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

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:

0 OVERVIEW OF THE PROCESSING

0.1 Controller(s)

Note: If there are Joint controllers, one table per controller, adding a row to identify their obligations and tasks

Controller	
Management units responsible for the processing inside the organisation	
Main establishment/point of contact or representative	
Information about the DPO or similar function, if applicable	

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

	Processor	**Definition of their obligations and tasks**
1		
2		
N		

0.3 Name of the processing

Internal name given to the processing (the given name in the record of processing activities)	Audit-Sentinel & Algorithmic Risk Assessment Protocol.
Current version (explaining the history of changes made to the processing in the past, if any)	Version 1.0 (March 2026).

0.4 Planning of the processing

Estimated launch date	
Estimated end date or expiration conditions (if applicable, i.e. because the processing is temporary)	

0.5 DPIA technical sheet

Current version and version log (explaining the history of changes made to the information contained in the DPIA template for this processing, if any)	
Team involved in conducting this DPIA (providing details of their roles, tasks, responsibilities, etc.)	
Guidelines, standards, codes of conduct and other reference materials used to conduct this DPIA[1]	
Reasons to conduct the DPIA[2]	1. New processing activity, DPIA likely to be required due to high-risk (legal obligation under Article 35.3 GDPR): x Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. □ Processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10. □ Systematic monitoring of a publicly accessible area on a large scale. 2. New processing activity, DPIA likely to be required due to likely high-risk (legal obligation under national law): Explanation: _____ 3. New processing activity, DPIA likely to be required due to likely high-risk (following EDPB and national guidance): □ Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements". □ Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person". □ Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area". x Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10.

[1] Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711
[2] Idem.

	□ Data processed on a large scale, considering the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; the geographical extent of the processing activity. □ Matching or combining datasets. □ Data concerning vulnerable data subjects (because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights.) x Innovative use or applying new technological or organisational solutions. □ When the processing in itself "prevents data subjects from exercising a right or using a service or a contract". □ Other (for example, national list regarding the processing operations subject to the requirement of a data protection impact assessment): _____ 4. New processing activity, DPIA necessary or beneficial: □ DPO opinion or recommendation. □ Data subjects' (or their representatives') opinion or recommendation. □ Required by a code of conduct, standard, best practice, etc. □ Other (for example for managing risk or demonstrating accountability and building trust): _____ 5. Existing high-risk processing activity for which there has been a change of the risks: □ Data processing has changed. □ The organisational or societal context for the processing activity has changed. How? _____
Scope of this DPIA (what has been considered and what has been left out of the assessment and why)	
Completion date	
Formal validation date (approval of the DPIA as complete and finished by a responsible official)	
Is the DPIA (or parts of it) intended to be published or to be shared externally?	□ No □ Yes it is going to be published: How?_____ □ Yes, it is going to be shared externally: How? _____

1 SYSTEMATIC DESCRIPTION OF THE PROCESSING

1.1 High-level description of the processing

1.1.a Processed personal data

	Processed personal data (item or element)	Explanation (data type, data subject category, additional details)	Special category of personal data
1		identification data, financial records, customer user transaction flows, and algorithmic behavior profiles. Possible indirect processing of data revealing ethnic origin or health if the audited algorithm presents discriminatory biases in those variables.	□ No Yes: □ Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. X Genetic data. □ Biometric data for the purpose of uniquely identifying a natural person. □ Data concerning health. □ Data concerning a natural person's sex life or sexual orientation.

1.1.b Purposes of the processing

	Purpose: specific and explicit reasons for processing the personal data	Personal data involved (considering personal data listed in 1.1.a) and justification
1	Identification, mitigation and correction of algorithmic biases and corporate criminal liability (CCL) risks for corporate clients.	Forensic detection of fraud, money laundering and the use of deceptive interfaces (Dark Patterns) in audited systems.
2		
N		

1.1.c Secondary or compatible uses

	Secondary or compatible uses of the data	Personal data involved (considering personal data listed in 1.1.a), under what conditions and assessment of compatibility
1		
2		
N		

1.1.d Nature, scope and context of the processing

Nature of the processing: the way personal data will be handled (operations involved, technologies used, etc.).	Automated filtering and in-depth statistical analysis operations on databases provided by the client, using isolated and secure virtual environments.
Scope of the processing: breadth and extent (the volume or scale given the number of data subjects or data items, geographical and organisational reach, frequency or duration for the data subject, etc.).	Large-scale processing determined by the volume of users that the audited corporation has.
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.).	High-Ticket B2B contractual relationship. Is this a cross-border processing? ☐ No X Yes (justification and details): When advising international companies, data may come from multiple EU and Latin American jurisdictions. Is personal data going to be transferred to a recipient in a third country or international organisation? ☐ No ☐ Yes (justification and details): _____

1.2 Functional description

Note: Ideally, this table should be supplemented with one or more diagrams representing data flows or a similar figure.

	Processing phase or stage	Type of operations	Explanation
1		☐ Collection ☐ Use ☐ Storage ☐ Sharing and Transfer ☐ Deletion and Destruction	

1.3 Means of processing, supporting assets and underlying architecture

Processing phase or stage (considering the functional description under 1.2)	Means of processing and supporting assets	Explanation

1.4 Compliance with approved codes of conduct

	Code of conduct	Explanation
1		□ Compliance is likely to be required (legal obligation). Why?:_____ □ Compliance is necessary or beneficial. Why?:_____

2 ANALYSIS OF THE PROCESSING

2.1 Lawfulness of the processing

2.1.a Legal basis

Purpose/use (considering 1.1.b on processing purposes and 1.1.c on secondary or compatible purposes)	Legal basis (Article 6(1) GDPR)	Justification (if applicable, analyse the legitimate interests pursued by the controller or by a third party conducting a balancing test[3])
Article 6 (1)(b) - Performance of a contract and Article 6 (1)(f) - Legitimate interests	□ (a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes. □ (b) The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. □ (c) The processing is necessary for compliance with a legal obligation to which the controller is subject. □ (d) The processing is necessary in order to protect the vital interests of the data subject or of another natural person. □ (e) The processing is necessary for the performance of a task carried out in the public	Article 6(1)(b) - Performance of a contract (The processing is strictly necessary to execute the strategic audit contract with the client) and Article 6(1)(f) - Legitimate interests (Meta-Sentinel Consulting and the client's legitimate interest in ensuring security, transparency and prevention of financial crime)

[3] 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

	interest or in the exercise of official authority vested in the controller. □ (f) The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	

2.1.b Reasons to lift the processing prohibition

Special category of personal data (item or element, considering 1.1.a)	**Reasons to lift the processing prohibition (Article 9(2) GDPR)**	**Justification**
Article 9(2)(f) - Establishment, exercise or defence of legal claims	□ (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the data subject. □ (b) The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject. □ (c) The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. □ (d) The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects. □ (e) The processing relates to personal data which are manifestly made public by the data subject. □ (f) The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity. □ (g) The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. □ (h) The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical	The analysis of sensitive data is carried out within the framework of legal compliance audits, prevention of regulatory sanctions, and preparation of defenses or corporate technical opinions.

	diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 article 9 GDPR. □ (i) The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. □ (j) The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.	

2.2 Data minimisation, retention periods, and data quality

2.2.a Data minimisation and retention periods

Processed personal data (item or element, considering 1.1.a)	**Justification of the need and relevance of the data**	**Recipients**	**Justification**	**Retention period**	**Justification**
Data Minimisation	Immediate application of anonymization and pseudonymization techniques in the backend before starting the technical analysis, eliminating any unnecessary identifiable data.			Retention Period: Raw data is deleted immediately after the technical audit opinion is completed. Only the final, anonymized report is retained for the statutory period of professional liability.	

2.2.b Data quality

Processed personal data (item or element, considering table 1.1.a)	Quality metrics, requirements or thresholds	Justification

2.3 Measures supporting compliance

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

Compliance with Article 5(1)(a-f) GDPR principles	List of supporting measures	Discussion of appropriateness and effectiveness	Implementation status
Fairness principle			□ Planned □ Partially implemented □ Implemented
Transparency principle			□ Planned □ Partially implemented □ Implemented
Purpose limitation principle			□ Planned □ Partially implemented □ Implemented
Data minimisation principle			□ Planned □ Partially implemented □ Implemented
Accuracy principle			□ Planned □ Partially implemented □ Implemented
Storage limitation principle			□ Planned □ Partially implemented □ Implemented
Integrity and confidentiality principle			□ Planned □ Partially implemented □ Implemented
Accountability principle			□ Planned □ Partially implemented □ Implemented

2.3.b Measures supporting the exercise of data subjects' rights

Data subject rights	List of supporting measures	Discussion of appropriateness and effectiveness	Implementation status
Information to be provided to the data subjects (Articles 12, 13 and 14 GDPR)			□ Planned □ Partially implemented □ Implemented
Right of access and to data portability (Articles 15 and 20 GDPR)			□ Planned □ Partially implemented □ Implemented
Right to rectification and to erasure (Articles 16, 17 and 19 GDPR)			□ Planned □ Partially implemented □ Implemented
Right to object and to restriction of processing (Article 18, 19 and 21 GDPR)			□ Planned □ Partially implemented □ Implemented
Right not to be subject to a decision based solely on automated processing (Article 22 GDPR)			□ Planned □ Partially implemented □ Implemented

2.3.c Measures supporting compliance with other GDPR requirements

Compliance with other GDPR requirements	List of supporting measures	Discussion of appropriateness and effectiveness	Implementation status
Requirements on the provisions and withdrawal of consent (Article 7 GDPR)			□ Planned □ Partially implemented □ Implemented
Relationship with processors (Article 28 GDPR)			□ Planned □ Partially implemented □ Implemented
Safeguards relating to international transfer(s) (Chapter V GDPR)			□ Planned □ Partially implemented □ Implemented

2.3.d Measures supporting data protection by design and by default

Data protection by design and by default (Article 25 GDPR)	List of supporting measures	Discussion of appropriateness and effectiveness	Implementation status
UI/UX Integrity		Transparent workflow design. Meta-Sentinel Consulting certifies that its own digital tools do not employ targeted cognitive biases or information fragmentation (Dark Patterns) towards its users or clients.	□ Planned □ Partially implemented X Implemented
			□ Planned □ Partially implemented □ Implemented

2.3.e Measures supporting security of processing

Security of processing (Article 32 GDPR)	List of supporting measures	Discussion of appropriateness and effectiveness	Implementation status (planned/partially implemented/ implemented)
			□ Planned □ Partially implemented □ Implemented
			□ Planned □ Partially implemented □ Implemented

3 CONSIDERATIONS ON NECESSITY AND PROPORTIONALITY

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

	Threats posed by the processing, as it has been designed and planned to be implemented (including technical, legal/contractual and organisational measures to mitigate risk(s))	**How can it be materialised?**	**Risk sources (purpose, wrong design and weaknesses, exposures, etc.)**	**Impact on data subjects' rights and freedoms**
1				

3.2 Assess the necessity of the processing[4]

Evaluate if the envisaged processing is effective and the least intrusive for the data subject's rights and freedoms[5]. Provide evidence (for example, concerning the different considered alternatives) and justification.

3.3 Assess the proportionality of the processing[6]

Discuss the importance of the processing and its potential benefits for the data subject and collectively. Conduct an evaluation that compares the potential impacts on rights and freedoms of data subjects with the advantages resulting from the processing, to ensure that the processing is proportional and fairly balanced. Provide evidence and justification.

[4] 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

[5] EDPB "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR", section II.B, paragraph 29, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf ; See also EDPB "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, Version 1.1, adopted on 23 May 2024", paragraph 32, https://www.edpb.europa.eu/system/files/2024-05/edpb_opinion_202411_facialrecognitionairports_en.pdf

[6] 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 EDPB "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, Version 1.1, adopted on 23 May 2024", paragraph 32, https://www.edpb.europa.eu/system/files/2024-05/edpb_opinion_202411_facialrecognitionairports_en.pdf

4 RISK ASSESSMENT AND MANAGEMENT

4.1 Risk assessment and management

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

Note: Identify, at least, threats that could lead to illegitimate access, undesired modification and disappearance of data.

	Threats posed by malfunctions and deviations from design and default, threats to data confidentiality, integrity and availability (related to cybersecurity), etc.	**How can it be materialised?**	**Risk sources (exposures and errors, vulnerabilities etc.)**	**Impacts on data subjects' rights and freedoms**
1				

4.1.b Method

Explain the details of the method followed to assess and manage risk and provide the necessary information to interpret the following:

- Likelihood and severity levels and their meanings (often a 2 to 5 levels scale is used).
- Risk metrics.
- How to prioritise risks.
- Risk acceptance levels.

If an established method is used, provide the link to the external source introducing this method[7].

4.1.c Inherent risk assessment

Note: If available, this table can be supplemented with one or more diagrams, charts, maps, priority lists, etc. documenting inherent risk assessment from different perspectives.

	Risks to the data subject's rights and freedoms (include scenarios laid out in the first column in 3.1 and 4.1.a)	**Likelihood[8]**	**Severity[9]**	**Modulating factors**	**Risk level**	**Discuss whether the risk is acceptable or not**
1	Risk Scenario 1: Unauthorized access to or breach of highly confidential corporate audit data.	2	4		High	
2	Risk Scenario 2: Persistence of undetected biases in the	2	3		Medium	

[7] For example, the documents listed in the Annex included in the explainer document.
[8] 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.
[9] Idem.

	client's software due to sampling failures					

4.2 Action plan

4.2.a Additional mitigating measures

Note: Include in this table all types of measures (see the different categories in section 2.3)

	Technical, legal/contractual and organisational measures	**Mitigated risks (considering 4.1.c)**	**Discussion of appropriateness and effectiveness**	**Implementation status (partially implemented/ implemented)**
1	Data encryption in transit and at rest (AES-256), exclusive use of secure official channels and sandbox environments without external internet connection during transaction log manipulation	Strict implementation of ISO 27001 (Information Security) and ISO 37001 (Anti-bribery) policies in the internal structure of Meta-Sentinel Consulting.	After the safeguards are implemented, the residual risk is reduced to Low/Acceptable	□ Planned □ Partially implemented X Implemented

4.2.b Residual risk assessment

	Reassessed risks to the data subject's rights and freedoms	**Additional mitigating measures that apply**	**Residual likelihood**	**Residual severity**	**Residual risk level**	**Discuss whether the risk is acceptable or not**
1						

4.2.c Plan

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, and to monitor, review and update the proposed measures once the processing is being carried out.

- Specific activities, responsible team, timelines, etc.
- Links to external documentation or annexes with the details.

5 INVOLVEMENT OF INTERESTED PARTIES

5.1 DPO advice

- If there is a DPO (or a similar function), provide their opinion, conclusions and recommendations concerning the envisaged processing.
- Explain how the DPO's advice has been implemented.

5.2 Views of data subjects or their representatives

- Where appropriate, provide the data subjects' (or their representatives') opinion, conclusions and recommendations concerning the envisaged processing.
- Explain their participation in the DPIA process, including explanations o 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

Based on the assessment of risks and rights, the following decision has been taken:

☐ **REJECTED:** The processing must be abandoned.

☐ **CONSULTATION:** The processing will be consulted with the SA (see 6.2).

☐ Yes, the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high) and does not wish to abandon the processing.

☐ Yes, there is a national law requiring the controller to consult with, and/or obtain prior authorisation from, the SA in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5) GDPR).

X **APPROVED:** The processing may proceed [immediately]. The residual risks are acceptable and there is no national law requiring consultation or prior authorisation from the Supervisory Authority (Article 36(5) GDPR).

☐ **CONDITIONALLY APPROVED:** The processing may proceed only after the following conditions are met:

- *Condition 1:* _____
- *Condition 2:* _____

Optionally, justify the decision made:

APPROVED. Processing may proceed immediately. Residual risks are acceptable, and enhanced due diligence, transparency, and data minimization measures have been implemented in accordance with EU standards.

For the European Data Protection Board

The Chair

Anu Talus