edgeGRC

Use case | Multi-region

Running a DPIA from screening to sign-off

A step-by-step method for data protection impact assessments: deciding when one is needed, describing the processing, assessing necessity and risk, choosing measures and recording the decision.

Last reviewed: 27 November 2026

General information only. Not legal advice, a legal opinion or a certification of compliance.

1 What a DPIA is for

A data protection impact assessment (DPIA) is a structured way to identify and reduce the risks a processing activity poses to people, before the processing starts. Done well, it is a design tool, not a form-filling exercise: it changes the processing so the risk to individuals is lower.

Law	When a DPIA is required
EU GDPR (Article 35)	Before processing that is likely to result in a high risk to individuals' rights and freedoms.
UK GDPR (Article 35)	The same high-risk test. The ICO publishes a list of processing types that require a DPIA.
India DPDP Act (section 10)	Significant Data Fiduciaries must carry out periodic DPIAs; the DPDP Rules set this at once every twelve months.

The method below follows the EU and UK GDPR, which give the most detailed requirements. The same steps work for DPDP assessments and for internal risk reviews where no law requires a DPIA.

2 The eight steps at a glance

1. **Screen:** decide whether a DPIA is needed, and record the decision either way.
2. **Describe the processing:** nature, scope, context and purposes.
3. **Consult:** the DPO, internal stakeholders, processors and, where appropriate, individuals.
4. **Assess necessity and proportionality:** lawful basis, minimisation, retention, transparency and rights.
5. **Identify and assess risks** to individuals, by likelihood and severity.
6. **Choose measures** to reduce each risk, and record the residual risk.
7. **Sign off:** record the DPO's advice, the decision and who made it.
8. **Act and review:** integrate the outcomes into the project, and revisit when anything changes.

3 Step 1: Screening

The GDPR names three cases that always need a DPIA:

- systematic and extensive evaluation of personal aspects based on automated processing (including profiling) that leads to decisions with legal or similarly significant effects;
- large-scale processing of special category data or criminal offence data;
- systematic monitoring of a publicly accessible area on a large scale.

European regulators' guidance on DPIAs (endorsed by the EDPB) adds a set of criteria that indicate likely high risk. As a rule of thumb, processing that meets **two or more** of them will usually need a DPIA:

Criterion	Example
Evaluation or scoring	Credit scoring, behavioural profiling.
Automated decisions with legal or similar effect	Automatic rejection of an application.
Systematic monitoring	Employee monitoring, tracking online behaviour.
Sensitive or highly personal data	Health data, location data, financial data.
Large scale	Many individuals, much data, wide geography or long duration.
Matching or combining datasets	Joining data collected for different purposes.
Vulnerable individuals	Children, employees, patients.
Innovative technology	New uses of AI, biometrics or connected devices.
Processing that blocks a right or service	Data used to decide access to a service or contract.

Also check your supervisory authority's published list of processing that requires a DPIA. If you decide a DPIA is **not** needed, record the reasons. That record is part of your accountability evidence.

4 Step 2: Describe the processing

Start from the record of processing for the activity. Then describe:

- **Nature:** how data is collected, used, stored and deleted, the sources, who has access, the processors and any high-risk technology;
- **Scope:** the categories of data (flag special category data), the number of individuals, the volume, frequency, retention and geography;
- **Context:** the relationship with individuals, their reasonable expectations, any vulnerable groups, prior concerns and the current state of technology;
- **Purposes:** what you want to achieve, the intended effect on individuals and the benefits for you and others.

A simple data flow diagram (collection, systems, sharing, transfers, deletion) helps reviewers spot risks quickly.

5 Step 3: Consult

- **Data Protection Officer:** the GDPR requires controllers to seek the DPO's advice. Record the advice and whether you followed it.

- **Internal stakeholders:** the process owner, information security, IT, legal and anyone who runs the processing day to day.
- **Processors:** they must assist with information about their part of the processing.
- **Individuals or their representatives:** seek their views where appropriate (Article 35(9)), for example through surveys or user research. If you decide not to, record why.

6 Step 4: Necessity and proportionality

Test whether the processing is justified and kept to what is needed:

- [ ] Is the lawful basis identified and appropriate? Is there an Article 9 condition for special category data?
- [ ] Does the processing actually achieve the purpose? Is there a less intrusive way to achieve it?
- [ ] Is each data item necessary? Remove any field you cannot justify.
- [ ] Are retention periods set, and is deletion built in?
- [ ] Will individuals receive clear information, and can they exercise their rights?
- [ ] Do processor contracts cover the processing? Are international transfers covered by a valid mechanism?

7 Step 5: Identify and assess risks

Focus on risks **to individuals**, not to the organisation. Typical risk sources include unauthorised access, inaccurate data, excessive collection, function creep, lack of transparency, unfair automated outcomes and loss of control over data. Consider physical, material and non-material harm such as discrimination, financial loss, distress or reputational damage.

Rate each risk on **likelihood** and **severity** using a consistent scale, and combine them into an overall level:

Likelihood \ Severity	Minimal	Significant	Severe
Remote	Low	Low	Medium
Possible	Low	Medium	High
Probable	Medium	High	High

The scale is illustrative. Use the one your organisation's risk framework defines, and apply it the same way across assessments.

8 Step 6: Measures and residual risk

For each risk, record the measures that reduce it and the resulting **residual risk**:

Risk	Measures	Effect	Residual risk
Example: staff can see more customer data than they need	Role-based access, access reviews, logging	Reduced	Low
Example: data kept longer than necessary	Retention schedule with automated deletion	Eliminated	Low
Example: individuals do not expect the use	Clear notice at collection, easy opt-out	Reduced	Medium

Give each measure an owner and a due date. A measure that is never implemented does not reduce risk.

9 Step 7: Sign-off

- Record who approved the DPIA. That should be a decision-maker with authority over the processing, not only the assessor.
- Record the DPO's advice and, if you did not follow it, the reasons.
- Record which residual risks were accepted, by whom and on what conditions.
- **Prior consultation:** if high risk remains that you cannot reduce, you must consult the supervisory authority before starting the processing (GDPR Article 36). Under the GDPR the authority has up to eight weeks to give written advice, extendable by six weeks for complex processing.

10 Step 8: Act and review

- Feed the measures into the project plan, and check they were delivered before go-live.
- Link the DPIA to the record of processing, the risk register and the evidence of controls.
- Review the DPIA when the processing changes (new data, purpose, technology, vendor or transfer), after a relevant incident, and on a regular cycle. For Significant Data Fiduciaries under India's DPDP Rules, the cycle is at least every twelve months.
- For a reassessment, start from the signed DPIA and focus on what changed. Re-sign the full assessment.

11 DPIA checklist

- [ ] Screening decision recorded, with reasons, including a "no DPIA needed" decision.
- [ ] Processing described: nature, scope, context, purposes and a data flow.
- [ ] DPO advice sought and recorded; stakeholders and processors consulted.
- [ ] Views of individuals sought where appropriate, or reasons recorded for not doing so.
- [ ] Lawful basis, necessity, minimisation, retention, transparency, rights, processors and transfers assessed.

- [ ] Risks to individuals identified and rated by likelihood and severity.
- [ ] Measures recorded with owners, due dates and residual risk.
- [ ] Residual risks accepted by an authorised decision-maker; prior consultation made if high risk remains.
- [ ] Outcomes integrated into the project; review triggers and date set.

12 Official sources

- Regulation (EU) 2016/679 (GDPR), Articles 35 and 36: eur-lex.europa.eu/eli/reg/2016/679/oj
- Article 29 Working Party guidelines on DPIAs (WP248 rev.01), endorsed by the European Data Protection Board: edpb.europa.eu
- ICO guidance on data protection impact assessments: ico.org.uk
- India: the Digital Personal Data Protection Act, 2023, section 10, and the DPDP Rules, 2025: meity.gov.in

---

About this guide

This guide summarises publicly available legislation and regulator guidance in our own words, as of the review date above. Laws, rules and regulator guidance change; always check the current official text and obtain advice appropriate to your organisation's circumstances.

EdgeGRC and Cyber Intelligence Private Limited is an Indian technology company focused on developing software platforms for enterprise privacy management and AI governance. Questions about this guide: **info@edgegrc.com** · edgegrc.com