

GSDC
Global Skill Development Council

DPIA Process and Pre-Launch Checklist

A Practical Guide to Identifying and Managing Privacy Risks Before Launching a Digital Service

DATA PROTECTION IMPACT ASSESSMENT | GDPR COMPLIANCE | PRIVACY BY DESIGN

Understanding the DPIA Process

A Data Protection Impact Assessment (DPIA) is a structured process for identifying, evaluating, and mitigating privacy risks before a digital service is launched or significantly changed. Under GDPR Article 35, a DPIA is mandatory when processing is likely to result in a high risk to the rights and freedoms of individuals — including systematic profiling, large-scale processing of special category data, or large-scale monitoring of publicly accessible areas. Beyond legal obligation, a DPIA functions as a governance tool that helps organisations embed privacy considerations directly into service architecture and development workflows.

The DPIA is not a one-time compliance exercise. It is a living document that must be updated whenever a material change is made to the service, its data flows, or the technologies involved. Organisations that treat the DPIA as a checkbox activity — completed once and filed away — typically miss emerging risks and expose themselves to regulatory scrutiny. The practical value of the assessment lies in the quality of the analysis, not the volume of documentation produced.

When Is a DPIA Required?

- Automated decision-making with legal or significant effects
- Large-scale processing of special category or criminal data
- Systematic monitoring of publicly accessible areas
- Processing biometric data for unique identification
- Processing data relating to vulnerable individuals
- Innovative use of new technologies or novel applications

Five Key Assessment Areas

01

Data Collection & Processing

What data is collected, why, and how it is processed

02

Data Flows & Third-Party Sharing

How data moves between systems and external processors

03

Necessity & Proportionality

Whether collection and processing is limited to what is required

04

Privacy Risk Identification

Systematic identification of risks to individuals

05

Risk Mitigation & Approval

Safeguard selection, residual risk review, and sign-off

Step 1 — Define the Digital Service and Processing Activities

Establishing a clear scope is the foundation of a credible DPIA. Without a precise description of the service, its features, and the personal data it handles, subsequent risk analysis will be incomplete or misdirected. The scope definition should cover the full breadth of processing — not only the primary user-facing features, but also background processes, analytics pipelines, administrative access, and any automated processing that occurs without direct user interaction.

Start by documenting the service's core features and functions, the categories of personal data collected, the data subjects affected (customers, employees, third parties), and the specific purpose for which each data element is collected. Extend this inventory to cover internal systems (CRM, identity management, logging infrastructure) and external providers (cloud platforms, payment processors, analytics vendors). Record where data is stored, in which jurisdiction, and under what legal basis processing is conducted.

Sample Processing Inventory — Digital Banking Application

Data Category	Processing Purpose	Legal Basis	Storage Location	Retention
Full name, DOB, national ID	Customer identity verification	Legal obligation	EU cloud (encrypted)	7 years
Bank account number, sort code	Account management	Contract performance	On-premises database	7 years
Transaction history	Fraud detection, statements	Contract / legitimate interest	EU cloud (encrypted)	7 years
Device ID, IP address	Session authentication	Legitimate interest	Log management system	90 days
Location data (optional)	Fraud prevention	Consent	EU cloud	30 days

Step 2 — Map Personal Data Flows

Data flow mapping traces every movement of personal information from the moment of collection through processing, storage, transfer, and eventual deletion. This is one of the most technically demanding steps of the DPIA, requiring input from both the development team and the security or infrastructure team. A data flow diagram (DFD) should represent all system components that handle personal data, the direction and nature of each data transfer, and the security controls applied at each boundary.

Commonly overlooked exposure points include unnecessary API transfers that send more data than the receiving service requires, excessive sharing with analytics platforms that ingest raw user identifiers, and unsecured integrations with third-party services that lack appropriate data processing agreements. Each integration point is a potential vulnerability — particularly where data crosses organisational or jurisdictional boundaries.

Frontend Applications

Mobile and web interfaces collecting user inputs, device signals, and behavioural data. Validate what is captured at source.

API & Integration Layer

APIs often transmit more fields than required. Review payload definitions and restrict data to minimum necessary transfers.

Backend Services

Core business logic, authentication, and processing engines. Confirm that internal service-to-service calls are authenticated and logged.

Cloud Databases & Storage

Verify encryption at rest, access control configurations, and geographic location of storage in relation to data transfer obligations.

Third-Party Processors

Analytics vendors, payment processors, and identity services. Each must have a valid DPA and must not use data for their own purposes.

Step 3 — Assess Data Necessity and Proportionality

Necessity and proportionality are the analytical heart of the DPIA. GDPR Article 5(1)(c) requires that personal data be "adequate, relevant and limited to what is necessary" in relation to the purposes for which it is processed — the data minimisation principle. This step requires the assessment team to interrogate every data element collected by the service and determine whether it is genuinely required, or whether it has been collected out of habit, convenience, or speculative future utility.

Beyond data minimisation, this step covers purpose limitation (Article 5(1)(b)), ensuring that data collected for one purpose is not repurposed without a compatible legal basis; data accuracy (Article 5(1)(d)), ensuring that mechanisms exist to keep data correct and up to date; and retention periods (Article 5(1)(e)), confirming that data is not held longer than necessary. Where less privacy-intrusive alternatives exist — such as aggregated analytics instead of individual tracking, or one-way hashes instead of storing raw identifiers — these should be evaluated and adopted where feasible.

Necessity Review Table

Data Collected	Intended Purpose	Is It Necessary?
Email address	Account creation, login, notifications	✓ Yes — primary contact and authentication identifier
Mobile number	MFA verification	✓ Yes — required if MFA via SMS is the selected method
Precise location data (continuous)	Fraud detection	⚠️ Partial — approximate location may be sufficient; continuous tracking likely disproportionate
Contact list access	Not defined	× No — no documented processing purpose; collection not justified
Government-issued ID document	KYC / identity verification	✓ Yes — required by financial regulation; must be deleted after verification
Behavioural analytics (page-level)	UX improvement	⚠️ Review — anonymised session data may achieve the same purpose with lower privacy impact
Date of birth (full)	Age verification	⚠️ Review — year-only or age-band may suffice depending on the verification requirement

Step 4 — Identify Privacy Risks

Privacy risk identification requires a systematic review of the service's architecture, access control model, integration landscape, and data processing activities. Unlike a general security risk assessment, privacy risk identification specifically focuses on risks to individuals — the likelihood that processing activities could result in physical, material, or non-material harm to data subjects, including loss of control over personal data, discrimination, identity theft, financial loss, reputational damage, or denial of service.

Reviewers should examine each component of the system against a structured list of risk categories. Common sources of privacy risk in digital services include API endpoints that expose more data than required, database access that is not restricted to need-to-know roles, weak authentication that enables unauthorised access, uncontrolled sharing of data with analytics or advertising platforms, and excessive retention of personal data beyond its defined purpose. Services that use AI or machine learning models must additionally assess whether personal data is transmitted to external AI providers, and whether inference outputs create risks from automated profiling or decision-making.

Risk Identification Matrix

Processing Activity	Vulnerability	Potential Impact on Individuals
Customer identity verification	ID documents stored after verification completes	Identity theft if storage system is compromised
Transaction processing via third-party API	Excessive data fields transmitted in API payload	Unnecessary exposure of financial data to processor
Session and device logging	Logs retained indefinitely without purge policy	Profiling of user behaviour; loss of anonymity
Analytics integration	Raw user identifiers sent to analytics vendor	Third-party tracking; repurposing of data beyond service scope
Automated fraud scoring	No human review of automated decisions	Discriminatory outcomes; denial of financial services
Admin access to production data	No RBAC; all engineers can access live personal data	Insider threat; unauthorised access to sensitive records

Step 5 — Evaluate Privacy Risks

Identified privacy risks must be evaluated to determine their severity and to prioritise mitigation effort. Each risk is assessed against two dimensions: the **likelihood** that the harm will materialise, and the **severity of impact** on affected individuals. Severity should account for the nature and sensitivity of the personal data involved, the number of individuals affected, and whether harm would be reversible. GDPR recital 76 notes that the likelihood and severity of risk should be determined by reference to the nature, scope, context, and purposes of the processing.

Organisations commonly conflate technical risk (likelihood of a system failure or breach) with privacy risk (impact on individuals' rights). These are distinct assessments. A low-probability vulnerability in a system processing highly sensitive health or financial data may still represent a high privacy risk due to the severity of potential harm. Existing security and privacy controls should be noted as mitigating factors, but should not be used to minimise a risk before it has been independently assessed.

Risk Scoring Dimensions

- **Likelihood:** Low / Medium / High — probability that the vulnerability leads to harm
- **Severity:** Low / Medium / High — magnitude of harm to individuals
- **Scope:** Number of data subjects who could be affected
- **Sensitivity:** Nature of the personal data (special category, financial, behavioural)
- **Reversibility:** Whether harm can be undone (identity theft vs. temporary inconvenience)

Sample Risk Register

Risk	Likelihood	Severity	Score
ID documents retained post-verification	Medium	High	HIGH — immediate deletion required
No RBAC on production database	High	High	HIGH — access controls required
Analytics receiving raw user IDs	High	Medium	MEDIUM — pseudonymise before transfer
Session logs retained 12+ months	Medium	Medium	MEDIUM — enforce 90-day purge
Weak password policy on admin accounts	Medium	Low	LOW — enforce MFA and complexity rules

Step 6 — Select Technical and Organisational Safeguards

Safeguards turn evaluated privacy risks into proportionate technical and organisational controls, as required by GDPR Articles 25 and 32, with organisational measures such as processor agreements, access policies, staff training, and incident response being just as important as technical ones.

Risk-to-Safeguard Mapping

Identified Risk	Recommended Safeguard	Type
Unauthorised access to personal data	Role-Based Access Control (RBAC); MFA for all admin accounts	Technical
Data interception in transit	TLS 1.2+ on all endpoints; certificate pinning on mobile client	Technical
Data exposure at rest	AES-256 encryption for databases; key management via HSM	Technical
Excessive API data transfer	API payload review; restrict fields to minimum required; OAuth 2.0 scopes	Technical
Third-party data misuse	Data Processing Agreement; contractual restrictions on sub-processing	Organisational
Excessive data retention	Automated retention schedule; tested deletion workflows	Technical / Organisational
Insider threat	Audit logging; privileged access monitoring; least-privilege policy	Technical / Organisational
Analytics tracking raw identifiers	Pseudonymisation; hashed user IDs before analytics transfer	Technical
Profiling / automated decisions	Human review workflow; documented logic; Article 22 notices	Organisational

Encryption

At rest and in transit for all personal data stores and transfer channels

Access Control

RBAC, MFA, and least-privilege access across all systems

Pseudonymisation

Replace direct identifiers before sharing with analytics or processors

Audit Logging

Comprehensive logs of access, modification, and export of personal data

Processor Agreements

DPAs signed with all third-party processors before go-live

Step 7 — Review Residual Risks and Obtain Approval

After safeguards have been designed and implemented, the assessment team must conduct a residual risk review — a reassessment of each identified risk in light of the controls now in place. The purpose is to determine whether the implemented measures have reduced the risk to an acceptable level, or whether a residual risk remains that requires further action, escalation, or acceptance by an accountable decision-maker. Residual risk is not simply the original risk minus the control; it reflects the risk that remains if the control fails, is misconfigured, or is circumvented.

Where residual risks remain at a high level and cannot be sufficiently mitigated by available technical or organisational measures, GDPR Article 36 requires the controller to consult with the competent supervisory authority prior to processing. This is a binding legal requirement, not an optional governance step. The supervisory authority will typically provide written advice within eight weeks, which may require the controller to delay or redesign the processing activity.

Residual Risk Review Checklist

- All implemented controls verified and tested
- Residual risk re-scored after controls applied
- DPO formal advice recorded in writing
- Stakeholder review completed (legal, security, product)
- Decisions and rationale documented in DPIA record
- High residual risks escalated for acceptance or redesign
- Article 36 consultation triggered where required
- Launch approval granted by accountable owner

⚠ Article 36 prior consultation is legally required where the DPIA indicates that residual high risks cannot be mitigated. Processing must not commence until the supervisory authority has provided advice or the statutory consultation period has elapsed.

Practical DPIA Example — Digital Banking Application

Note: The following case study is illustrative. It is based on a hypothetical digital banking application and is intended to demonstrate how the DPIA process applies in a realistic context. All organisations, services, and risk assessments described are fictional.

A retail bank is preparing to launch a mobile banking application that enables customers to register, verify their identity, manage accounts, make payments, and access location-based features such as nearest branch and ATM finder. The application integrates with a third-party identity verification provider, a payment processor, and a third-party analytics SDK. The service processes identity documents, account data, transaction history, device identifiers, and optional location data for a projected customer base of 500,000 individuals within the first year of operation.

Privacy Risk Assessment — Mobile Banking Application

Processing Activity	Privacy Risk	Risk Level	Recommended Safeguard
Identity verification (KYC)	ID documents retained beyond verification; breach risk exposes government IDs	HIGH	Automated deletion immediately after verification; third-party provider restricted to verification only via DPA
Transaction data processing	Excessive retention of detailed transaction history enabling behavioural profiling	HIGH	Enforce 7-year retention aligned to AML obligations; restrict internal access via RBAC
Analytics SDK integration	Raw user identifiers transmitted to third-party analytics provider	MEDIUM	Pseudonymise user IDs before SDK transmission; review SDK data collection scope; sign DPA
Location-based features	Continuous background location collection beyond stated fraud prevention purpose	MEDIUM	Restrict to foreground collection only; obtain explicit consent; store for maximum 30 days
Automated fraud scoring	Automated decisions to block accounts without human review; potential for discriminatory outcomes	HIGH	Implement mandatory human review for all account blocks; document decision logic; provide Article 22 right to contest

DPIA Documentation and Risk Register Template

A DPIA record serves as both an internal governance tool and evidence of accountability under GDPR Article 5(2). Each row should represent one processing activity and its privacy risk, traceable from identification through to residual risk and resolution.

Processing Activity	Purpose & Legal Basis	Identified Risk	Safeguard	Residual Risk & Status
Customer identity verification *Name, DOB, national ID*	Legal obligation — AML/KYC	ID documents retained post-verification Medium / High	Auto-delete post-verification; DPA with provider	**Low — Closed**
Transaction processing *Account no., transaction data*	Contract performance	Excessive retention enabling profiling Medium / High	7-year retention schedule; RBAC on data access	**Low — Closed**
Analytics SDK *User IDs, page interactions*	Legitimate interest	Raw IDs shared with third party High / Medium	Pseudonymise before transfer; DPA in place	**Low — Closed**
Automated fraud scoring *Transaction patterns, device data*	Legitimate interest / legal obligation	Automated decisions without human review Medium / High	Human review workflow; Article 22 notices	**Medium — Open (owner: Compliance Lead)**
Admin access — production DB *All categories*	Internal operations	No RBAC; all engineers access live data High / High	RBAC implemented; PAM tooling deployed	**Low — Closed**

All processor relationships must have a valid, signed Article 28 DPA before processing can proceed. Add a "Data Recipient / Processor" column when multiple third-party processors are involved.

Pre-Launch DPIA Verification Checklist

Use the following checklist to verify that all DPIA requirements have been addressed before the digital service is approved for launch. This checklist should be completed by the project team in collaboration with the DPO, security lead, and relevant technical owners. All open items must be resolved or formally accepted by an accountable owner before go-live approval is granted.

1. Data Processing

- [ ] All processing activities documented in a processing record
- [ ] Data collection purposes defined and legal bases confirmed
- [ ] Data minimisation reviewed — only necessary data collected
- [ ] Special category data identified and additional legal basis confirmed
- [ ] Retention periods defined for each data category
- [ ] Transparency information provided to data subjects

2. Data Flows and Integrations

- [ ] Data flow diagrams completed and reviewed
- [ ] API payload contents reviewed and restricted to minimum necessary
- [ ] Third-party data sharing documented with legal basis
- [ ] Article 28 DPAs signed with all processors
- [ ] International data transfers assessed; transfer mechanisms in place
- [ ] Analytics and tracking SDKs reviewed and scoped

3. Privacy Risk Assessment

- [ ] Privacy risks identified for all processing activities
- [ ] Likelihood and impact evaluated for each risk
- [ ] High-risk activities reviewed and escalated to DPO
- [ ] Automated decision-making risks specifically assessed
- [ ] AI and machine learning data flows reviewed

4. Safeguards

- [ ] Encryption at rest and in transit verified and tested
- [ ] RBAC and least-privilege access controls implemented
- [ ] MFA enforced for all privileged and administrative accounts
- [ ] Retention schedules implemented and deletion workflows tested
- [ ] Audit logging and monitoring enabled on all personal data stores
- [ ] Penetration testing or privacy testing completed

5. Approval and Documentation

- [ ] Residual risks documented and scored
- [ ] DPO formal advice recorded where applicable
- [ ] Article 36 consultation completed where required
- [ ] Required stakeholder approvals obtained and documented
- [ ] Outstanding items assigned to named responsible owners with deadlines
- [ ] DPIA record finalised and stored under version control

Common DPIA Mistakes and Practical Recommendations

The following mistakes represent the most frequent failures observed in DPIA practice across digital service development programmes. Each failure reduces the effectiveness of the assessment and may result in regulatory non-compliance, unmitigated privacy risks, or enforcement action. Practical recommendations are provided for each.

Conducting the DPIA After Development Is Complete

Mistake: Teams treat the DPIA as a sign-off formality rather than a design input, completing it days before launch when architectural changes are no longer feasible.

Recommendation: Initiate the DPIA at the design phase, before architecture decisions are finalised. Embed a DPIA trigger into the project intake process.

Missing Data Flows Between Third-Party Systems

Mistake: Data flow diagrams cover internal systems only, omitting analytics SDKs, identity providers, payment processors, and sub-processors used by processors.

Recommendation: Require developers and vendors to provide explicit documentation of all data transmitted, including hidden SDK data collection. Audit API payloads in a test environment.

Collecting More Personal Data Than Necessary

Mistake: Services collect data fields "just in case" without documented purposes, violating the data minimisation principle from day one.

Recommendation: Conduct a mandatory necessity review for every data element. Any field without a documented processing purpose and legal basis must be removed before launch.

Treating Security Controls as a Complete Privacy Assessment

Mistake: Teams equate implementing encryption and firewalls with completing a DPIA, without assessing risks to individuals' rights from the nature or purpose of the processing itself.

Recommendation: Maintain separate privacy risk and security risk registers. Privacy risk must assess harm to individuals, not only technical vulnerabilities.

Ignoring Profiling and Automated Decision-Making Risks

Mistake: Fraud scoring, credit assessment, and behavioural analytics are deployed without assessment of discrimination risk, transparency obligations, or Article 22 rights.

Recommendation: Explicitly identify any processing that constitutes automated decision-making. Document the logic, assess fairness risks, and implement human review mechanisms where required.

Failing to Reassess Residual Risks

Mistake: Teams identify risks and assign safeguards but do not re-evaluate whether the safeguard actually reduces the risk to an acceptable level.

Recommendation: Require a formal residual risk re-score after each safeguard is implemented and verified. Only close a risk once the residual score meets the organisation's acceptance threshold.

Not Updating the DPIA After Significant Changes

Mistake: The DPIA is completed once and treated as permanent, even as the service evolves, new integrations are added, and processing volumes grow.

Recommendation: Define a DPIA review trigger list (new processor, new data category, new feature with profiling, significant scale increase) and assign a named owner for DPIA maintenance.

Final Review and GSDC Certification

A well-executed DPIA is one of the most effective privacy engineering tools available to a digital product team. By systematically scoping the service, mapping data flows, assessing necessity, identifying and evaluating privacy risks, selecting proportionate safeguards, and obtaining accountable approval, organisations can launch digital services with confidence — and with the documentation required to demonstrate compliance under GDPR Article 5(2). The seven steps below summarise the complete assessment process.

1

Define the Service

Document processing activities, data categories, purposes, and legal bases

2

Map Data Flows

Trace personal data from collection through all systems to deletion

3

Assess Necessity

Apply data minimisation, purpose limitation, and retention principles

4

Identify Risks

Systematically identify privacy risks to individuals' rights and freedoms

5

Evaluate Risks

Score each risk by likelihood, severity, scope, and sensitivity

6

Implement Safeguards

Select and verify technical and organisational controls proportionate to each risk

7

Review and Approve

Reassess residual risks, obtain DPO advice, and document formal launch approval

> Privacy risks do not resolve themselves after launch. Assessing and mitigating risks before a digital service goes live is not only a regulatory requirement under GDPR — it is the most cost-effective and responsible approach to building data protection into the fabric of digital products from the outset.



Develop Your Data Protection and Privacy Management Knowledge

The **GSDC Certified Data Protection Officer** certification is a professional programme designed to develop practical knowledge of data protection principles, privacy regulations, risk assessment, DPIA methodology, and compliance practices. It is designed for DPOs, privacy professionals, compliance officers, IT managers, and security practitioners working with personal data in digital services.

The certification provides structured knowledge aligned to GDPR obligations, equipping professionals to lead data protection programmes, conduct DPIAs, advise on privacy risks, and demonstrate accountability to regulators and stakeholders.

Explore the GSDC Certified Data Protection Officer Certification

GSDC
Global Skill Development Council

DATA PROTECTION OFFICER CERTIFICATION



ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Understand GDPR and data protection principles.
- Learn data classification and access controls.
- Explore DPIAs, privacy risks, and data governance.
- Understand breach management and compliance.

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org