies shall therefore serve as a tool to assist police agencies when conducting of a DPIA, in particular when it is aimed at the implementation of new and intelligent technologies like VALCRI.

As such, it needs to be noted that this report does not cover surveillance and intelligence services due to the significant divergence of national legislation and the non-applicability of the new European legislation requiring DPIA's to be conducted.

DISCLAIMER

Neither the VALCRI project nor the authors of this document shall be held responsible, liable or accountable for the outcome of the data protection impact assessments conducted by law enforcement officials or system end users. The responsibility to comply with data protection law lies on the data controller. As achieving full compliance with legal obligations requires a thorough analysis of the specific situation, organizational structure and processing practices of the national or regional police authorities, the methodology provided in this document should be seen as an overview of good practices, measures and steps towards conducting a proper and satisfactory impact and risk assessment. The following chapters are general guidelines providing end users with recommendations, resources and procedures to allow and support an adequate DPIA being conducted. The mere reference to or reliance on this document alone does not constitute the approval of any system nor does it guarantee legal compliance. It remains the sole responsibility of the data controller to properly conduct the assessment as is prescribed by national law.

[1] Article 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 17/EN WP248 rev.01, 4 April 2017 (revised on 4 October 2017), p.4.

[redacted] Methodology

As mentioned above, the aim of these guidelines is to draft a methodology and step-by-step procedure that can be followed by VALCRI end-users and police agencies implementing new technologies to conduct an adequate DPIA and achieve legal compliance. To achieve this, this first section of the report consists of a comparative analysis and summary of several notable DPIA guidelines and templates at the national and European level. The consulted methodologies will include the Article 29 Working Party Guidelines[2], the German SDM (Standard Data Protection Model)[3], the Spanish Practical Guide for the Assessment of Impact and Protection of Data Subjects[4], the French CNIL Privacy Impact Assessment Methodology[5] and software tool[6], the UK ICO GDPR DPIA Guidance[7] and the Belgian DPIA Guidelines[8]. Following the overview and summary of these different approaches to the DPIA, key findings shall be presented and used to draft a new methodology in section two that focuses in particular on law enforcement data processing activities and draws upon the national guidelines and their key aspects to arrive at a comprehensive process built around the different strengths of the existing methodologies. Where appropriate, reference shall be made to the European Project PIAF (Privacy Impact Assessment Framework) which has in the past compiled and analysed all Privacy Impact Assessments in the European Union.

II. Data Protection Impact Assessments and Directive (EU) 2016/680

[redacted] Data Protection Impact Assessment Requirements

In 2016, the European Union legislator concluded its long-awaited data protection reforms and adopted two new pieces of legislation. It's these legal instruments, being the General Data Protection Regulation[9] (GDPR) and the Data Protection Law Enforcement Directive[10] (DPLED or Directive 2016/680), that introduced the current concept of the data protection impact assessment. As described in the previous chapter, the purpose of the DPIA is to support the building and demonstrating of compliance by assessing risks and implementing appropriate measures and mitigation techniques. To this end, the DPLED sets out the circumstances under which a DPIA must be conducted and the minimum requirements that the process must meet for the law

[2] Article 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 17/EN WP248 rev.01, 4 April 2017 (revised on 4 October 2017).

[3] Conference of the Independent Data Protection Authorities of the Bund and the Länder, Standard Data Protection Model, as adopted by the Conference of the Independent Data Protection Authorities of the Bund and the Länder, Kühlungsborn, 9-10 November 2016.

[4] Agencia Española de Protección de Datos, Guía práctica para Las Evaluaciones de Impacto en la Protección de Los datos sujetas al RGPD, 2018.

[5] Commission Nationale de l'Informatique et des Libertés (CNIL), Privacy Impact Assessment (PIA) Methodology, Feburary 2018 edition.

[6] https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

[7] Information Commissioner's Office, Consultation: GDPR DPIA Compliance, Version March 2018.

[8] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, "Ontwerp van aanbeveling uit eigen beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging voorgelegd voor publieke bevraging, CO-AR-2016-004, 20 December 2016.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

enforcement data controller to achieve legal compliance. This section will refer to the relevant provisions of the legislation and provide a brief explanatory overview of the text and the requirements therein. In the DPLED, the relevant provisions are article 27 and recital 58.

Art. 27 Directive (EU) 2016/680:

> *Data protection impact assessment*
>
> *1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.*
>
> *2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.*

Rec. 58 Directive (EU) 2016/680:

> *Data protection impact assessment*
>
> *A data protection impact assessment should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes, which should include, in particular, the measures, safeguards and mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with this Directive. Impact assessments should cover relevant systems and processes of processing operations, but not individual cases.*

First, article 27.1 details when and under what circumstances a DPIA must be conducted. This is the case when a processing activity is likely to result in a high risk to the rights and freedoms of natural persons. While the law does not provide a definition of what constitutes an operation that is “likely to result in a high risk”, it is expected that the controller acts with due diligence and conducts a thorough assessment of how the planned processing activities might risk negatively affecting the data subjects. Among others, the rights and interests of privacy, due process and non-discrimination must be considered in this sense. Particularly in the instance in which the processing involves the use of new technologies, it is increasingly likely that the processing should be considered as high risk. To determine whether or not it is indeed a high risk, the data controller must take into account the nature, scope, context and purpose of the processing when considering its potential impact. In other words, when the particular circumstances or technologies of the processing of the personal data suggest that there might be a significant risk that the rights of the data subjects can be negatively affected, the data controller is under the obligation to conduct a data protection impact assessment prior to the processing.

Following this, article 27.2 provides the minimum requirements that a DPIA must meet in order to achieve legal compliance. As such, the DPIA must contain a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of the data subjects, and the planned counter-measures, safeguards and security mechanisms to protect the personal data and to demonstrate compliance. Recital 58 provides further explanation and states that the impact assessment should cover relevant systems and processing of processing operations, but not individual cases. The latter is to be interpreted as meaning that the DPIA refers to evaluating the organization and practices rather than assessing particular cases of processing and policing. Taking into account the rights and legitimate interests of the persons involved, it is therefore up to the data controller perform a full assessment of the processing activities and systems used, the potential risks and impacts involved, and the measures to be taken to mitigate the risks and protect the personal data and rights of the persons involved.

An analysis of the risk-based approach and the protection of fundamental rights that underlies the DPIA process can be found in the section below. A complete overview of the DPIA process, including the pre-assessment of the reasons to perform a DPIA, the practical steps to be taken, the evaluation of risks and the determination of safeguards, is included in the full version of this report.

[redacted]Risk-based approach and the protection of fundamental rights

With the new European data protection framework, an increased emphasis on the risk-based approach for DPIA is evident. Therefore, it is crucial to understand what exactly 'risk' in the sense of Directive (EU) 2016/680 means.

The ultimate goal of a DPIA is to minimize the risks to the rights and freedoms of the data subject.[11] With the background of the European fundamental rights, especially Art. 8 of the Charter of Fundamental Rights (CFR) of the European Union must be taken into account. However, the right to the protection of personal data cannot be seen isolated. Rather, this right is not a purpose in itself, but had been manifested with the intention of protecting the individuals to whom the personal data relates to. Insofar are the other fundamental rights of individuals of importance as well, such as the right to private and family life (Art. 7), the right to freedom of expression and information (Art. 11), the right to freedom of assembly and association (Art. 12), or the right to non-discrimination (Art. 21).[12]

Therefore, when determining risks to the rights of freedoms of the data subject, the perspective of the individual is the central aspect of the assessment. This is an important difference especially with regard to risk assessments in the IT security domain, which are primarily focused on the protection of the data controller's organisation and its assets. While many technical and organisational measures may also serve the purpose of protecting the personal information of the data subject as well, it is not always so. For example, in IT security, the data processing entity (controller) itself is often neglected as a potential attacker. Therefore, data protection requires a different viewpoint to identify effective operational measures specifically aimed at reducing or even eliminating the impact on the fundamental rights of individuals whose personal data is processed.

Recital 51 of Directive (EU) 2016/680 clarifies that the damage that may result of a risk can be not only physical and material, but also non-material. It gives a large number of examples for different types of damage for the data subject, such as:

- discrimination,
- identity theft or fraud,
- financial loss,
- damage to the reputation,
- loss of confidentiality of data protected by professional secrecy,

[11] The term '*rights and freedoms'* can also be found in Art. 52 paragraph 1 of the Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000, p. 1–22. It is synonymous with the same term in the European Convention of Human Rights, describing the entirety of the European fundamental rights.

[12] Cf. also the argumentation of the Court of Justice of the European Union (CJEU) in the data retention case, where the court first examined Art. 7 CFR, then stated that the retention of personal data also falls within the application scope of Art. 8 CFR, thereby taking a holistic approach examining potential infringement on the rights and freedoms of natural persons: joined Cases C‑293/12 and C‑594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* - Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof, Judgment of the Court (Grand Chamber), 8 April 2014, ECLI:EU:C:2014:238, see paragraph 29.

- unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage,
- deprivation of the data subjects of the own rights and freedoms or from exercising control over their personal data,
- personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership,
- genetic data or biometric data are processed in order to uniquely identify a person or data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed,
- personal aspects are evaluated, in particular analysing and predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles,
- personal data of vulnerable natural persons, in particular children, are processed,
- the processing involves a large amount of personal data and affects a large number of data subjects.

The extensive listing of these examples underline that the risk may not only mean some kind of specific material damage, but is already manifested by the interference with a fundamental right of an individual. This interpretation is supported by a comparison with Recital 94 sentence 2 of the General Data Protection Regulation (GDPR)[13], which clarifies that in case of a high risk, this '*may result also in a realisation of damage or interference with the rights and freedoms of the natural person*'.

This conversely shows that in fact each collection and processing of personal data constitutes by itself interference on the right to the protection of personal data derivable from Art. 8 CFR. This viewpoint is moreover supported by the settled jurisprudence of the CJEU, which also assumes fundamental rights interference already once personal data is being collected and processed.[14] The settled case-law thereby emphasizes that in this context, it is irrelevant whether the personal data is particularly sensitive or whether the data subject has experienced substantive detriments.[15] This viewpoint has been laid down also in Directive (EU) 2016/680 through the principle of prohibition with permission reservation, meaning that always a legal ground is required to collect and process personal information lawfully.[16]

Therefore, addressing risk must be aimed at reducing the level of interference as much as possible. However, the determination of risk is stuck in kind of circular argumentation in Directive (EU) 2016/680; according to Recital 52 in the directive, the risks are meant to have different levels of likelihood and severity. Together with the above cited list of potential damages materializing the risk, it must be assumed that the risk assessment actually consists of two steps, namely assessing

- the likelihood and severity of the risk with regard to a possible physical, material or non-material damage and
- the fundamental rights interference due to the processing in itself.

With regard to an interference on Art. 8 CFR, while it encompasses also the former category of risks, a specific determination of likelihood is obsolete since already with the collection of personal information, the probability of occurrence is always 100%. Therefore, this interference on a fundamental right of a natural

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[14] Cf. the CJEU judgement in the joined cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen* of 9 November 2010, ECLI:EU:C:2010:662, see paragraphs 60-63.

[15] CJEU judgement in joined cases C-465/00, C-138/01 and C-139/01 *Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk* of 20 May 2003, ECLI:EU:C:2003:294, see paragraph 75.

[16] Art. 8 Directive (EU) 2016/680.

person is to be seen as a risk occurred. The impact of this interference then needs to be reduced by tangible technical and organisational measures to the lowest possible level. Once sufficient technical and organisational are identified and implemented the personal data processing still remains interference, if only then a legitimate and acceptable one.

In chapter 3.4 (Evaluation of risks), a more detailed description of individual risks is presented and can be used as a starting point for the DPIA. In general, its results should not be seen as a theoretical conclusion. Rather, the DPIA outcomes need to convey a very concrete imperative for the controller how to handle the intended processing operation when taking into account the above mentioned risks. This is particularly focused on how to determine technical and organisational measures and procedures to protect the data subject's personal data. Recital 53 of Directive (EU) 2016/680 emphasizes this very clearly:

> '*Where the controller has carried out a data protection impact assessment pursuant to this Directive, the results should be taken into account when developing those measures and procedures.*'

As a consequence, a DPIA is by its nature a tool to determine the needed technical and organisational measures to provide for legal compliance with Directive (EU) 2016/680. Any change of the processing operation must lead to a review and eventually adaption of the risk assessment. Therefore, the DPIA is never static and definitely concluded. Rather, it advisable to establish view the DPIA as a classical PDCA cycle[17] or to integrate an iterative process such as suggested by the Article 29 Working Party.[18]

III. Privacy Impact Assessment Methodologies Overview

Directive (EU) 2016/680 does not provide for a specific methodology to follow to conduct a DPIA. Rather, controllers may conduct a DPIA with an own chosen framework, as long as it is compliant with the general requirements of a DPIA according to Article 27, complemented by Recital 58 of Directive (EU) 2016/680.

Nonetheless, a number of DPIA frameworks exist, ranging from generic ones suggested by EU data protection authorities (DPA's), to non-European and sector-specific PIA approaches.

This section will present a brief overview of existing privacy impact assessments (PIA) used in several European Union member states and of other PIA frameworks, such as from Anglo-Saxon jurisdictions. Countries covered in this section are:

- Germany
- United Kingdom
- Belgium
- France
- Spain

In all of these above mentioned countries, the DPIA methodologies need to be aligned to the general requirements for a DPIA in the police and justice sectors as laid down in Art. 27 Directive (EU) 2016/680. The minimum elements of a DPIA, according to Art. 27 para. 2 Directive (EU) 2016/680, are at least the following:

- A general description of the envisaged processing operations
- An assessment of the risks to the rights and freedoms of data subjects

[17] PDCA stands for 'plan –do – check – act', which is an acknowledged iterative management methodology to control and continually improve processes and products, cf. Tague, Nancy R., '*The Quality Toolbox*', Second Edition, ASQ Quality Press, 2005, pages 390-392.

[18] Cf. Article 29 Working Party, 17/EN WP248 rev.01, 4 April 2017 (revised on 4 October 2017), page 16.

- The measures envisaged to address those risks,
- The safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Directive (EU) 2016/680, while taking into account the rights and legitimate interests of the data subjects and other persons concerned

As the following subsections will show, many of these methodologies have similarities and overlaps, while there are sometimes fundamental differences in the details. However, a synthesis of these methodologies appears thinkable, which could be subject to future research as well.

[redacted] Germany

In Germany, the national DPA's have published an officially acknowledged DPIA framework called the 'Standard Data Protection Model' (hereinafter referred to as SDM).[19] While the current version of the SDM handbook addresses mainly the GDPR requirements for DPIA, this framework has already been analysed and found to be also compliant with the provisions of Directive (EU) 2016/680.[20]

The key concept of the SDM is an approach using protection goals to identify needed technical and organisational measures to ensure that the envisioned personal data processing is compliant with the European data protection framework. Already known in IT security is the so-called CIA triad for the protection goals confidentiality, integrity, and availability, which is commonly used to conduct risk assessments. However, a data protection impact assessment is not required to convey the perspective of the controller. Instead, it must take the perspective of the data subject and his/her fundamental rights to ensure adequate protection, even from the controller conducting the processing. Therefore, these first three protection goals have been complemented by additional ones in the German model. Briefly summarized, the additional data protection goals unlinkability (incl. data minimisation), intervenability, and transparency complement the initial set of protection goals (see figure below).

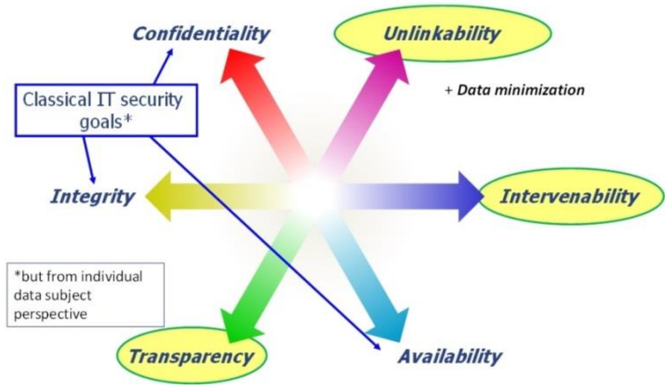


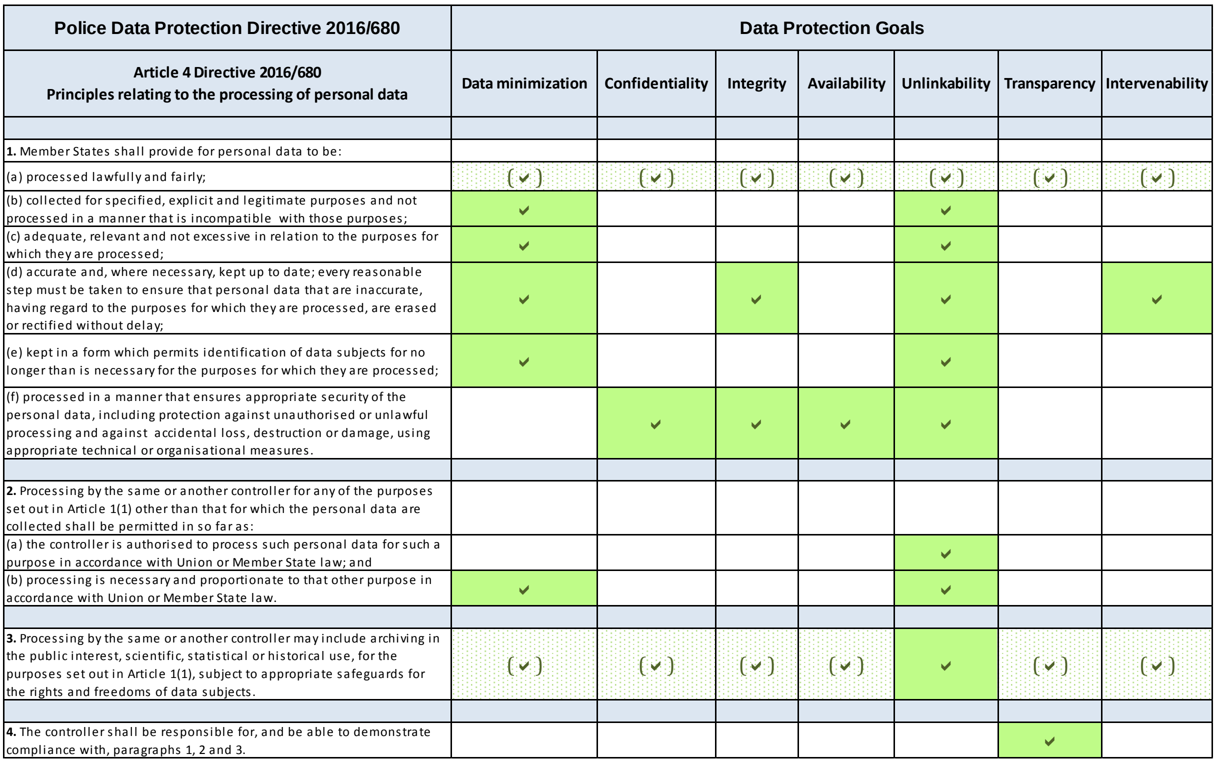
Figure 1: Six data protection goals, integrating the classical IT Security goals in the German DPIA model

[19] '*The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals*', V.1.0 – Trial version. This is an unanimously and affirmatively framework acknowledged (under abstention of Bavaria) by the 92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn on 9-10 November 2016. See for a very first English version: https://www.datenschutzzentrum.de/sdm/. A second and improved English version is currently in the works.

[20] Cf. Schlehahn, E., '*Die Methodik des Standard-Datenschutzmodells im Bereich der öffentlichen Sicherheit und Justiz*', analysis published in DuD (Datenschutz und Datensicherheit) issue 01/2018, pages 32-36.

These protection goals are primarily derived from the key provisions of the GDPR, whereas mostly are mentioned already as principles in Article 5 GDPR, namely integrity, availability, confidentiality, transparency and data minimization. Despite unlinkability and intervenability not being mentioned there explicitly, those two protection goals are manifested at least inherently through numerous provisions, mostly in the context of purpose limitation, data deletion, data portability and through the data subject's rights.[21]

For Directive (EU) 2016/680 setting the framework to implement rules for personal data processing in the police and justice sectors on national level, it has been proven in detail that these protection goals are anchored there as well.[22] This is also due to the fact that many fundamental principles for the protection of personal information known already for quite some time in Europe have been introduced both into the GDPR as well as into Directive (EU) 2016/680. The table below shows in an exemplary way how the individual protection goals are manifested in Article 4 of Directive (EU) 2016/680:



Police Data Protection Directive 2016/680	Data Protection Goals						
Article 4 Directive 2016/680 **Principles relating to the processing of personal data**	Data minimization	Confidentiality	Integrity	Availability	Unlinkability	Transparency	Intervenability
1. Member States shall provide for personal data to be:							
(a) processed lawfully and fairly;	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)	(✓)
(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;	✓				✓		
(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;	✓				✓		
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	✓		✓		✓		✓
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;	✓				✓		
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.		✓	✓	✓	✓		
2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:							
(a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and					✓		
(b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.	✓				✓		
3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.	(✓)	(✓)	(✓)	(✓)	✓	(✓)	(✓)
4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.						✓	

Figure 2: Example mapping of data protection goals to Article 4 Directive (EU) 2016/680

The German SDM sees protection as the link between the legal requirements in GDPR (or Directive (EU) 2016/680) and the technical plus organisational circumstances of a personal data processing operation. Therein, protection goals function as intermediary between often rather abstract, vague and complex norms and tangible functions and protection measures. They are intended to help a controller identify and determine technical and organisational measures to reduce the impact of a personal data processing activity. The GDPR as well as Directive (EU) 2016/680 both demand the implementation of appropriate technical and organisational measures by the data controller to ensure that the risk to the rights and freedoms of the concerned data subject becomes containable.[23] Due to this requirement, the SDM also foresees a risk analysis.[24] The risk

[21] Ibidem '*The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals*', see chapter 6.4, page 27 for a detailed overview how the protection goals are anchored within the GDPR.

[22] Ibidem Schlehahn, E., '*Die Methodik des Standard-Datenschutzmodells im Bereich der öffentlichen Sicherheit und Justiz*'.

[23] See for example Articles 24 (1), 32 (1) GDPR, Articles 19 (1), 29 (1) Directive (EU) 2016/680.

analysis requires the controller to assess the whole personal data processing lifecycle, including all data, formats, IT systems, processes and functions. The German DPIA methodology provides for a structured approach with different phases of a data protection management. Notable publications explaining the SDM approach in more detail available at the moment are the project Forum Privatheit's DPIA White Paper[25], which is complemented by an essay of Bieker et al.[26] Both publications propose procedures and stages of the DPIA process using the German Standard Data Protection Model in detail.[27] This data protection management cycle has four concerted phases or stages, namely:

(1)	Preparation phase	(Plan)
(2)	Execution phase	(Do)
(3)	Implementation phase	(Act)
(4)	Review phase	(Check)

[24] '*The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals*', page 38 f.

[25] Friedewald, M.; Bieker, F.; Obersteller, H.; Nebel, M.; Martin, N.; Rost, M.; Hansen, M., for the project Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt: '*White Paper - Datenschutz-Folgenabschätzung, ein Werkzeug für einen besseren Datenschutz*', 3rd Edition, November 2017.

[26] Bieker, F.; Hansen, M.; Friedewald, M.: '*Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung*', essay published in RDV 2016/09 (Recht der Datenverarbeitung) issue 4, pages 188-197.

[27] The DPIA procedure model of the White Paper was developed as a synthesis of several PIA-models, while in the essay the model was specifically aligned to the GDPR. See in comparison the DPIA models of the CNIL (Commission Nationale de l'Informatique et des Libertés) (2015). Privacy Impact Assessment: Methodology (how to carry out a PIA). Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf (10.03.2016) and from the English-speaking region: Warren, A.; Charlesworth, A. (2012): Privacy Impact Assessment in the UK. In: Wright, D.; De Hert, P. (ed.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), pages 205-224.

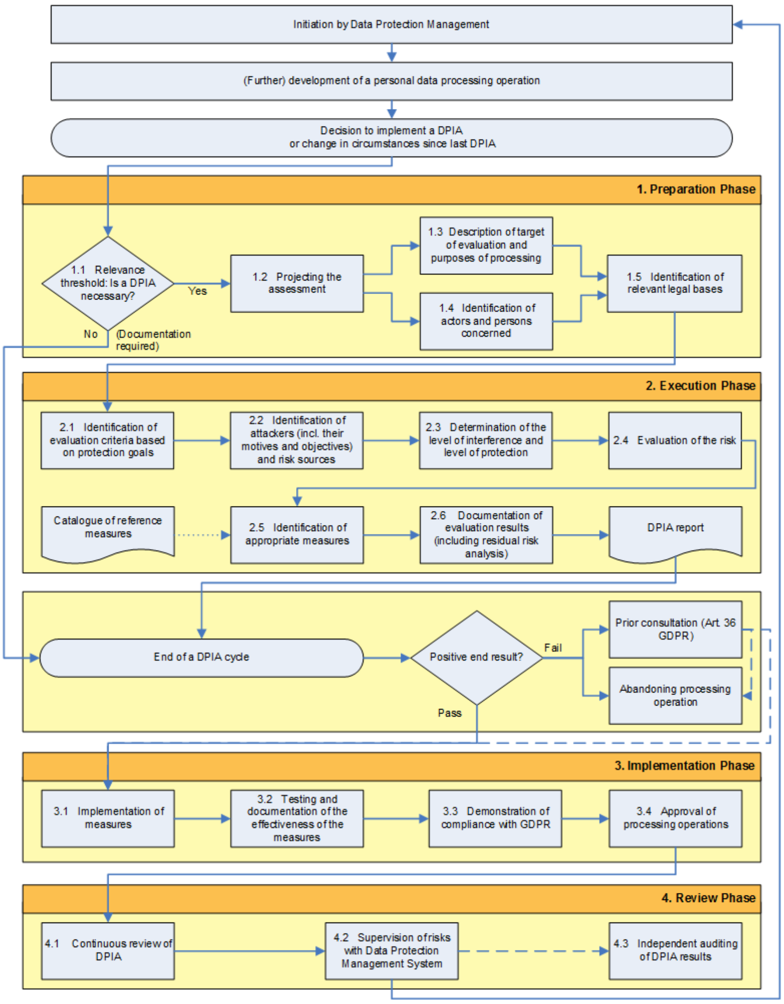

Initiation by Data Protection Management
(Further) development of a personal data processing operation
Decision to implement a DPIA
or change in circumstances since last DPIA
1. Preparation Phase
1.1 Relevance threshold: Is a DPIA necessary?
Yes
No
(Documentation required)
1.2 Projecting the assessment
1.3 Description of target of evaluation and purposes of processing
1.4 Identification of actors and persons concerned
1.5 Identification of relevant legal bases
2. Execution Phase
2.1 Identification of evaluation criteria based on protection goals
2.2 Identification of attackers (incl. their motives and objectives) and risk sources
2.3 Determination of the level of interference and level of protection
2.4 Evaluation of the risk
Catalogue of reference measures
2.5 Identification of appropriate measures
2.6 Documentation of evaluation results (including residual risk analysis)
DPIA report
End of a DPIA cycle
Positive end result?
Fail
Pass
Prior consultation (Art. 36 GDPR)
Abandoning processing operation
3. Implementation Phase
3.1 Implementation of measures
3.2 Testing and documentation of the effectiveness of the measures
3.3 Demonstration of compliance with GDPR
3.4 Approval of processing operations
4. Review Phase
4.1 Continuous review of DPIA
4.2 Supervision of risks with Data Protection Management System
4.3 Independent auditing of DPIA results

Figure 3: Workflow of the German DPIA methodology

In the preparation phase (1), the threshold for the obligation to conduct a DPIA is assessed first; this may happen due to a direct specification of the EU data protection supervisory authorities, and by an initial assessment of fundamental rights interference and risks for the data subject. Furthermore, a description of the target of evaluation, namely the intended data processing must occur. This also includes a description of the related processing purposes, the involved actors and data subjects concerned, as well as the identified legal ground(s) and the operational/organizational context.

In the following execution (evaluation) phase (2), the evaluation criteria are determined first. In the context of the above mentioned methodology, these would be the data protection goals. Furthermore, potential attackers and risk sources are identified. In a next step within the evaluation, the level of interference on the fundamental rights and freedoms of the data subject and the correlating needed level of protection have to be determined. Subsequently, an assessment of the risks and the identification of suitable (technical and organisational) mitigation measures must be conducted, followed by a documentation of evaluation results including an analysis of residual risks.

In the implementation (realization) phase (3), it must be determined if the implementation of technical and organisational measures lead to a positive result, either by eliminating or at least mitigating the identified risks in such a way that the residual risk is controllable. In case of a negative result, the realization stage faces the controller with the decision to either discard the intended personal data processing because of the too high risk to the rights and freedoms of data subjects, or to consult the competent data protection supervisory authority according to Article 28 (1) of Directive (EU) 2016/680. Either way, the realization stage requires a coherent test, release and documentation activity in the context of measures implementation.

The review phase (4) foresees a continued cycle addressing the personal data processing again once its legal and/or factual circumstances change in any way (e.g. other/more controllers, processors, recipients, data subjects, change of technical tools or the like). In other words, the DPIA cannot be a conclusive assessment. Rather it is a tool for assisting legally compliant processing and decision-making which should be applied as a continual process with updates where needed.

The above explained proposal for a data protection management cycle is not static. Rather, it is to be expected that it will be adapted and further improved continually in expectation of the new European data protection framework being applicable by May 2018. Moreover, the German DPA working subgroup for the SDM ('UAGSDM') is continually working on updated versions of the SDM handbook, while a complementary measures handbook is currently in the works as well.

[redacted] United Kingdom

In the United Kingdom, the Data Protection Impact Assessment Guidelines are drafted and published by the Information Commissioner's Office (ICO) taking on the role of the country's DPA. These guidelines consist of several consecutive documents. The so-called Privacy Impact Assessment Handbook sets out the base procedure of conducting an impact assessment. In addition, a Code of Practice on Conducting Privacy Impact Assessments provides further details to streamline the process and update the initial Handbook. However, in light of the adoption of the GDPR and the ICO's intentions of fully complying with the new European standards, this section of our analysis of national DPIA guidance practices shall focus on the recently presented guidelines that is currently undergoing review. In a document referred to as "Consultation: GDPR DPIA Guidance", the ICO launched a public consultation in March 2018 to receive feedback and finalize its new guidelines. As the updated guide shall soon replace the previous code of practice, the overview provided in this section shall be limited to the most recent version of the upcoming guidelines.

In these guidelines, the DPIA procedure is envisioned as a 9-step process.

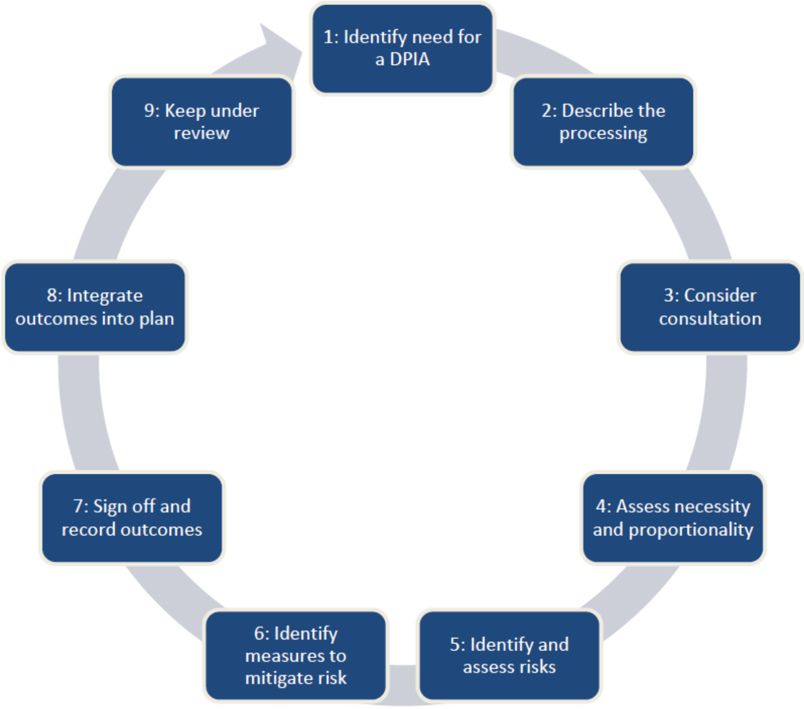

1: Identify need for a DPIA
2: Describe the processing
3: Consider consultation
4: Assess necessity and proportionality
5: Identify and assess risks
6: Identify measures to mitigate risk
7: Sign off and record outcomes
8: Integrate outcomes into plan
9: Keep under review

Figure 4: 9-step process of the UK DPIA methodology

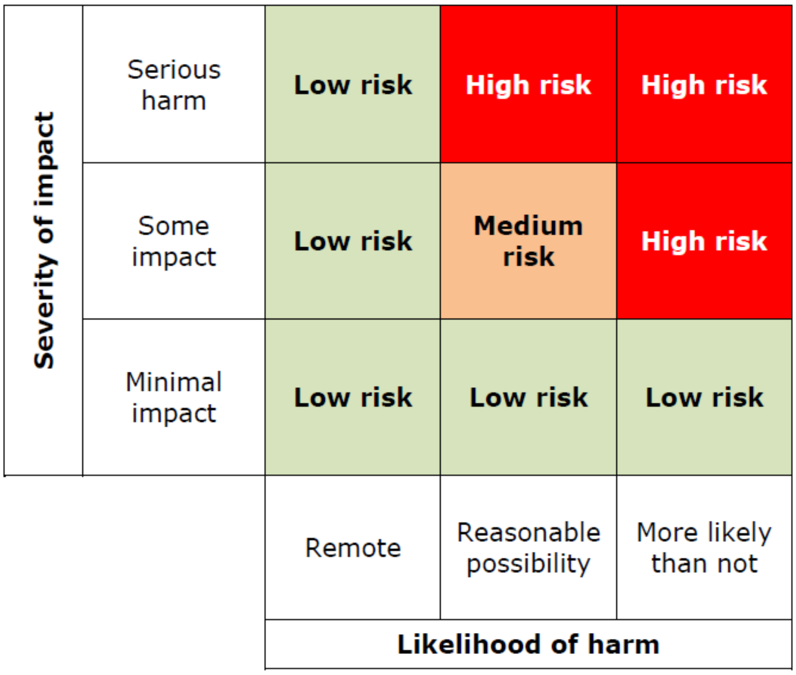
1. First, the data controller needs to determine whether there is a need for a DPIA to be conducted. The guidelines reiterate the general requirements from the GDPR. Generally speaking, a DPIA is required when the type of processing is likely to result in a high risk to the rights and freedoms of individuals. This is the case when either the likelihood of the harm occurring is higher, when the potential impact is more severe, or a combination of both. As such, the data controller must screen for red flags indicating that such a higher risk is present. In addition to the existing lists of processing activities that are inherently high risk, one of which is provided by the ICO and includes the likes of genetic data and risk of physical harm, the ICO follows the 9 criteria of likely high risk processing activities as presented by WP29 and further details key terms such as 'systematic and extensive', 'significantly affect' and 'large scale'.

2. Once the need to conduct a DPIA has been affirmed, the data controller must describe the processing activities in detail. This shall include their nature (being what the data is intended to be used for), their scope (being all that is covered by the processing), their context (being the wider picture, including the relevant internal and external factors which might affect expectations or impact) and their purpose (being the reason for which the data is processed).

3. Additionally, the data controller should consider consulting the data subjects and involved individuals for the DPIA. The ICO recommends that this is done at all times with the exception of instances in which valid reasons such as the need for confidentiality apply. In these instances, the data controller should include this in the DPIA and justify why the individuals or their representatives were not consulted.

4. Under the fourth step, the data controller should assess the necessity and proportionality of processing activities. This is done by assessing whether the planned processing of personal data helps to achieve the purpose and whether any other reasonable way exists to achieve the same results. As evaluating general data protection compliance is a good measure of necessity and proportionality, it is recommended that this requirement is met through the satisfaction of the general data protection principles such as data minimization, purpose limitation, data quality, access rights and legal basis.

5. Following this, the risks of the data processing should be identified and assessed. This is done by evaluating the potential harm that might befall individuals and the likelihood of this happening. The harms might include discrimination, limited exercise of rights, financial damages and loss of control over the use of data. Security risks such as unauthorized access and the potential impact of data breaches should therefore be considered as well. As previously stated, both the severity and likelihood of the risks materializing should be taken into account to determine how high the risk is. Both a smaller chance of large negative impact and a higher chance of a comparatively small fallout can amount to high risk requiring considerable counter-measures. The ICO states this analysis should be done as objectively as possible and suggests a structured approach such as the table provided below.



Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Figure 5: UK approach for likelihood of risk and impact severity assessment

6. The source of each identified risk should then be determined in order to implement measures to mitigate the risk. It should be clarified whether the measure taken is set to minimize or eliminate the risk. These measures might include additional training, anonymization, reductions to the scope of the processing, adding a human element to automated decisions, using different technologies or empowering the data subjects with further mechanisms to exercise their rights. Additionally, an analysis of the costs and benefits can be included to determine whether the measure is appropriate.

7. Once the risks have been assessed and appropriate risk mitigation techniques have been identified, the DPIA should record the outcomes of the analysis. This shall include the planned measures, the status of each risk (eliminated, reduced, or accepted), the level of residual risk and whether or not the DPA should be consulted. The latter is the case if a high risk still remains after the conception of counter-measures. The outcomes should be signed off and the advice of the DPO should be requested.

8. Once the outcomes have been recorded and validated, the mitigation techniques should be integrated in the practical data processing activities and project plans. Action points should be drafted and responsibilities assigned. It’s also suggested that the DPIA, or where necessary a redacted version thereof, should be published to aid transparency and accountability.

9. The DPIA should be kept under review. The assessment is an ongoing process that should be updated and revised in light of changes to the processing activities, risks and relevant circumstances. In these instances, the data protection impact assessment cycle should start at step 1.

In addition, the ICO Guidelines also contain further details on when the DPA should be contacted as well as a further overview of the purposes and circumstances of a DPIA. The document concludes with DPIA checklists for awareness, screening and legal compliance.

[redacted] Belgium

In Belgium, the national DPA known as the Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL) recently published the latest version of its DPIA guidelines[28]. After presenting a draft version during a public consultation period, the final guidelines were made available in February 2018. In the guidelines, the CBPL stresses that a DPIA is a process that consists of a description of the data processing, an assessment of the necessity and proportionality thereof, and a management of the risks for the rights and freedoms that emerge from the processing of personal data.

Similarly to the French approach, the Belgian DPA makes clear that its suggestions take close account of the advice made available by the WP29. In addition, it emphasizes that its guidelines are no complete one-size-fits-all manual for the execution of a DPIA and that those conducting such an assessment should develop codes of conduct and specific approaches adapted to their particular situation and sector. As the DPIA is to be considered a tool to assist in the demonstration of accountability with the legislative framework, the document states that the risk-based approach is invaluable to the lawful processing of personal data and can support the realization of adequate data protection by design.

The Belgian DPIA guidelines consist of several sections detailing a variety of aspects of the execution of a DPIA. Following a general introduction, the guidelines first cover when and at what moment in time a DPIA is required. Then, they cover the essential elements of the impact assessment and under what circumstances a preliminary consultation with the DPA is mandated. Finally, the different actors involved and their roles are explained in detail, and some additional information on codes of conduct, particular processing activities and oversight is provided. The following flow-chart of the considerations to be taken when conducting a DPIA is provided as a general guideline throughout the document.

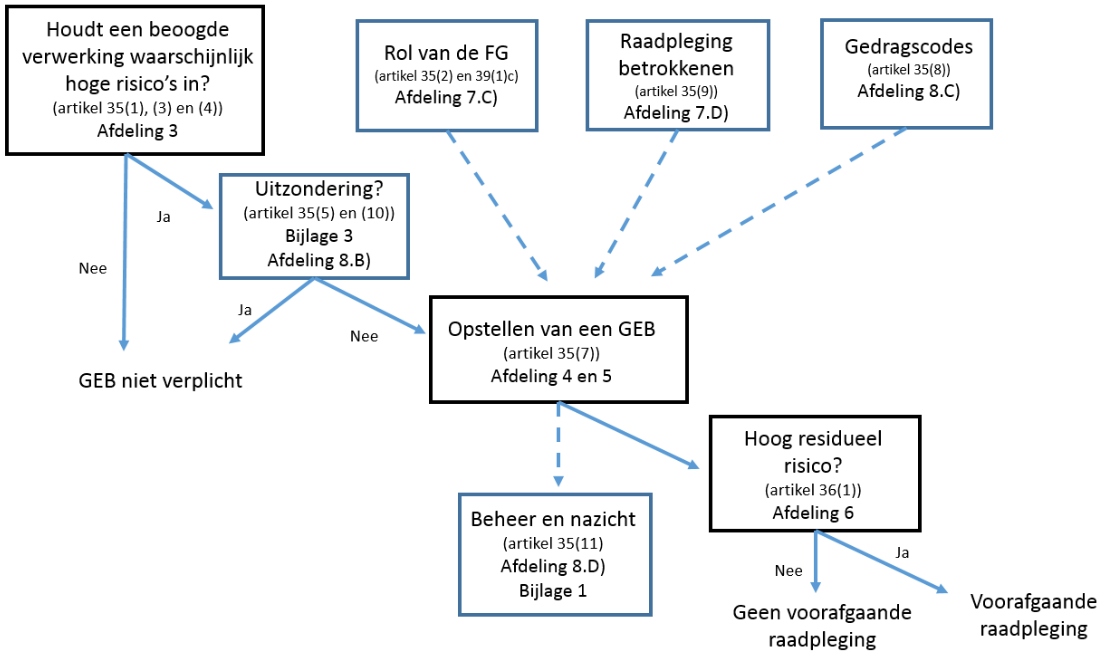

Houdt een beoogde verwerking waarschijnlijk hoge risico's in? (artikel 35(1), (3) en (4)) Afdeling 3
Rol van de FG (artikel 35(2) en 39(1)c) Afdeling 7.C)
Raadpleging betrokkenen (artikel 35(9)) Afdeling 7.D)
Gedragscodes (artikel 35(8)) Afdeling 8.C)
Ja
Nee
Uitzondering? (artikel 35(5) en (10)) Bijlage 3 Afdeling 8.B)
Ja
Nee
GEB niet verplicht
Opstellen van een GEB (artikel 35(7)) Afdeling 4 en 5
Hoog residueel risico? (artikel 36(1)) Afdeling 6
Beheer en nazicht (artikel 35(11) Afdeling 8.D) Bijlage 1
Nee
Ja
Geen voorafgaande raadpleging
Voorafgaande raadpleging

Figure 6: Necessary considerations for a DPIA according to the Belgian DPA

[28] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, "Aanbeveling nr. 01/2018 van 28 februari 2018 met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging", CO-AR-2018-001.

1. Under the Belgian approach, significant attention is first paid to when and under what circumstances a DPIA is required in practice. The guidelines further elaborate upon the legal requirements in the GDPR and define a risk as the probability that a certain even or threat occurs with a certain impact and severity as a consequence. For a risk to be considered "high", the data processing activities are likely to result in significant negative effects for the fundamental rights and freedoms of the data subject. In this sense, the guidelines reiterate the 9 criteria for assessing the probability of a high risk as provided by the WP29. Additionally, the document cover the situations in which a DPIA is always mandatory by reiterating the advice given by the WP29 and by providing a number of examples. Finally, it's made clear that the DPIA must be conducted before the processing of the personal data commences and preferably as soon as possible to leave the opportunity for later improvements and revisions where necessary due to the DPIA being a continuous process rather than a one-time event.

2. After framing the timeframe and circumstances under which a DPIA must be executed, the guidelines detail the essential elements of the impact assessment.

- Description of the intended processing activities and the purposes of the processing. This is to be understood as a systematic, detailed and precise overview of the processing activities, the personal data, the involved actors, the timeframe of the processing and the surrounding circumstances and resources surrounding the personal data.
- Assessment of the proportionality and necessity of the processing in relation to the purposes. This requires an explanation as to why the chosen processing techniques are adequate and not excessive for the purposes of the project. A balance must be struck between the interests of the actors involved and, while performing the assessment, account must be taken of the nature of the purpose, the legal basis, the interests at stake and the justification as to why the processing is proportional, adequate, non-excessive and not ongoing for longer than necessary. In this sense, the guidelines stress that all applied measures to comply with the GDPR should be considered and listed, including the dealings with data processors, safeguards for international transfers and the guarantee of data subject rights to information, access, portability, erasure, rectification and objection.
- Risk assessment. In order to conduct an effective risk assessment, three steps must be undertaken. First, the risks must be identified. Next, they must be analysed. Finally, they must be evaluated. A distinction is therefore made between the analysis of the risk, which is to be understood as the determination of the threat level and the nature of the risk, and the evaluation of the risk, being the comparison of the risk analysis with the predetermined criteria to assess whether the risk is acceptable. The distinction between inherent risks and residual risks is as such maintained in the Belgian guidelines. Regarding the envisioned risks, the guidelines stress that they do not merely refer to those that might negatively affect the rights of privacy and data protection but instead extend to any fundamental right as well other interests such as those of a financial nature. In assessing each risk, the responsible actors must assess the likelihood of the risk materializing and the potentially negative effects thereof, as well as determining the sources of the risks, the possible consequences and the threats that can directly impact the personal data. The suggested scope here is broad as the Belgian DPA suggests considering all non-negligible risks. No preferred method of assessing the risks is provided but the guidelines stress that it must be an objective, consistent and identified process of evaluation in line with the conditions present in the GDPR. Reference is made to ISO guidelines and other risk assessment measures but it is maintained that contextual elements of the specific situation must be taken into account.
- Description of intended measures and risk mitigation techniques. These measures can be of a technical, organizational and legal kind. The guidelines stress that the big picture must be considered in the determination of these measures, meaning that the type of processing, the technical state of the art, the risks and the costs should all be taken into account to manage the risks to an acceptable level and strike an adequate balance.

3. Following its overview of the necessary elements of the DPIA, the Belgian DPA provides an overview of all relevant actors and their roles in the process. In summary, the guidelines reaffirm that the data controller carries the responsibility for the legal compliance of the data processing. Still, those exerting specific functions within the agency or company should be involved to provide support regarding certain aspects of the DPIA. This includes legal personnel, IT staff, security experts and so forth. The data protection officer (DPO) is also required by law to assist in the process, and it's recommended that the final decisions made as a result of the DPIA involve higher executive staff validating and approving the findings of the assessment. Other actors that can to a certain extent provide assistance are the data processor, the DPO, the DPA and the data subjects or those who represent them. It's also encouraged that the DPIA's or a cleaned up version thereof are made available to the general public.

4. The final main section of the guidelines addresses a number of diverse aspects of the DPIA process. The Belgian DPA iterates that a single DPIA can be conducted for several similar or joint processing activities. In other words, there is no necessity to needlessly repeat the DPIA procedure for processing activities that are highly similar or conducted in a joint enterprise. It also stresses the importance of codes of conduct drafted by those processing the data and, as DPIA's are an ongoing process of which the outcome might change over time following differences in the processing activities and potential risks, recommends the adoption of periodic reviews every 3 years and the formal validation by the higher management. Regarding existing processing activities that were ongoing before the entry into force of the GDPR, the guidelines reiterate that a DPIA is only required when the risks change after that date. Still, it recommends controllers to conduct at DPIA if these processing activities pose a high risk to the rights and freedoms of the natural persons involved.

5. In addition, the guidelines contain two annexes. The second is of little relevance to this overview as it contains a list of instances under which private actors are required by law to conduct a DPIA. The first, however, provides 7 so-called minimum requirements or criteria to evaluate the quality of a DPIA with.

[redacted] France

In France, the primary DPIA guidelines are provided by the French DPA known as the Commission Nationale Informatique & Libertés (CNIL). These guidelines, the latest versions of which were published in February 2018, are referred to as a "Privacy Impact Assessment" and consist of three parts. Part one sets out the general methodology to be used when applying fundamental data protection principles to assess the impacts and risks of data processing techniques. In other words, this section sets out the general French approach and its context to conducting privacy and data protection impact assessments. Part two provides pre-made templates that can be used by end-users and data controllers when performing a DPIA. In doing so, it contains facts and resources that can be used to formalize and streamline the DPIA process. Part three lists an overview of the so-called knowledge bases, being an index of controls for the purpose of complying with legal requirements and mitigating risks. In addition, a fourth and final PIA document exists to cover the specificities and unique aspects of connected objects and the assessment of the impact on privacy in an IoT context.

In its methodology, the CNIL makes clear that its approach is in line with the criteria presented by the Working Party 29 (WP29) and applies the EBIOS method[29] in the context of data protection as to maintain compatibility with international standards on risk management such as ISO 31000. The appendices of the document provide an overview of the WP 29 guidelines and the manner in which they correspond with the CNIL's approach.

In summary, the French approach to performing a DPIA is based on two core pillars. In order to achieve full legal compliance, one must respect both the fundamental rights and general principles of privacy and data

[29] http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

protection law, as well as manage the data subjects' privacy risks by assessing threats and determining the appropriate technical and organizational controls necessary to protect personal data.

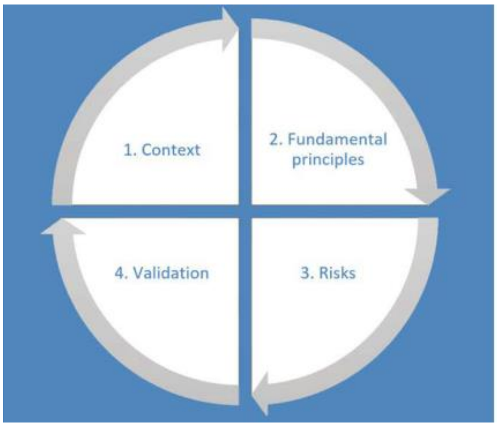


Figure 7: General approach for carrying out a PIA according to the French DPA

1. Under the French approach, the first step of performing a DPIA and achieving legal compliance of data processing activities is the defining and describing of the context in which the data is being processed. This includes the presentation of an overview of the nature, scope, context, purposes and stakes of and relevant to the processing operations. The data controller and processors should be identified and the personal data as well as its recipients and storage duration should be clarified. In summary, the complete cycle of the personal data from collection to erasure and the ways in which it shall be processed should be provided in detail.

2. The second step involves the analysis of the relevant fundamental principles and rights described in the GDPR. First, as principles, one can consider the general requirements of proportionality and necessity. This includes the legal concepts of purpose limitation, lawfulness of processing and storage period requirements, as well as data minimization, adequacy, quality and accuracy that were originally formulated in Directive 95/46/EC and have since been included in articles 5 and 6 of the GDPR. Second, regarding the fundamental data subject rights, the methodology refers to the rights to information, consent, access, data portability, rectification, erasure and objection. In light of both of the abovementioned instances, full legal compliance requires the data controller to explain and justify the choices made to comply with the requirements and details the controls used to implement them further.

Compliance with the fundamental rights and principles
Management of the data security risks
Compliance

Figure 8: Compliance approach using a PIA according to the French DPA

3. The third step requires the assessment of the risks to privacy that are associated with data security. In doing so, the CNIL considers a privacy risk to be a "hypothetical scenario that describes how certain risk sources could

exploit the vulnerabilities of supporting assets in a context of threats and allow feared events to occur on personal data thus generating impacts on the privacy of data subjects." In order to properly assess the risk level, one must take into account both the severity, being the magnitude and potential negative effects, and the likelihood of the risk actually materializing and occurring in practice. The former depends on the nature of the impacts while the latter results from the level of vulnerabilities and the opportunities for risk sources to exploit them.

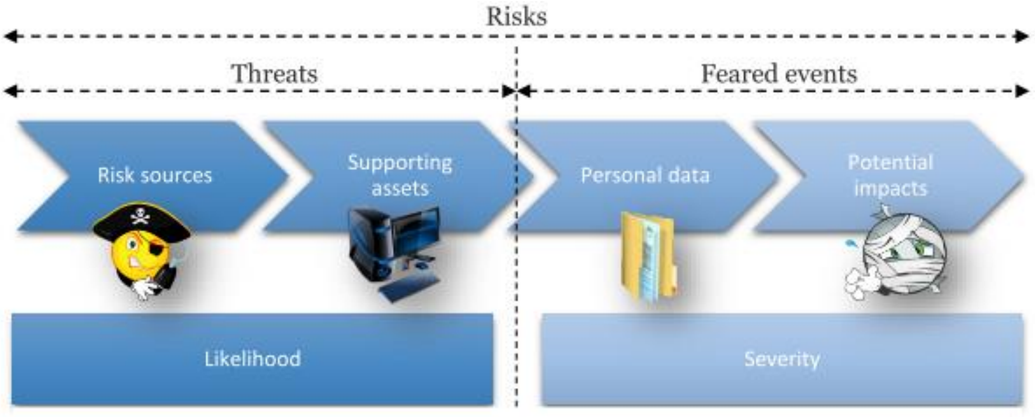


Figure 9: Risk components according to the French DPA

To properly conduct the analysis of the risks, the data controller must first assess the existing or planned controls. The CNIL considers these to fall into three different categories, being controls that bear specifically on data being processed (like encryption and anonymization), general security controls regarding the system (such as backups and hardware security), and organizational controls or governance (such as policy and incident management). In addition to assessing the security measures and their uses in the specific context of the processing activities, the causes and consequences of the different risks must be considered. For each feared event and possible negative effect to occur, the project owner should determine the potential impacts on the privacy of the data subjects, the threats and risk that could cause these negative effects, the severity of the these consequences were they to materialize, and the likelihood of this actually occurring in practice. Following this, one must determine whether these risks are acceptable in light of the existing or planned controls. If not, additional controls and assessments should be suggested and conducted in order to minimize and determine the residual risks.

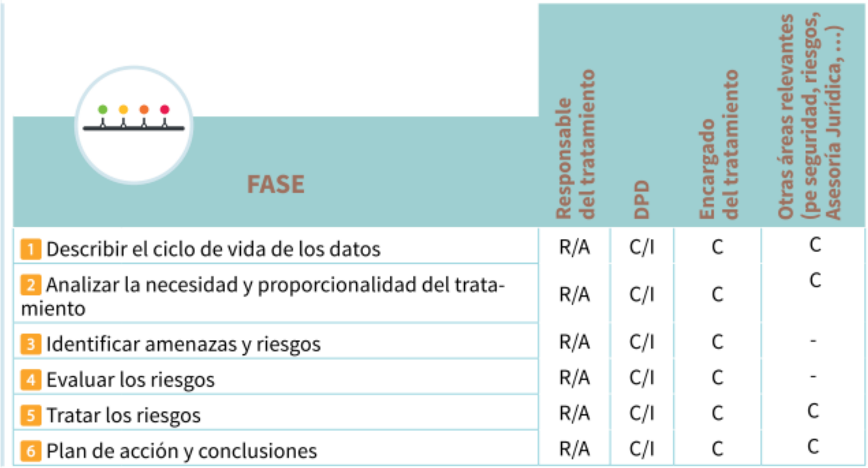
4. In the fourth and final step, the methodology poses that the documents and outcomes of the DPIA are formally validated in view of the facts so that, if necessary, the previous steps can be revised and alterations to the risk assessment and security measures can be made. This consists of the consolidation of the study's findings by presenting the controls selected to ensure legal compliance and contribute data security, mapping the risks and drawing an action plan based on the additional possible measures previously identified. In addition, the considerations of stakeholders such as the data subjects and the data protection officer. Following this, the selected controls, residual risks and action should be considered and the decision should be made whether the impact assessment should be validated, refused or held conditional on improvement.

Finally, the CNIL provides two further main suggestions. One, that a DPIA should be conducted and a risk-mitigating approach should be implemented as soon as a new processing of personal data is designed. As such, it is stressed that the analysis and assessment should be made at the outset of the processing rather than after the system has been created and put into use. Two, that a DPIA should be considered a continuous process of improving the management of privacy risks and the implementation of measures to further protect personal data. This requires changes to the processing activities, the context and the risks to be monitored over time and, when necessary and in light of significant changes, that updates are made to the policy and security techniques. As such, the visual representation of the DPIA process is circular rather than linear. Finalizing and delivering a DPIA is not an end point marking a full and final validation of the processing activities. Instead, it's a process that must be repeated and re-assessed over time as circumstances, technologies and priorities change.

[redacted] Spain

Already in 2014, the Spanish data protection authority Agencia española de protección de datos (hereinafter: AGPD) published a guideline for data protection impact assessment based on the Data Protection Directive 95/46 EC (hereinafter: 2014 '*Guía para una Evaluación de Impacto en la Protección de Datos Personales*', or just 2014 document or guidelines). The Spanish model builds upon an assessment of data protection risks at an utmost early stage prior to the actual processing. In March 2018, the AGPD has published an updated version of their methodology aligned to the GDPR, whereas many cross-references are still made to the 2014 publication.[30] Similarly to the German model, the Spanish DPIA has different stages or phases to address the intended processing operation. Basically, it consists of six different phases[31], namely:

(1) Description of the data processing lifecycle, from the moment of collection to deletion
(2) Analysis of necessity of a DPIA
(3) Identification of the threats and risks
(4) Evaluation of identified risks
(5) Management of identified risks
(6) Action plan and conclusions



FASE	Responsable del tratamiento	DPD	Encargado del tratamiento	Otras áreas relevantes (pe seguridad, riesgos, Asesoría Jurídica, ...)
1 Describir el ciclo de vida de los datos	R/A	C/I	C	C
2 Analizar la necesidad y proporcionalidad del tratamiento	R/A	C/I	C	C
3 Identificar amenazas y riesgos	R/A	C/I	C	-
4 Evaluar los riesgos	R/A	C/I	C	-
5 Tratar los riesgos	R/A	C/I	C	C
6 Plan de acción y conclusiones	R/A	C/I	C	C

Figure 10: Phases of the Spanish DPIA

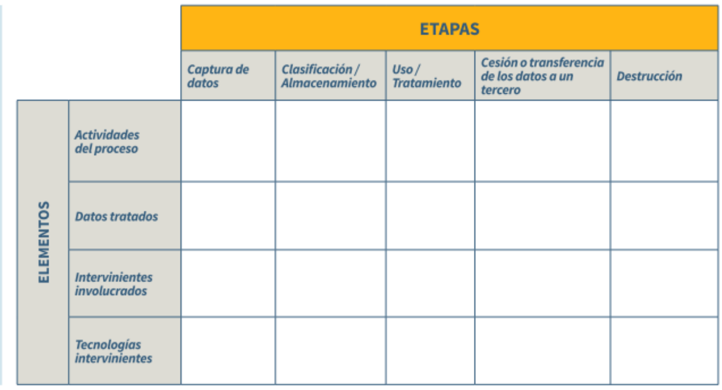
In the first phase (1), a description of intended data processing and the flow of data need to be described. In this context, the AGPD makes the recommendation to set up the DPIA as a project with an interdisciplinary team, whereas all entities dealing with the personal information should be involved. Already in its 2014 version of the DPIA methodology, the AGPD recommended to have a responsible project manager with decision powers and with the support of the higher management of the controller organisation. Furthermore, involved

[30] 2018 '*Guía práctica para las Evaluaciones de Impacto en la Protección de Datos Sujetas al RGPD*', available at: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf.

[31] Ibid., see p. 9 and 13.

should be the organisation’s data protection officer, the IT security officer, responsible personnel for from the ICT department, and representatives of those business areas or departments which are most affected by the intended processing operation.[32] Once the team is put together, it shall work towards a description of all data protection relevant aspects of the intended processing operation. Therein, the minimum elements of this description are the:

- foreseen means of processing and technologies usage (including hardware & software), especially if this leads to a greater risk to privacy,
- categories of personal data to be processed and their sources,
- uses (purposes) for the intended processing, and foreseen retention period,
- data recipients for each category of personal data and the correlating reasons and justifications,
- data flows including the collection, the circulation within the organisation, transfers outside the organisation and the receipt of personal data from other organisations, transfers to a third country.[33]



		ETAPAS				
		Captura de datos	*Clasificación / Almacenamiento*	*Uso / Tratamiento*	*Cesión o transferencia de los datos a un tercero*	*Destrucción*
ELEMENTOS	*Actividades del proceso*					
	Datos tratados					
	Intervinientes involucrados					
	Tecnologías intervinientes					

Figure 11: Data processing flow capture in the Spanish model

The controller can include additional information and diagrams to illustrate aspects of the intended processing for greater clarity, such as the organisation’s access control schema or an overview of the foreseen retention or destruction period of the personal information. The AGPD provides in its DPIA guidance a possible model for systematizing, summarizing and managing this information, which is also displayed below:

[32] Cf. 2014 ‘*Guía para una Evaluación de Impacto en la Protección de Datos Personales*’, chapter 4 ‘*Constitución del equipo de trabajo y definición de sus términos de referencia*’, page 17 f.

[33] 2018 ‘*Guía práctica para las Evaluaciones de Impacto en la Protección de Datos Sujetas al RGPD*’, chapter 3.2, ‘*Contexto del tratamiento*’, page 17.

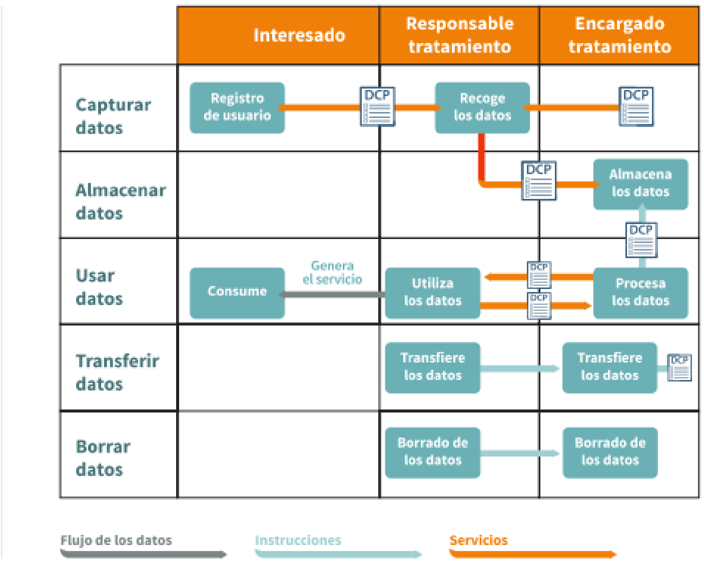


Figure 12: Example visualization of the processing flow in the Spanish DPIA

In the second phase (2), a threshold analysis is done whether a DPIA is required. Thereby, the AGPD provided already in 2014 an indicative list of situations in which it recommends a DPIA, for example the enrichment of existing data with new data categories, the processing for further purposes, or the processing of personal data about minors. Other examples are processing carried out to predict a data subject's behaviour, Big Data approaches, or involving highly invasive technologies such as video-surveillance or drones. Beyond the list of examples provided by the AGPD, a DPIA is recommended for processing operations with specific security risks potentially compromising the confidentiality, integrity or availability of personal information, especially when the processing occurs through telecommunications networks. Moreover, a DPIA is advised in case of potential risks which, if not addressed, could lead to legal, economic or reputational consequences. The goal of the DPIA should be to identify all possible risks to privacy and to establish risk elimination or reduction measures.[34]

For the phase of the threats and risk identification (3), two different types of risks impact were differentiated in the 2014 document: first, the effect of the processing on the data subject with regard to a possible violation of their rights, the loss of necessary information, or damage caused by an illegal or fraudulent use of the data needs to be assessed. Second, the risks for the controller with regard to not being data protection compliant must be considered. The AGPD defines risk as the probability that a threat will materialize through the exploitation of information system vulnerabilities or as an incident that causes an impact with certain damage to information systems. The AGPD presents eleven categories of different risks. These are (with some excerpts of the examples mentioned there):

(1) General risks
- ➢ Example: General non-compliance with the data protection law

(2) Legitimisation of a processing and transmission of personal data
- ➢ Example: Violation of purpose limitation, lack of clear legal ground, or invalid consent

(3) International data flows
- ➢ Example: Non-compliant cross-border transfer into a third country, lack of safeguards

(4) Notification about a processing
- ➢ Example: Controller not knowing when notification obligations towards the DPA exist

(5) Transparency of processing
- ➢ Example: Necessary information not provided, obscure/imprecise language in consent forms

(6) Data quality

[34] Ibidem 2018 document, chapter 2.1 '*¿Qué es una Evaluación de Impacto en Protección de Datos?*', page 4.

- Example: Request of unnecessary data, lack of information integrity, especially in the context of behavioural monitoring, profiling and (automated) decisions based on transactional, navigation or geolocation data, which may lead to adverse consequences or discrimination

(7) Special categories of data

- Example: No valid consent or other legal ground, poor or reversible anonymization allowing re-identification of sensitive data in research processes

(8) Confidentiality of data

- Example: Unauthorised data access and breach of confidentiality

(9) Data processing on behalf

- Example: Contractual deficiencies lacking necessary clauses and adequate safeguards

(10) Rights of the data subject

- Example: No procedures or tools to exercise data subject rights

(11) Data security

- Example: No information security officer or security policy within the organisation[35]

The AGDP recommends for the analysis of these risks that all affected parties should be consulted in some way. Stakeholders are the data subjects themselves, all relevant entities within the organisation and eventually, third parties with whom information is shared. Regardless of which approach the controller chooses (e.g. public consultations, working groups), it should occur at an utmost early stage of the DPIA process.[36]

In phase (4) addressing the evaluation of identified risks, it is highlighted that the ultimate goal of the risk analysis should be the avoidance or elimination of the risks. For each of these risks, the evaluation needs to convey both an assessment of the level of interference on the data subject's fundamental rights and an assessment of risk occurrence probability. Therein, it is important that the risk assessment is conducted from the perspective of the data subject.[37] In Annex II of the 2014 AGDP guidance (page 66), exemplary models had been provided, using varying values to ascertain both. Prior to the 2018 guidelines, the AGDP refrained from definitely recommending a general specification of a risk assessment methodology. Rather, it mentioned a number of different approaches, such as the Commission Nationale de l' Informatique et des Libertés (CNIL) publication 'Methodology for Privacy Risk Management', as well as the Risk IT (ISACA), ISO 27005, ISO 31000 and ISO 31010. However, the updated 2018 guidelines differentiate between three main categories of risks to the personal data, which are:

• Illegitimate access to data	-> violation of confidentiality
• Unauthorized modification of data	-> violation of integrity
• Deletion of data	-> violation of availability

Moreover, a catalogue of necessary steps and initial questions is provided to help controllers cover the relevant areas of threats and risks for data subjects. Thereby, the updated Spanish guidelines provide a number of examples to help with the organization-internal classification of threats.[38] The risk probability is determined based on the likelihood of whether the threat materializes. For both risk likelihood/probability and impact determination, the Spanish model proposes an assessment approach using a classification matrix based on four different levels in accordance with ISO 29134. For the likelihood of the risk, classifications such as '*negligible*', '*limited*', '*significant*', and '*maximum*' are suggested. For the impact, the same levels are suggested to cross-

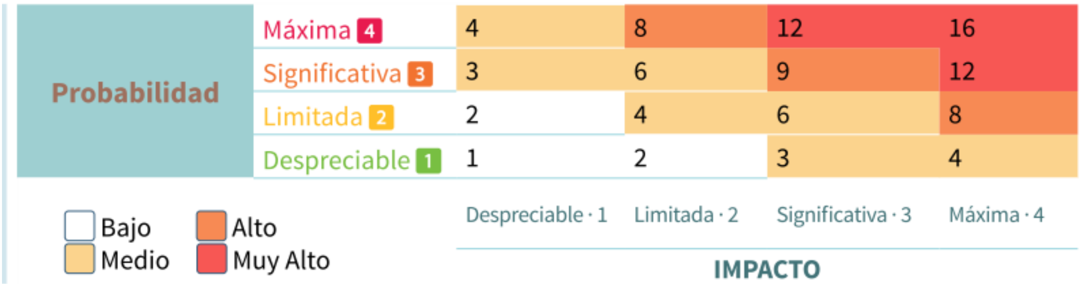
[35] 2014 '*Guía para una Evaluación de Impacto en la Protección de Datos Personales*', chapter 6 '*Identificación de los riesgos*', pages 21-26.

[36] Ibid, 2014 document, chapter 7 '*Consulta con las partes afectadas*', page 27 f.

[37] 2018 document, chapter 3.3 '*Gestión de riesgos: Identificar, evaluar y tratar*', p. 21 f., p. 26.

[38] Ibid., chapter 3.3 '*Gestión de riesgos: Identificar, evaluar y tratar*', p. 23 ff.

check with the probability. Moreover, the 2018 DPIA guidance differentiates between various areas of impact, such as physical, material, and moral impact, all of which need to be considered.[39]



		Despreciable · 1	Limitada · 2	Significativa · 3	Máxima · 4
Probabilidad	Máxima 4	4	8	12	16
	Significativa 3	3	6	9	12
	Limitada 2	2	4	6	8
	Despreciable 1	1	2	3	4

IMPACTO

□ Bajo
🟨 Medio
🟧 Alto
🟥 Muy Alto

Figure 13: Risk likelihood and impact matrix in the Spanish DPIA

Based on this matrix, a number score for the risk is determined to assess whether the risk is low (Bajo), medium (Medio), high (Alto), or even very high (Muy Alto).

For phase (5), the management of identified risks, four different responses are identified to address risks, namely reduction, retention, transfer, and cancellation of the risk. Thereby, the risk control measures need to mitigate or minimize the risk associated with a processing operation while the DPIA does not need to completely eliminate the risk of the processing. Rather, the risk must be reduced to an acceptable level so the rights and freedoms of the data subject can be guaranteed.[40] To achieve an avoidance, elimination, or at least reduction of the risks, exemplary countermeasures have been given in the 2014 guidance already. In any case, it is stressed that the residual risk must be determined and that all measures to mitigate those risks must be monitored on a regular basis to ensure that they are effective and comply with the purposes for which they have been implemented. In the event of changes in purpose, the measures must be adjusted accordingly.[41]

Phase (6) requires the provision of an action plan and conclusions. These should entail a description of all risk-mitigating measures and a conclusion on the outcome of the DPIA. The action plan should set a plan to implement the needed technical and organisational measures and should entail at least the following information:

- Measure identified
- Description of the measure
- Which entity is responsible for the implementation
- Time frame for implementation[42]

Thereby, the action plan should mention whether the DPIA has addressed an already existing or a new, intended processing of personal information, whereas in the latter case, an utmost early adoption of privacy by design approaches should be considered. The outcome conclusion of the PCIA should make recommendations based on the level of residual risk after the implementation of the measures, which may eventually include the suggestion that the competent supervisory authority should be consulted.[43] The realization of the final report's

[39] Ibid. p. 26 f.

[40] 2018 document, chapter 3.3 '*Gestión de riesgos: Identificar, evaluar y tratar*', page 31.

[41] 2014 document, chapter 8 '*Gestión de los riesgos identificados*', pages 29 ff., and 2018 document chapter 3.3 '*Gestión de riesgos: Identificar, evaluar y tratar*', page 31 ff.

[42] 2018 document, chapter 3.4 '*Conclusión*', page 33.

[43] 2018 document, chapter 3.5 '*Comunicación y consulta a la autoridad de control*', page 35 f.

recommendations and the implementation of measures should be monitored. It may depend on the organisation and the circumstances of the case how the implementation can be carried out. However, the DPIA needs to follow a supervision and revision cycle (like the PDCA life cycle of a management system). In case of any changes during the personal data processing operation, the DPIA phases must be repeated.[44]

IV. Conclusion

When comparing all these above described methodologies, there are of course noticeable similarities, but also differences. Most similarities can be perceived in the overall structure of a DPIA, usually beginning with a description of the evaluation target (processing, data, involved actors...) then proceeding with the determination of whether a DPIA needs to be conducted. In the case of the Spanish DPIA methodology, these first steps are in reversed order, though. However, all DPIA methodologies convey the risk assessment itself, a separate step for the determination of risk-mitigating measures, and conclude with the notice that a continuous review cycle must be foreseen by the controller. However, there are some fundamental differences in the DPIA methodologies of each country. Identifiable differences are:

- Different degree of '*anchoring*' within the GDPR, including different levels of abstraction:
    - For example, some DPIAs do not even fully cover the principles (see e. g. Art. 5 GDPR, reflected in Art. 4 Directive (EU) 2016/680), or do so by subsuming them fully under necessity and proportionality.
    - Some DPIA methodologies focus stronger on some selected aspects of the data protection law than other, such as data subject's rights, yet do so in a very detailed manner.
    - In contrast, the German method with the protection goals has a higher abstraction level, yet each goal can be re-traced back to provisions of the GDPR or Directive (EU) 2016/680.
- Differences in definitions:
    - For example, some DPIAs seem to not even define what a '*risk*' in the sense of the GDPR is
- Level of structured approach in determining mitigation measures:
    - This links back to the '*anchoring*' mentioned above.
    - Some DPIAs focus on mitigation approaches well known from IT security and in standards like ISO, yet often without giving reason why these can be suitable for the fundamental rights perspective a DPIA has to provide.

Moreover, all existing DPIA guidelines were made on the basis of the GDPR, whereas the law enforcement sector and the application area of Directive (EU) 2016/680 are mostly not mentioned at all. An exception is the German model, where at least a mapping of its protection goals approach to Directive (EU) 2016/680 already exists.

Being a fairly new requirement in the police and justice sectors, there are still many uncertainties regarding the most feasible approach to conduct a DPIA. Nonetheless, already the process of the DPIA can be an extremely helpful tool to identify risks for the rights and freedoms of data subjects foreseeably caused by an intended personal data processing operation. So it functions as an early warning mechanism for any data controller, so risks can be identified and addressed.

Therein, and regardless of the methodology chosen, it must be understood that any processing of personal data falling within the application scope of Directive (EU) 2016/680 and its national implementations is in fact an interference on fundamental rights, a 'risk that has occurred'. This interference remains, even if the processing operation is legally justified, and the information technology used for processing is verifiably secure. Moreover, the interference on the fundamental rights of the data subject causes risks for this individual, with

[44] Ibid., chapter 3.6 'Supervisión y revisión de la implantación', page 36.

direct consequences for this individual, and indirect consequences by inherent broader societal impact. Against this backdrop, the ultimate goal of any DPIA must be to reduce the level of interference must be reduced to the absolutely necessary level through the implementation of technical and organizational measures.

V. RESOURCES

This section shall contain an overview of resources that the end users can rely on for further information. It shall refer to existing guidelines and materials that they can use to complete their DPIA if necessary.

Article 29 Data Protection Working Party, Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 3211/15/EN WP233, Adopted on 1 December 2015, Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf.

Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN WP237, Adopted on 13 April 2016. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

Article 29 Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 17/EN WP248 rev.01, 4 April 2017 (revised on 4 October 2017). Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

Commissie voor de Bescherming van de Persoonlijke Levenssfeer, "Ontwerp van aanbeveling uit eigen beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging voorgelegd voor publieke bevraging, CO-AR-2016-004, 20 December 2016. Available at: https://www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_NL.pdf.

Commission Nationale de l'Informatique et des Libertés (CNIL), "Privacy Impact Assessment (PIA) Methodology (how to carry out a PIA)", June 2015. Available at: https://www.cnil.fr/fr/node/15798.

Agencia española de protección de datos (AGPD)

'*Guía para una Evaluación de Impacto en la Protección de Datos Personales*'

Published 2014

Available at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

Agencia española de protección de datos (AGPD)

‘*Guía práctica para las Evaluaciones de Impacto en la Protección de Datos Sujetas al RGPD*’

Published 2018

Available at: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn

‘*The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals*’

V.1.0 – Trial version 9-10 November 2016

Initial English version available at:

https://www.datenschutzzentrum.de/sdm/ (second and improved English version is currently in progress)

European Union Agency for Fundamental Rights (FRA), “Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU”, 2015.

Information Commissioner’s Office (ICO), “Privacy Impact Assessment Handbook”, Version 2.0. Available at: http://www.adls.ac.uk/wp-content/uploads/2011/08/PIA-handbook.pdf.

Information Commissioner’s Office (ICO), “Conducting Privacy Impact Assessments – Code of Practice”, Version 1.0, 2014. Available at: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

VI. REFERENCES

This section shall contain our footnotes. There will be overlap with the resources section.

Note:

URL addresses listed in the references section to point to the respective document sources originate from those which could be found on the Internet at the time of writing this White Paper, i. e. were valid links at the appointed date of April 10th 2018. No guarantee is given that those URLs still function at the time of any recipient reading this document.

Academic sources

Bieker, F.; Hansen, M.; Friedewald, M.

‘*Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung*’

RDV 2016/09 (Recht der Datenverarbeitung) issue 4, pages 188-197

Friedewald, M.; Bieker, F.; Obersteller, H.; Nebel, M.; Martin, N.; Rost, M., Hansen, M.

‘*White Paper - Datenschutz-Folgenabschätzung, ein Werkzeug für einen besseren Datenschutz*’,

Project Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt

3rd Edition, November 2017

Available at:

https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf

Schlehahn, E.

‘*Die Methodik des Standard-Datenschutzmodells im Bereich der öffentlichen Sicherheit und Justiz*’

DuD (Datenschutz und Datensicherheit) issue 01/2018, pages 32-36

Springer Gabler Publishing House

Tague, Nancy R.

‘*The Quality Toolbox*’

Second Edition, ASQ Quality Press, 2005

ISBN: 978-0-87389-639-9

Legislation

Charter of Fundamental Rights of the European Union

OJ C 364, 18.12.2000, p. 1–22

Available at:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000X1218(01)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

OJ L 119, 4.5.2016, p. 1–88

Available at:

http://eur-lex.europa.eu/eli/reg/2016/679/oj

European case law and policy documents

Article 29 Data Protection Working Party,

'*Working document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*'

16/EN WP237, Adopted on 13 April 2016

Available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

Court of Justice of the European Union (CJEU)

Judgement of the Court (Grand Chamber)

Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen

Joined cases C-92/09 and C-93/09 of 9 November 2010

ECLI:EU:C:2010:662

Available at:

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62009CJ0092

Court of Justice of the European Union (CJEU)

Judgement of the Court

Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v Österreichischer Rundfunk

Joined cases C-465/00, C-138/01 and C-139/01 of 20 May 2003

ECLI:EU:C:2003:294

Available at:

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62000CJ0465

Court of Justice of the European Union (CJEU)

Judgement of the Court (Grand Chamber)

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others

Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof,

Joined Cases C‑293/12 and C‑594/12 of 8 April 2014

ECLI:EU:C:2014:238

Available at:

http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TXT&ancre=

European Parliament Committee on Civil Liberties, Justice and Home Affairs

'*Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*'

(2016/2225(INI)), 20 February 2017

Available at:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0044+0+DOC+XML+V0//EN

Non-European and national legislation, case law and policy documents

Agencia española de protección de datos (AGPD)

'*Guía para una Evaluación de Impacto en la Protección de Datos Personales*'

Published 2014

Available at:
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

Agencia española de protección de datos (AGPD)

'Guía práctica para las Evaluaciones de Impacto en la Protección de Datos Sujetas al RGPD'

Published 2018

Available at: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn

'*The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals*'

V.1.0 – Trial version 9-10 November 2016

Initial English version available at:

https://www.datenschutzzentrum.de/sdm/ (second and improved English version is currently in progress)

VII. LIST OF FIGURES

VIII. LIST OF ACRONYMS AND ABBREVIATIONS

CoE	Council of Europe
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EEA	European Economic Area
EFTA	European Free Trade Association
EU	European Union
GDPR	General Data Protection Regulation
LEP	Legal, Ethical, Privacy (as part of WP3 in VALCRI)
LEA	Law Enforcement Agencies
OJ	Official Journal of the European Communities
OJ L […]	Official Journal of the European Communities – Legislation
OJ C […]	Official Journal of the European Communities – Information and notices
PETs	Privacy Enhancing Technologies
Rec	Recommendation
SDM	Standard Data Protection Model
SEPL	Security, Ethics, Privacy, Legal (as unofficial, work package overarching work subgroup in the VALCRI project)
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union