GSDC

GLOBAL SKILL DEVELOPMENT COUNCIL

FREE STARTER PACK

The DPO Starter Pack

The GDPR tools & templates a DPO actually uses

A free starter pack of the most-used data-protection artifacts — a sample DPIA and DPIA guide, a ROPA template and data-mapping starter, a GDPR audit checklist and retention-policy template — plus a neutral shortlist of the GDPR compliance tools and privacy-management platforms teams actually use. Adaptable today.

4
ARTIFACTS

28-Page Field Guide • DPIA · ROPA • Audit & Retention • Tools Shortlist

Four artifacts you can adapt today

This isn't a catalogue — it's a starter pack. Four of the most-used DPO artifacts, each shown as an adaptable sample with a short how-to, plus an honest shortlist of the software teams use to run them at scale. Take it, adapt it, and you're moving today.

1 Sample DPIA + impact-assessment guide

2 ROPA template + data-mapping starter

3 GDPR audit checklist + retention-policy template

4 Shortlist of GDPR tools & privacy platforms

\+ How the artifacts & tools fit together

\+ Article map, glossary, FAQ & quick-start

How to use this pack: each template is a starting point, not a finished document. Adapt the wording to your organisation, fill in your real processing, and have a colleague review it. A starter artifact in use beats a perfect one that never ships.

A note on the tools shortlist: it's organised by job and named neutrally — no endorsements. The right tool depends entirely on your size, budget and stack.

ARTIFACT 1

The DPIA

Data Protection Impact Assessment — the guide

A DPIA is a structured way to identify and reduce the privacy risks of a project *before* it goes live — a risk assessment for people's data, required under Article 35 when processing is likely to be high-risk.

When a DPIA is required

- Large-scale processing of sensitive data
- Systematic monitoring of public areas
- Profiling with significant effects
- New or high-risk technologies

When in doubt, run the short screening first (next page). If it flags risk, do the full DPIA. Doing one when not strictly required is rarely wasted effort — it's evidence of accountability.

The mindset: a DPIA isn't box-ticking — it's asking "how could this hurt someone, and how do we prevent it?" while changes are still cheap.

SAMPLE · DPIA TEMPLATE

DPIA template — the sections

A working DPIA template captures these sections. Copy the structure and fill in your project's detail.

Section	What you record
1 · Describe the processing	What data, why, how, scope & duration
2 · Necessity & proportionality	Why it's needed; lawful basis
3 · Consultation	Views of stakeholders & the DPO
4 · Risks to individuals	Each risk, scored by likelihood & severity
5 · Mitigations	Measures to reduce each risk
6 · Outcome & sign-off	Residual risk; approval; consult regulator if high

Tip: keep section 1 factual and specific — a vague description undermines the whole assessment.

SAMPLE · DPIA SCREENING & SCORING

DPIA screening & risk scoring

Two quick tools that make the DPIA practical: a screening checklist to decide if one is needed, and a simple way to score risk.

SCREENING — DO WE NEED A DPIA?

- Sensitive / special-category data?
- Large scale?
- Systematic monitoring?
- Profiling or automated decisions?
- New technology?

SCORING — RATE EACH RISK

- Likelihood: low / med / high
- Severity: low / med / high
- Combine for overall risk
- Mitigate; re-score residual

Residual risk	Action
Low	Proceed with standard controls
Medium	Add mitigations; document & monitor
High	Mitigate hard; if still high, consult the supervisory authority

ARTIFACT 2

The ROPA

Records of Processing Activities (Article 30)

The ROPA is the central accountability record — the map of everything your organisation does with personal data. One row per processing activity.

SAMPLE · ROPA TEMPLATE

Field	Example entry
Processing activity	Customer email marketing
Purpose	Send offers to opted-in customers
Lawful basis	Consent (Art 6(1)(a))
Data categories	Name, email, preferences
Data subjects	Customers & subscribers
Recipients	Email platform (processor)
Transfers	US — via SCCs
Retention	Until consent withdrawn + 30 days
Security measures	Access control, encryption

Build one row per activity — start with your ten biggest and grow from there.

Data-mapping starter

A ROPA is only as good as the data map behind it. Data mapping is simply working out what personal data you hold, where it lives, and where it flows. Here's a starter method.

1. **List your systems**
   Every app, database & tool that holds personal data
2. **For each, note the data**
   What categories of personal data it holds & about whom
3. **Trace the flows**
   Where data comes from & where it goes (incl. processors)
4. **Flag the risks**
   Transfers abroad, sensitive data, long retention
5. **Feed it into the ROPA**
   Each mapped activity becomes a ROPA row

> **Start small:** a spreadsheet covering your top systems is a perfectly good first data map. Tools (Section 4) help once the scale outgrows a spreadsheet.

SAMPLE · DATA MAP

A data map, worked

What a simple data-map row looks like once filled in — the bridge between “what systems do we have” and a finished ROPA.

System	Data held	Source → flow	Risk flag
CRM	Contact & sales data	Web forms → sales team	—
Email platform	Name, email, consent	CRM → US processor	**Transfer**
HR system	Employee records	Onboarding → payroll	**Sensitive**
Support desk	Tickets & messages	Customers → agents	**Retention**

Why the risk flags matter: they tell you where to focus next — a transfer needs SCCs, sensitive data needs extra care, long retention needs a schedule. The map doesn’t just record; it points to your next actions.

ARTIFACT 3

GDPR Audit Checklist

Self-check your programme — part 1

A practical checklist to gauge where your data-protection programme stands. Mark each: **Yes**, **Partial**, or **No** — the gaps are your to-do list.

☐	Lawfulness & records
☐	We have a ROPA covering all processing
☐	Each activity has a documented lawful basis
☐	Privacy notices are accurate & accessible
☐	We have a data-protection policy in force
☐	Consent (where used) is freely given & logged
☐	A retention schedule is defined & applied

Part 2 (rights, security, breaches & third parties) on the next page.

GDPR audit checklist — part 2

☐	Rights & security
☐	A DSAR procedure handles requests within a month
☐	All data subject rights can be actioned
☐	Appropriate security measures are in place (Art 32)
☐	Privacy by design is applied to new projects

☐	Breach & third parties
☐	A breach plan covers the 72-hour rule
☐	A breach register logs all incidents
☐	Processors are covered by DPAs (Art 28)
☐	International transfers use a valid mechanism
☐	A DPO (or lead) is designated where required

Any “No” or “Partial” is a priority — tackle the highest-risk gaps first.

ARTIFACT 4

Data Retention Policy

Keep data no longer than needed

Storage limitation (one of the seven principles) means not keeping data forever. A retention policy sets how long each type of data is kept — and when it's deleted.

SAMPLE · RETENTION POLICY STRUCTURE

1. **Purpose & scope**
   What the policy covers & who owns it
2. **Retention schedule**
   Each data type, its period & the reason (next page)
3. **Deletion method**
   How data is securely deleted or anonymised
4. **Review cycle**
   How often the policy is reviewed & updated

SAMPLE · RETENTION SCHEDULE

Retention schedule — sample rows

The heart of the policy: a table mapping each data type to how long it's kept and why. These are illustrative — set your own periods against your legal & business needs.

Data type	Retention period	Reason
Marketing contacts	Until consent withdrawn	Consent basis
Customer orders	6–7 years (typical)	Tax / legal
Job applicants (unsuccessful)	6–12 months	Recruitment record
Employee records	Duration + statutory period	Employment law
Support tickets	2–3 years	Service history
Website analytics	14–26 months	Business need

Always confirm periods against the laws that apply to you — these are starting points, not legal advice.

SECTION 2

Tools & Platforms

A neutral shortlist, by job

Templates take you a long way, but at scale teams reach for software. The crucial thing to understand first: **GDPR compliance software isn't one product** — it's several different jobs, and most tools cover only some of them.

The jobs GDPR software does

- Consent / cookie management
- Data discovery & mapping
- Vendor / processor management
- DSAR & rights automation
- DPIA / ROPA workflow
- Breach & security (Art 32–34)

The common trap: a cookie-consent tool makes your banner defensible — it does *not* make you GDPR-compliant. Consent is just one of six lawful bases and one of several jobs. Many organisations combine a consent tool with a broader platform.

Comprehensive privacy-management platforms

These aim to cover many jobs in one suite — typically used by larger teams. Listed neutrally; capabilities & pricing change, so evaluate against your own needs.

- **OneTrust**
  One of the most widely used; broad coverage (consent, DSAR, data mapping, DPIA/ROPA). Enterprise-scale; can be complex & costly
- **TrustArc**
  Structured privacy programmes plus managed services; strong DPIA/PIA/ROPA & cookie consent
- **Securiti**
  Data-first: discovery & classification across systems, feeding privacy workflows
- **BigID**
  Deep data discovery, classification & mapping; strong for complex data estates

Multi-framework note: platforms like Vanta & Drata cover GDPR alongside SOC 2 / ISO 27001 — useful if audit-readiness across frameworks is the goal.

Consent & cookie management (CMPs)

Consent management platforms handle the website consent layer — cookie banners, granular choices and the consent audit trail (Articles 6–7 at the web layer).

- **Cookiebot**
  Widely used cookie consent & scanning
- **Usercentrics**
  Consent management with optimisation, popular in Europe
- **Didomi**
  Strong for media, publishing & regulated industries
- **Osano**
  Simple, fast-to-deploy consent & basic privacy features
- **Ketch / Enzuzo**
  No-code consent orchestration; accessible for smaller teams

Remember: passing a cookie audit means your consent banner is defensible — not that the whole organisation is GDPR-compliant. A CMP is one piece of the picture, usually paired with a broader tool or solid templates.

DSAR automation & data discovery

Two more specialised jobs: automating individuals' rights requests, and finding & mapping personal data across systems.

DSAR / RIGHTS AUTOMATION

- **DataGrail** — many integrations
- **Transcend** — security-focused fulfilment
- **Ketch** — API-driven orchestration

DATA DISCOVERY & MAPPING

- **BigID** — discovery & classification
- **Securiti** — data intelligence
- Suites (OneTrust/TrustArc) include mapping modules

These shine when scale outgrows manual work — hundreds of DSARs a month, or personal data scattered across dozens of systems. Below that, a good DSAR procedure and a spreadsheet data map (your starter-pack artifacts) often suffice.

> **Fair caveat:** tool names, features & ownership shift over time. Treat this as a map of the categories, then check current capabilities before you buy.

How to choose (or whether to)

Before buying anything, work out which jobs you actually need to cover — then match tools to those, not the other way around.

1. **Start with the templates**
   For small teams, the starter-pack artifacts may be enough

2. **Identify your real jobs**
   Consent? DSARs at scale? Data discovery? Don't buy jobs you don't have

3. **Mind the gaps & overlaps**
   One suite, or several point tools? Avoid paying twice for the same job

4. **Weigh cost & complexity**
   Enterprise suites are powerful but heavy to implement

THE HONEST TAKE

No tool makes you compliant on its own — it automates work you must still understand. A DPO who knows the templates and the law can run a solid programme on a spreadsheet; tools then scale that work. Knowledge first, tools second.

SECTION 3

How It Fits Together

Artifacts + tools, in one flow

The four artifacts and the tools aren't separate — they're one workflow. Here's how a DPO uses them together.

1	2	3	4	5
Map	**Assess**	**Control**	**Check**	**Scale**
Data map → ROPA	DPIA on risky processing	Retention & policies	Audit checklist	Tools where needed

Start with the templates to establish the programme; add tooling only where volume or complexity demands it. The audit checklist is your recurring health check that keeps the whole thing honest.

One coherent system: map what you have, assess what's risky, control how long you keep it, check yourself regularly, and automate the heavy lifting last.

The four artifacts, article-mapped

Each starter artifact exists to help satisfy specific GDPR requirements. The map:

Artifact	Helps satisfy	In short
DPIA	Article 35	Assess high-risk processing before it starts
ROPA + data map	Article 30	Document what you do with personal data
Audit checklist	Articles 5 & 24	Demonstrate accountability & find gaps
Retention policy	Article 5(1)(e)	Keep data no longer than necessary

Why mapping matters: a DPO doesn't just produce documents — they can point to the article each one serves. That's the difference between paperwork and accountability you can defend to a regulator.

Common mistakes with these artifacts

A few traps that turn good templates into weak compliance. Avoid these.

THE MISTAKE	THE FIX
A ROPA that's out of date	Review the ROPA on a schedule
A DPIA done after launch	Run the DPIA at design stage
A retention policy nobody applies	Automate deletion to the schedule
Treating a cookie tool as "done"	Cover all six jobs, not just consent
Templates filled in vaguely	Be specific & factual

The pattern: these artifacts only protect you if they're accurate, current and actually used. A living document beats a perfect one in a drawer.

From starter pack to full programme

This pack covers the essentials. As your programme matures, you'll add more artifacts — here's what comes next.

→ **Privacy notices & DSAR procedures**
Operationalise individuals' rights

→ **Breach response playbook & register**
Be ready for the 72-hour clock

→ **DPAs & processor due diligence**
Govern your third parties (Art 28)

→ **Training & awareness materials**
Build a privacy culture across the org

→ **LIAs, TIAs & a DPO activity log**
The mature programme's supporting records

The good news: the four artifacts here teach the pattern — describe, assess, document, control. Every later artifact follows the same logic.

THE CREDENTIAL

Where This Is Taught

The certification behind the toolkit

GSDC

GLOBAL SKILL DEVELOPMENT COUNCIL

This is to certify that

[Your Name]

has successfully achieved the credential of

Certified Data Protection Officer

Credential ID: GSDC-DPO-2026-XXXX

Globally recognised

DPO

Build every artifact — with judgement

The Data Protection Officer program teaches you to build and apply each of these tools, and the judgement to know which to reach for, when — the skill behind the templates.

GDPR quick-reference

The articles these starter artifacts touch, on one page.

Art 5 — the 7 principles, including storage limitation & accountability.

Art 6 — the 6 lawful bases for processing.

Art 7 — conditions for valid consent.

Art 24 — responsibility of the controller (accountability).

Art 28 — processors & the DPA requirement.

Art 30 — records of processing (the ROPA).

Art 32 — security of processing.

Art 33–34 — breach notification (72 hours).

Art 35 — data protection impact assessments (DPIAs).

Ch. V — international transfers (adequacy, SCCs).

Starter-pack glossary

The terms in this pack, in plain English.

DPIA — Data Protection Impact Assessment; a risk assessment for higher-risk processing (Art 35).

ROPA — Records of Processing Activities; the Article 30 register of what you do with data.

Data mapping — working out what personal data you hold, where it lives & how it flows.

Retention schedule — how long each data type is kept before deletion.

DSAR — Data Subject Access Request; an individual's request to see their data.

CMP — Consent Management Platform; handles website cookie/consent choices.

DPA — Data Processing Agreement; the Article 28 contract with a processor.

SCCs — Standard Contractual Clauses; a safeguard for international transfers.

Lawful basis — the legal reason for processing (one of six under Art 6).

Data discovery — finding & classifying personal data across systems, often via software.

Frequently asked questions

Can I really adapt these templates today?

Yes — that's the point. Copy the structures, fill in your real processing, and have a colleague review. A starter version in use beats a perfect one that never ships.

Do I need to buy a tool to be compliant?

No. Small teams can run a solid programme on templates and a spreadsheet. Tools help when scale or complexity outgrows manual work.

Is a cookie-consent tool enough for GDPR?

No — it covers the consent layer only. GDPR spans several jobs (records, rights, breaches, transfers, security); consent is just one.

Are these templates legal advice?

No — they're practical starting points. Confirm specifics (especially retention periods) against the laws that apply to you.

Where do I learn to use all this properly?

The GSDC Data Protection Officer program teaches each artifact hands-on, with the judgement to apply them — see the next pages.

The starter pack on one page

Everything here, distilled — your at-a-glance checklist.

Artifact	What it does	Build it…
DPIA + guide	Assess risk before launch	Per risky project
ROPA + data map	Document your processing	Once, then maintain
Audit checklist	Find your gaps	Quarterly
Retention policy	Don’t over-keep data	Once, then review

Tools by job (evaluate for your needs)

- Suites: OneTrust, TrustArc, Securiti, BigID
- Consent: Cookiebot, Usercentrics, Didomi, Osano
- DSAR: DataGrail, Transcend, Ketch
- Multi-framework: Vanta, Drata

Tool names & features change — verify current capabilities before choosing.

Your first-week quick-start

Don’t wait for perfect. Do these five this week and you’ve started a real programme.

Adapt today

- \2713 Copy the ROPA template
- \2713 List your top 10 systems (data map)
- \2713 Copy the retention schedule

Assess

- \2713 Run the audit checklist
- \2713 Note every “No” / “Partial”
- \2713 Pick your top 3 gaps

Plan

- \2713 Adopt the DPIA template
- \2713 Decide: templates or a tool?
- \2713 Book time to close gap #1

One week, four artifacts started. That’s further than most organisations get in a month — and the foundation everything else builds on.

GSDC

Four artifacts.
One running start.

A sample DPIA and guide, a ROPA and data-mapping starter, a GDPR audit checklist and retention-policy template, and an honest shortlist of the tools teams use — everything you need to start running a real data-protection programme today.

Next steps & resources

Explore the toolkit
The full set of DPO tools & templates.

Enrol in the program
Self-paced, globally recognised, toolkit included.

Grab the study materials
Modules, case study & practice questions.

Talk to an advisor
Questions about the toolkit or path? Ask.

OFFER ENDS SOON

Adapt the pack — then master it.

You've got the four core artifacts and a clear-eyed tools shortlist. The full editable toolkit and the skill to run it come with the program. Join the GSDC DPO program; this offer closes in 48 hours.

FINAL CALL · OFFER VALID 48 HOURS

Enroll Now ›