Template [2026] for Data Protection Impact Assessment ('DPIA')

Explainer

Version 1.0

Adopted on 10 March 2026

Version history

Version	Date	Adoption information
version 1.0	10 March 2026	adoption of the guidelines for public consultation

Table of Contents

The European Data Protection Board has adopted the following template - explainer:

The EDPB template can be used as a data entry for Data Protection Impact Assessment ('DPIA') documenting and reporting. Controllers can benefit from pre-defined fields that prompt complete and structured responses. Designed for ease of use, such template ensures that all necessary information is captured accurately, while minimizing errors and saving time.

This explainer document provides a concise explanation for completing this template effectively. This document is just an explanatory tool, intended to be useful for both controllers and Supervisory Authorities (SAs) and does not preclude the publication of other additional explanations, visual aids, or guides.

Controllers can conduct their risk analysis and management processes as they prefer, using the DPIA methodology of their choice (see Annex A). The EDPB template is one way to record the most important results, a minimum amount of information that should always be documented, in the format adopted by the EDPB and easily accepted by all SAs.

It is recommended to review the entire template before starting to understand its flow, gather all required data (such as dates, descriptions, and supporting evidence/documentation), use concise language, and expand only where elaboration is requested. Certain redundancy between the DPIA template sections ensures that each mandatory element is addressed explicitly and in a traceable manner, while enabling cross-referencing. Furthermore, the same fact serves different functions across sections. Please ensure that appropriate links are established between sections, where necessary, and provide consistent information across the different tables.

0 OVERVIEW OF THE PROCESSING

0.1 Controller(s)

0 Identify the GDPR controller. Provide all necessary contact details (management units responsible for the processing inside the organisation, main establishment and point of contact, representative, DPO, etc.). If applicable, identify Joint controllers. Clearly define each party's obligations and tasks[1].

0.2 Processor(s) and sub-processor(s)

1 Identify the processors/sub-processors involved in the processing with the unequivocal definition of their obligations and tasks[1].

0.3 Name of the processing

2 Provide the internal name given to the processing (the given name in the record of processing activities), and, if possible, identify the current version explaining the history of changes made to the processing in the past, if any.

0.4 Planning of the processing

3 Provide the estimated launch date by the controller.
4 Provide the estimated end date or expiration conditions (if applicable, i.e. because the processing is temporary, for example, associated with a project with a limited duration).

0.5 DPIA technical sheet

5 Identify the current version of the DPIA template and provide a version log (explaining the history of changes made to the information contained in the DPIA template for this processing, if any).
6 Identify the team involved in conducting this DPIA. You can provide details of their roles, tasks, responsibilities, etc. A RACI (Responsible, Accountable, Consulted, Informed) matrix can be used.
7 List the guidelines, standards, codes of conduct, and other reference materials used to conduct this DPIA[2].
8 Explain the reasons to conduct the DPIA[3]. It may be mandatory or there may be reasons that, in the opinion of the controller, make the DPIA necessary or beneficial. More than one checkbox may be selected.
9 Clarify the scope of this DPIA: identify what has been considered and what has been left out of the assessment and why, what are the boundaries of the assessment.

[1] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf
[2] Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711
[3] Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

10 Provide the completion date and the formal validation date: the DPIA must be formally approved by a responsible official (Managing Director, CEO, etc.) as complete and finished. The DPIA template might include a seal and signature. Information about the decision-making, validation, monitoring and review methods for the DPIA may be requested, and it should be documented somewhere although it is not included in this template.

11 Explain whether and to what extent the DPIA is intended to be published or to be shared externally. While it may be a good practice from a transparency point of view, sensitive information should not be published (concerning security, for example).

1 SYSTEMATIC DESCRIPTION OF THE PROCESSING

1.1 High-level description of the processing

1.1.1 Processed personal data

12 List the processed personal data (items or elements, data type, data subject category, etc.). Identify, if applicable, special categories of personal data.

1.1.2 Purposes of the processing

13 Identify the specific and explicit reasons for processing the personal data listed in 1.1.1. Consider the objectives that the processing aims to achieve, its high-level goals in the operational sense, and how the processing contributes to that result (e.g. supporting a business process, policy implementation, user experience (UX) and accessibility, or safety/security goals).

1.1.3 Secondary or compatible uses

14 Refer to an existing analysis (documented somewhere, not in this template) or examine any secondary or compatible uses of the data (compatibility assessment). State clearly whether data listed in 1.1.1 may be re-used for another purpose, and under what conditions, applying the purpose limitation principle.

1.1.4 Nature, scope and context of the processing

15 Describe the nature of the processing: the way personal data will be handled (operations involved, technologies used, etc.).

16 Describe the scope of the processing: breadth and extent considering the volume or scale given the number of data subjects or data items, geographical and organisational reach, frequency or duration for the data subject (processing recurrence from the data subject's perspective, i.e. per use / per session, periodically, continuous or near-continuous, event-driven or occasionally)

17 Describe the context of the processing: circumstances and environment (use cases, supported business processes, status of the controller and relationship with the data subjects, data subjects categories and potential vulnerable groups, cross-border processing, international transfers, etc.). Cross-border processing means either a processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union

where the controller or processor is established in more than one Member State; or a processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State. International transfers are transfers of personal data to a third country or an international organisation (an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries).

1.2 Functional description

18 Outline the processing in a structured way, decomposing it into phases or stages. Include information about the full chain composed of controller, processors and sub-processors.

19 Explain the data lifecycle and data flows: provide a comprehensive overview of how personal data is managed throughout its entire lifecycle, from collection to deletion. Key aspects to include:

Collection: Describe what data is collected and how, including the sources and the information provided to data subjects.

Use: Detail the operations performed on the data, the technologies used, and any automated decision-making or profiling involved. Clarify how data is used and whether it is combined with other datasets.

Storage: Specify where and how data is stored (physical, cloud, third-party), and who has access to the data.

Sharing and Transfer: Explain any data sharing to third parties or transfers outside the EU, and the legal mechanisms or tools used (e.g., SCCs, adequacy decisions).

Deletion and Destruction: Specify the criteria and procedures for securely deleting data when it is no longer needed, including methods for permanent erasure.

1.3 Means of processing, supporting assets and underlying architecture

20 From the functional description in section 1.2, explain the means of processing. Cover how the processing is performed, technical and organisational methods, tools, infrastructure and resources used to carry out the processing on personal data.
Specifically, provide a list or inventory of the essential supporting assets. An “asset” typically refers to any resource, tangible or intangible, that is used to process personal data, enabling an effective management throughout its lifecycle. Assets represent vectors for both value and risk in the context of data protection. Examples of assets are hardware, infrastructure, and network assets (i.e., servers, laptops, mobile devices, storage media, scanners, VPN gateways), software (database engines, business applications), APIs and models, personnel (users, administrators, developers, operators, support staff, decision-makers), sites and premises (data centres, archives), organisational assets (policies, procedures, contracts with processor and sub-processors), etc.
Include assets that are essential for risk analysis, i.e. whose compromise would plausibly impact rights and freedoms in a non-trivial way (for example, assets directly storing or processing personal data, assets that control access or protect data, exposed or high-impact components such as public-facing portals, APIs or, data-sharing interfaces to third parties). Very small, generic, or easily substitutable elements usually do not need individual listing.

Group the assets by logical module, by technical layer, by function, etc. Within each group, briefly state what it contains and how it relates to the processing, then use that level of granularity in the risk assessment and management later. Balance completeness and manageability, keep the very detailed inventory (per device, per service, etc.) in separate technical documentation and provide an explanation of the underlying architecture closely related to risk assessment and management.

1.4 Compliance with approved codes of conduct

21 Identify compliance with approved codes of conduct. Analyse the compliance obligation, if applicable; or the reasons that, in the opinion of the controller, make such compliance necessary or beneficial.

2 ANALYSIS OF THE PROCESSING

2.1 Lawfulness of the processing

2.1.1 Legal basis

22 Analyse the legal basis of the processing. The analysis of each legal basis should be carried out in relation to each of the purposes of the processing (1.1.2) including secondary or compatible purposes (1.1.3).

23 If applicable, refer to an existing analysis (documented elsewhere, not in this template) or analyse the legitimate interests pursued by the controller or by a third party and conduct a balancing test[4]. If this analysis relies on any hypothesis on the implemented measures, residual risks, etc. please ensure they are properly reported in the appropriate sections in this template.

2.1.2 Reasons to lift the processing prohibition

24 If special categories of data are processed (see 1.1.1Processed personal data), the reasons that led to the lifting of the prohibition on processing special categories of data must be properly identified and justified.

2.2 Data minimisation, retention periods, and data quality

2.2.1 Data minimisation and retention periods

25 Document in detail the justification to process personal data listed in 1.1.1, identifying recipients and providing retention periods. Justify the design choices too.

2.2.2 Data quality

26 Provide data quality metrics, requirements or thresholds.

[4] EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

2.3 Measures supporting compliance

2.3.1 Measures supporting compliance with principles in Article 5(1)(a-f) GDPR

27 List the measures contributing to the compliance with the principles established in Article 5(1)(a-f) GDPR (data minimisation, purpose limitation, accuracy, etc.) and discuss their appropriateness and effectiveness. Describe the implementation status of each safeguard at the time of the assessment: (a) Planned (the safeguard is only at the intention or design stage, it has been identified as necessary, but is not yet deployed in production); (b) Partially implemented (some elements of the measure are in place, but important aspects are missing or incomplete) or (c) Implemented (the measure exists, is deployed, and is effectively operating in the live environment, not just on paper, there is evidence that the control works as intended).

2.3.2 Measures supporting the exercise of data subjects' rights

28 List the measures envisaged to comply with the GDPR, taking into account the rights of the data subjects, inter alia, information provided to data subjects (Articles 12, 13 and 14 GDPR), right of access and to data portability (Articles 15 and 20 GDPR), right to rectification and to erasure (Articles 16, 17 and 19 GDPR), right to object and to restriction of processing (Article 18, 19, 21 and 22 GDPR) and discuss their appropriateness and effectiveness. Describe the implementation status of such measures.

2.3.3 Measures supporting compliance with other GDPR requirements

29 List the measures envisaged to comply with the GDPR, taking into account consent requirements (Article 7 GDPR), relationships with processors (Article 28 GDPR) and safeguards relating to international transfer(s) (Chapter V GDPR). Discuss their appropriateness and effectiveness and describe their implementation status.

2.3.4 Measures supporting data protection by design and by default

30 List the measures contributing to the compliance with data protection by design and by default[5] (Article 25 GDPR), discuss their appropriateness and effectiveness and describe their implementation status.

2.3.5 Measures supporting security of the processing

31 List the measures contributing to the security of the processing (Article 32 GDPR), discuss their appropriateness and effectiveness and describe their implementation status. Consider measures supporting the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, etc.

[5] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

3 CONSIDERATIONS ON NECESSITY AND PROPORTIONALITY

3.1 Impacts of the processing on the rights and freedoms of the data subjects

32 Explain how the threats that the planned processing (as it has been designed and is projected to be implemented, including technical, legal/contractual and organisational measures to mitigate risk) poses to the rights and freedoms of the data subjects can be materialised and identify their impacts and all possible risk sources. These are risks that exist even if everything works exactly as designed and all actors follow the rules.
These threats flow, mainly, from the processed personal data (1.1.1), the very purpose of the processing (1.1.2) and its nature, scope and context (1.1.4). Even if the processing is correctly implemented and works as specified, there are risks tied to its inherent and structural characteristics: everything goes as intended, but design choices themselves create risks for data subjects' rights and freedoms, even where there is no failure or attack.
A threat is any circumstance or event with the potential to adversely impact data subject's rights and freedoms (for example, linking, identifying, inaccuracy or data disclosure) and it may cause physical, material or non-material damage to data subjects.
A risk source is the origin or underlying cause from which a threat can materialise. Typical examples are the characteristics of the processing itself i.e., its purpose, wrong design and weaknesses (for example, use of unique identifiers, or long retention periods), exposures, etc.
Impact is the consequences that can be expected from the threat materialisation, always considering data subject's rights and freedoms (see recital 75 GDPR, for example).

3.2 Assess the necessity of the processing

33 Assess the necessity of the processing[6]. Evaluate if the envisaged processing is effective and the least intrusive for the data subject's rights and freedoms. Analyse if the processing demonstrably works as intended, at least to the appropriate or required level. Provide evidence (for example, concerning the different considered alternatives and their effectiveness in achieving the purpose) and justification.

3.3 Assess the proportionality of the processing

34 Assess the proportionality of the processing[7], remember that necessity is a pre-condition for proportionality. Discuss the importance of the processing and its potential benefits for

[6] EDPS "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", https://www.edps.europa.eu/sites/default/files/publication/17-04-11_necessity_toolkit_en_0.pdf ; See also Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR) https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112024-use-facial-recognition-streamline_en

[7] EDPS "Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection", https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf ; See also Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR) https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112024-use-facial-recognition-streamline_en 8

the data subject, your organization and collectively. The advantages resulting from the processing should not be outweighed by the disadvantages it causes with respect to the exercise of individuals fundamental rights and freedoms (consider the results obtained in 3.1 to reflect on the balance advantage/disadvantage, benefit/cost). You should answer this question with complete and updated information: is the processing envisaged to fulfil the purpose a proportionate response to the need you have, given the limitations to the data protection and privacy rights? Provide evidence and justification.

4 RISK ASSESSMENT AND MANAGEMENT

4.1 Risk assessment and management

4.1.1 Impacts on the rights and freedoms of the data subjects caused by non-default, accidental, unlawful, or abnormal events

35 Explain how non-default, accidental, unlawful, or abnormal events pose a threat to the data subject's rights and freedoms, and how these can be materialised. Identify their impacts and all possible risk sources. Consider threats posed by malfunctions and deviations from design and default, threats to data confidentiality, integrity and availability (related to cybersecurity), etc. Identify, at least, threats that could lead to illegitimate access, undesired modification and disappearance of data.
These threats are different from those identified in 3.1 because they materialise when something does not go as intended in the design, implementation, configuration or operation, or when there are malicious actors. The root cause is a deviation from the intended, compliant state.
For the definition of a threat, see above (para 32).
A risk source is the origin or underlying cause from which a threat can materialise. Typical examples in this context are software bugs, misconfigurations, wrong access rights, operational errors (sending data to the wrong recipient, wrong dataset used, forgotten de-provisioning), lack of maintenance (unpatched vulnerabilities, outdated components), insider abuse (staff exceeding their authorised use) or external attacks (phishing, ransomware).
For the notion of impact see above (para 32).

4.1.2 Method

36 Explain the details of the method followed to assess and manage risk. Provide the information necessary to understand and interpret the following aspects: likelihood and severity levels and their meanings (often a 2 to 5 levels scale is used), risk metrics, how risks are prioritised, risk acceptance levels, etc. If an established method is used, provide the link to the external source introducing this method[8].

4.1.3 Inherent risk assessment

37 Considering the identified threats, their risk sources and impacts, list the specific risks to the data subject's rights and freedoms posed by the processing. Include scenarios laid out in subsections 3.1 and 4.1.1. For a specific data processing, inherent risk is the risk

[8] For example, the documents listed in the Annex.

level the controller assigns to the planned processing assuming the baseline or initial set of planned measures.

A risk is a scenario describing an event (the threat materialisation) and its consequences. The risk level expresses the extent to which data subjects are affected by the corresponding threat and typically a function of: (i) the likelihood of the threat materialisation; and (ii) the magnitude of the adverse impacts that would arise if the threat materialises (severity). Estimate the likelihood and severity of all the identified risks to the rights and freedoms of data subjects.

Identify risk modulating factors, characteristics that increase or decrease the likelihood or severity of a risk (without being the primary source of the corresponding threat). Examples of aggravating (upward-modulating) factors are a very large number of data subjects or high data sensitivity, data subjects in a situation of dependency or vulnerability (children, patients, workers, migrants), or high exposure to external adversaries. Mitigating (downward-modulating) factors are design choices and measures (section 2.3).

Risk level calculation usually follows the standard Risk = likelihood × severity, typically using qualitative scales to derive a level (for example, low/medium/high). Follow the method explained or identified in 4.1.2. Modulating factors, not always present, may help in adjusting the baseline risk (likelihood × severity) up or down to reflect real-world nuances for this specific processing and its context.

38 Assess inherent risks considering their likelihood and severity[9] and other modulating factors.

39 Clearly identify risks; non-acceptable risks requiring additional mitigation before the envisaged personal data processing can take place.

40 If available, provide additional visual aids (such as diagrams, charts, maps, priority lists, etc.) to document the inherent risk assessment from different perspectives.

4.2 Action plan

4.2.1 Additional mitigating measures

41 Detail any additional (i.e. not initially planned) appropriate technical, legal/contractual and organisational measures to manage specific risks (from 4.1.3), describe their implementation status, and discuss their appropriateness and effectiveness. Include all types of measures (see section 2.3): measures supporting compliance with principles in Article 5 GDPR, measures supporting the exercise of data subjects' rights, measures supporting compliance with other GDPR requirements, measures supporting data protection by design and by default, and security measures.

4.2.2 Residual risk assessment

42 Residual risk is the risk that still remains after the controller has reflected on the unacceptable or excessively high risks, has decided to add additional mitigating measures, and has assessed how far those new measures actually reduce the inherent (initial or baseline) risk.

[9] A risk in data protection may be deemed non-acceptable if the potential severity of its impact is very high, even when its likelihood of occurring is low. This means that if the consequences for data subjects could be extremely serious, the risk may be considered unacceptable, regardless of how rarely the event is expected to occur.

43 Reassess risks considering all these new measures. If available, provide additional visual aids (such as diagrams, charts, maps, priority lists, etc.), documenting inherent risk assessment from different perspectives.

4.2.3 Plan

44 Provide information about the necessary activities to properly add these new measures to the processing so as to properly manage the risks for the rights and freedoms of individuals (responsible team, timelines, etc.), and to monitor, review and update the proposed measures once the processing is being carried out. Refer or link external documentation or annexes with the details.

5 INVOLVEMENT OF INTERESTED PARTIES

5.1 DPO advice

45 If there is a DPO (or a similar function), provide their opinion, conclusions and recommendations concerning the envisaged processing (for instance, document any input from the DPO on risks and how to mitigate them).
46 Outline the actions taken following the DPO's advice through the process of conducting the DPIA and planning the processing. Answer the question "How the controller has implemented DPO's advice?".

5.2 Views of data subjects or their representatives

47 Where appropriate, provide the data subjects' (or their representatives') opinion, conclusions and recommendations concerning the envisaged processing.
48 Explain their participation in the DPIA process, including explanations of why it has not been considered appropriate for them to participate or why it has not been possible for them to do so.

6 CONCLUSION AND DECISION

49 Conclude with the decision on the data processing viability: (a) abandon the data processing (risks are unacceptable, any of the required tests cannot be passed, advised by the DPO, data subjects or Supervisory Authority, etc.); (b) consult with the SA ; (c) proceed with data processing as planned, or (d) conditionally proceed with data processing (i.e., by modifying the data processing design to better address identified risks). In the latter, explain the specific conditions that must be met before proceeding with the processing (for example by linking them to previous sections in the template, i.e., sub-section4.2).
50 Optionally, explain/justify your decision.

For the European Data Protection Board

The Chair

Anu Talus

Annex 1 : SAS' GUIDELINES TO CONDUCT DPIAS

Please also take note that the EDPB data protection guide for small business may help when conducting DPIAs: https://www.edpb.europa.eu/sme-data-protection-guide/home_en

Supervisory Authority	Link
1. **Austria (AT)**	https://dsb.gv.at/faqs/verpflichtungen-fuer-unternehmen
2. Belgium (BE)	
3. Bulgaria (BG)	https://cpdp.bg/%d1%81%d0%bf%d0%b8%d1%81%d1%8a%d0%ba-%d0%bd%d0%b0-%d0%b2%d0%b8%d0%b4%d0%be%d0%b2%d0%b5%d1%82%d0%b5-%d0%be%d0%bf%d0%b5%d1%80%d0%b0%d1%86%d0%b8%d0%b8-%d0%bf%d0%be-%d0%be%d0%b1%d1%80%d0%b0%d0%b1%d0%be/ https://cpdp.bg/%D1%81%D0%BF%D0%B8%D1%81%D1%8A%D0%BA-%D0%BD%D0%B0-%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8%D1%82%D0%B5-%D0%BF%D0%BE-%D0%BE%D0%B1%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B2%D0%B0%D0%BD%D0%B5-%D0%BD/
4. Croatia (HR)	https://azop.hr/procjena-ucinka-na-zastitu-podataka-eng-data-protection-impact-assessment-dpia/ https://olivia-gdpr-arc.eu/hr/topic/show/9
5. Cyprus (CY)	
6. Czech Republic (CZ)	https://uoou.gov.cz/media/profesional/metodika-obecneho-posouzeni-vlivu-na-ochranu-osobnich-udaju.pdf
7. Denmark (DK)	https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/konsekvensanalyse
8. EDPS	
9. Estonia (EE)	https://www.aki.ee/uudised/mis-asi-mojuhinnang
10. Finland (FI)	(FI) https://tietosuoja.fi/vaikutustenarviointi (EN) https://tietosuoja.fi/en/impact-assessments
11. France (FR)	(FR) https://www.cnil.fr/fr/guides-aipd (EN) https://www.cnil.fr/en/privacy-impact-assessment-pia
12. Germany (DE)	https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
13. Greece (EL)	(EL) https://www.dpa.gr/el/foreis/ektimisi_adiktipou_kai_diavouleush, https://www.dpa.gr/foreis/ektimisi_adiktipou_kai_diavouleush/ektimisi_adiktipou (EN) https://www.dpa.gr/en/Organisations/Impact_Assessment https://www.dpa.gr/en/by-design/risk-assessment-dpia https://www.dpa.gr/en/by-design/ict-organizational-gdpr-roles-dpia
14. Hungary (HU)	
15. Iceland (IS)	

16. Ireland (IE)	https://www.dataprotection.ie/en/dpc-guidance/guide-data-protection-impact-assessments
17. Italy (IT)	
18. Latvia (LV)	https://www.dvi.gov.lv/lv/novertejums-par-ietekmi-uz-datu-aizsardzibu-nida
19. Lichtenstein	
20. Lithuania (LT)	
21. Luxembourg (LU)	
22. Malta (MT)	https://idpc.org.mt/for-organisations/data-protection-impact-assessment/
23. Netherlands (NL)	(NL) https://autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia (EN) https://autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia
24. Norway (NO)	
25. Poland (PL)	(PL): https://uodo.gov.pl/pl/598/3617 (EN): https://uodo.gov.pl/en/553/1882 https://monitorpolski.gov.pl/MP/2019/666 https://uodo.gov.pl/500 https://uodo.gov.pl/pl/138/605
26. Portugal (PT)	
27. Romania (RO)	
28. Slovakia (SK)	
29. Slovenia (SI)	https://www.ip-rs.si/fileadmin/user_upload/Pdf/Ocene_ucinkov/Smernice_o_ocenah_ucinka_DPIA_julij2018.pdf
30. Spain (ES)	(ES) https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf (EN) https://www.aepd.es/guides/risk-management-and-impact-assessment-in-processing-personal-data.pdf
31. Sweden (SE)	