

Outsourced DPO & Privacy Office: The Enterprise Buyer's Guide



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval.
NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Decide whether each entity needs a formal DPO designation.
2. Apply the independence and capacity gates before comparing price.
3. Use the selection matrix and contract checklist to make a documented appointment decision.

How to select a defensible statutory DPO arrangement, protect independence, define the Privacy Office mandate and procure effective oversight across complex organisations

Executive summary

Choosing an outsourced Data Protection Officer (DPO) is not simply deciding who will answer privacy questions or complete a compliance checklist. Where a formal appointment is required — or voluntarily made — the appointment must provide an appropriately qualified, independent DPO with sufficient resources, timely involvement, direct access to senior management and the capacity to fulfil statutory tasks. A supplier's wider operational services are a different question. [S1][S2]

A buyer can secure extensive Privacy Office administration yet still procure a weak DPO mandate. Conversely, a credible statutory DPO may provide strong independent oversight without undertaking every operational task within a client's privacy programme. **These are distinct capabilities, and the contract should make the boundary visible.**

This guide helps enterprises to answer five decisions:

1. **Duty:** Must each relevant organisation appoint a DPO, or would non-statutory privacy governance support be the better fit?
2. **Mandate:** Which responsibilities belong to the DPO, to management, and to a separately scoped Privacy Office?
3. **Independence:** Can the DPO challenge processing decisions and the performance of any operational team without conflicts of interest?
4. **Coverage:** Will the provider have the expertise, access, availability and cross-border arrangements that your actual processing demands?
5. **Evidence:** Can procurement defend its provider choice with documented criteria, hard-stop safeguards and a usable statement of work?

The central principle is **appoint for independence and competence; scope for operational delivery; contract for accountability; and measure the quality of evidence and advice.**

This guide includes a statutory responsibilities reference table, independence/conflicts framework, operating-model comparison, group and international applicability matrix, service-scope ledger, procurement questions, a weighted DPO service-selection matrix and a board decision memorandum.

At a glance: what exactly are you buying?

Component	Primary purpose	Accountability boundary	The contractual question
Formal statutory DPO	Independent advice, monitoring, DPIA advice, regulator and data-subject contact	The controller or processor remains responsible for its legal compliance and decisions	Who is appointed, how is independence preserved, and are all statutory tasks supported?
Retained privacy governance / Privacy Office	Organises recurring privacy work, programme coordination, risk registers, reporting and agreed operational support	Operational decisions remain with the designated organisational owners	What tasks, capacity, outputs and response processes are actually included?
Project consultancy	Defined work such as a maturity assessment, policy review or transfer assessment	Project deliverables do not automatically amount to statutory DPO appointment	What is the project scope, acceptance criterion and handover?
UK/EU Article 27 representative	Where required, serves a distinct territorial contact role for relevant controllers/processors without an establishment in the jurisdiction	The representation mandate is not the DPO mandate	Does an obligation arise in each jurisdiction and who is separately authorised to fulfil it?
Internal privacy team	Implements controls, handles workflows, owns data and risk decisions	Does not lose its responsibilities when an external DPO is appointed	Which named internal owners can act on advice and maintain records?

Buyer safeguard: A UK GDPR Article 27 representative and an EU GDPR Article 27 representative are separate territorial appointments where the respective legal test is met. Neither follows automatically from retaining a UK or EU DPO, and neither is included unless expressly commissioned and deliverable in the relevant jurisdiction. [S7][S8]

Decision rule: Do not substitute a privacy-helpdesk subscription for a statutory DPO appointment. Equally, do not purchase a formal DPO appointment merely because an organisation needs short-term DPIA, DSAR, records-of-processing or policy support. Establish the legal need and buying objective first.

1. When must a UK organisation appoint a DPO?

Under UK GDPR Article 37, appointment is required where processing is carried out by a public authority or body (subject to the courts' judicial-capacity exception); where core activities involve large-scale, regular and systematic monitoring of individuals; or where core activities involve large-scale processing of special-category data or information concerning criminal convictions and offences. These conditions apply to controllers and processors. Other applicable laws may introduce additional requirements. [S1][S2]

The analysis must be specific. Organisation size alone is not the test, and processing ordinary customer information does not automatically make a DPO compulsory. Conversely, a relatively small enterprise may still need one because of the nature, scale and purpose of its processing.

A voluntary appointment is possible, but **once an organisation formally appoints a DPO under the UK GDPR, the role must meet the same position and task safeguards as a mandatory appointment.** If the need is only for non-statutory privacy support, describe that role accurately rather than calling it a DPO without accepting the corresponding obligations. [S1]

DPO designation triage: questions for the board and procurement team

Question	Evidence to examine	Required action if uncertain
Are we a public authority or body, or subject to an additional sector-specific duty?	Legal status, statutory functions, operating entities	Obtain legal analysis, including any applicable exception
Do our core activities involve regular, systematic, large-scale monitoring?	Business model, profiling/monitoring inventory, volume, duration and reach	Assess activities, not merely employee count
Do our core activities involve large-scale special-category or criminal-offence data?	Clinical, HR, research, biometric and other processing registers	Evaluate scale and core purpose with documented reasoning
Are we both a controller and processor in different operations?	Contracts, processing purposes, data-flow maps	Assess DPO duties for relevant capacities
Are other jurisdictions or entities involved?	Group entity list, establishments, targeting and monitoring footprints	Evaluate EU GDPR and local-law obligations separately
If no appointment is mandatory, do we nevertheless want a formal DPO?	Governance objectives and role specification	Record whether voluntary designation or non-statutory advisory support is intended

Record the outcome: entity, applicable law, rationale, date, reviewer and whether the proposed role is a statutory/voluntary DPO designation or a separate privacy adviser. A documented negative determination should be revisited when the organisation's activities materially change.

2. Statutory DPO responsibilities: what cannot be stripped out

Articles 37–39 of the UK GDPR establish the DPO's designation, position and core tasks. The externally appointed DPO should have the same statutory standing as an appropriately appointed internal DPO. These responsibilities should not disappear inside tiered packages or be made optional by a restricted monthly-hour allowance. [S1][S2]

Statutory responsibility or safeguard	What this means in practice	Evidence buyers should request
Inform and advise the controller/processor and relevant personnel	Relevant, documented advice on data protection duties and consequences	Advisory record, routes for obtaining advice, escalation examples
Monitor compliance with law and internal policies	Risk-based review of responsibilities, awareness, training arrangements and audits	Monitoring plan, findings register, reporting format
Advise on DPIAs and monitor their performance	Input at the appropriate time, including scrutiny of risk and controls	DPIA consultation workflow, advice logs, evidence of follow-up
Co-operate with the UK supervisory authority	Maintain an effective regulator contact and consultation process	Contact protocol and responsibility map
Act as regulatory contact point	Communicate, including where consultation is appropriate	Published contact details and regulator notification evidence
Be accessible to individuals	Ensure suitable channels for people who need to contact the DPO	Publicly available contact route, appropriate confidentiality measures
Act independently	No direction about the result of statutory advice or monitoring; no penalty for proper discharge of tasks	Independence clause, escalation process, conflicts register
Report to highest management level	Ability to escalate directly to senior decision-makers when necessary	Board access, meeting rights, reporting cadence

Statutory responsibility or safeguard	What this means in practice	Evidence buyers should request
Receive adequate resources and timely access	Sufficient time, information, training, tools, organisational support and continuity	Capacity plan, executive sponsor, access arrangements and named cover
Avoid conflicting duties	No task that makes the DPO determine purposes/means of the processing they are expected to oversee	Role map and independence assessment

A critical procurement test: A capped-hours retainer can define operational capacity and change-control arrangements, but it must not be framed as removing the DPO's statutory functions. Where capacity is inadequate for the actual organisation, the remedy is to adjust scope, staffing, escalation arrangements or the appointment model — not to disclaim mandatory functions.

What the DPO does not take away from management

The **controller** determines the purposes and means of processing and is responsible for its lawful basis and applicable controller duties. A **processor** acts on the controller's documented lawful instructions and retains its own statutory and contractual responsibilities; it does not ordinarily decide the controller's purposes and means. Each organisation remains responsible for the decisions, resources and controls within its role. The DPO advises and monitors rather than taking over those management responsibilities. [S3][S4]

For a DPIA, for example, the organisation retains responsibility for the assessment and must seek the DPO's advice. If it departs from the advice, it should document why and how the decision is justified. [S4]

Complaint handling is a separate operational process. The ICO states that the DUAA data-protection provisions were in force by 19 June 2026. Organisations must acknowledge a data-protection complaint within 30 days and respond without undue delay; 30 days is not a universal deadline for final resolution. Allocate that process explicitly rather than assuming an outsourced DPO administers it. [S9][S11]

3. Independence is not a line in the contract: the DPO integrity test

A mature buyer assesses independence **before** evaluating cost, technology or promised turnaround. An external provider can be highly experienced and still be unsuitable if it controls the processing activities it must independently challenge.

The IG-Smart DPO Mandate Integrity Test — a practical procurement model

This is an IG-Smart proposed decision aid, not an official ICO assessment, accreditation, certification or independently validated benchmark.

Gate I — Appointment integrity. Is the organisation's statutory designation need assessed, the appointed person/team identifiable and the contract sufficient to support all DPO responsibilities?

Gate II — Independence. Does the DPO have freedom from instructions on professional findings; direct access to the highest management level; a documented conflict assessment; and a mechanism to record dissent?

Gate III — Operational sufficiency. Are expected workload, response channels, specialist cover, language, incident availability, access to data and reporting proportionate to the organisation's risk?

Gate IV — Role separation. Are the DPO's oversight tasks clearly distinguished from the client's operational responsibilities and any additional provider-delivered services?

Gate V — Defensible decisions. Can the organisation show advice, follow-up, management acceptance or rejection, escalation and periodic review without implying that the DPO has guaranteed compliance?

A failed gate is not offset by a low fee or a polished proposal. Rectify it before treating the supplier as an eligible formal-DPO candidate.

Common conflicts and safeguards

Arrangement	Independence concern	Safeguard / buyer response
Chief executive, head of IT, HR leader or similar business owner also acts as DPO	Role may determine purposes and means of processing that the DPO must review	Assess actual decision authority; separate the appointment if materially conflicting
DPO provider designs a programme and independently certifies its own success	Self-review risk and confusion about independent assurance	Separate implementer and reviewer or obtain independent assurance where needed
Provider handles DSAR administration and statutory DPO oversight	The DPO may be asked to assess the quality of work under provider control	Allocate operational ownership; document supervision, escalation and independent challenge
DPO reports only to the manager whose decisions are under review	Impaired escalation	Contract direct board-level access and unfiltered reporting
DPO must obtain pre-approval before giving adverse regulatory advice	Independence compromised	Remove approval rights over advice; preserve confidential escalation routes
A shared DPO covers many complex entities without named cover	Resource and accessibility risk	Require entity-by-entity coverage plan, capacity evidence and deputies

Conflicts depend on **actual authority and duties**, not job titles alone. The EDPB identifies roles deciding processing purposes and means as particularly problematic; external-provider conflicts also require scrutiny. [S5]

The 'advice–decision–implementation–challenge' chain

A particularly useful separation for larger engagements is:

1. **DPO advises and monitors** — identifies legal and governance concerns.
2. **Management decides** — accepts, defers or rejects recommendations with recorded reasons.
3. **Operational owner implements** — carries out policy, DPIA, access request, system or supplier remediation work.
4. **DPO reviews and escalates** — monitors the evidence and retains freedom to challenge the outcome.

This chain is an operating recommendation. It is not a statutory four-stage procedure. It preserves the organisation's accountability and helps avoid an adviser acting as the sole judge of work they deliver.

4. Scope ledger: a statutory appointment is not an unlimited Privacy Office

The statement of work should distinguish **A. mandatory DPO tasks**, **B. agreed governance support**, **C. separately commissioned operational support**, **D. client obligations**, and **E. exclusions and safeguards**.

Scope category	What should be documented	Commercial rule
A. Statutory DPO functions	Article 39 duties and Article 38 safeguards, including advice, monitoring, DPIA advice, supervisory-authority co-operation and contact	Not optional where a DPO is formally appointed
B. Retained governance delivery	Agreed reporting rhythm, risk register, escalation procedures, programme reviews, governance meetings and relevant advisory outputs	Describe capacity and reasonable service expectations precisely
C. Separately scoped operational support	Rights-request administration; detailed records-of-processing administration; policy remediation; major maturity programmes; complex breach investigations; specialist transfer projects; training; cyber-incident support; other agreed consultancy	Do not imply automatic inclusion in the statutory appointment; assess conflicts
D. Client-owned responsibilities	Business decisions, lawful basis, control implementation, system and data access, risk acceptance, staff, recordkeeping, resource provision and regulatory accountability	Named internal owner and timely co-operation required
E. Exclusions and safeguards	Work not contracted; legal representation; certification or outcome guarantees; decisions impairing independence; specialist appointments not agreed	Exclusions cannot remove statutory tasks in A

The provider may offer some category C services where genuinely supported and individually contracted. Procurement should not treat this table as proof that every listed service is included in IG-Smart's DPO retainer.

Three outcomes to demand from the statement of work

- **An appointment that is legally intelligible:** named accountable parties, appointment scope, contact routes, reporting and independence.
- **An operating model that can actually function:** capacity, continuity, working procedures, information access, records and escalation.
- **Commercial boundaries that prevent disputes:** what is included, what requires an additional statement of work, responsibilities and a change-control mechanism.

5. Compare operating models before comparing providers

Model	Best fit	Strength	Main limitation / risk	Procurement check
Internal DPO	High-volume, complex organisation with strong permanent talent pipeline	Deep day-to-day knowledge and accessibility	Recruitment continuity, internal conflicts, skill coverage	Protect independent challenge and direct senior access
External DPO on a retainer	Needs formal designation and sustained specialist oversight without permanent appointment	Specialist expertise, continuity through defined contract and independent perspective	Insufficient hours or poor integration with internal teams	Examine named coverage, capacity, escalation and conflicts

Model	Best fit	Strength	Main limitation / risk	Procurement check
Hybrid: external DPO + internal Privacy Office	Regulated groups with substantial operational work and a need for independent oversight	Separates challenge from execution and can scale operationally	Hand-off gaps, duplicate work and unclear decision ownership	Obtain responsibility matrix and escalation rules
Shared group DPO	Several entities with compatible governance and an accessible common function	Consolidated coordination across a group	May be overstretched, not appropriately accessible or incompatible across jurisdictions	Test each entity, local law, languages and resources
Non-statutory privacy adviser only	No formal DPO requirement and narrower project or advisory needs	Proportionate access to expertise	Must not be mistaken for statutory designation	Document why no DPO is required or intended
Project-only consultancy	Specific DPIA, audit, framework or transfer project	Defined deliverable and acceptance point	Does not necessarily provide retained statutory oversight	Verify whether a DPO is separately appointed

Cost comparison warning: An internal salary, external retainer and project fee are not directly comparable without assessing total capacity, continuity, legal duties, management time and operational responsibilities. The cheapest monthly option may have the greatest unpriced exposure if it lacks independent challenge or usable coverage.

6. International groups: separate the entities, laws and mandates

An enterprise may have a UK parent, EEA subsidiaries, a US processor, clinical trials in several countries and customers in jurisdictions without a local office. A single commercial contract does **not** automatically establish one legally sufficient DPO designation or satisfy territorial representative obligations everywhere.

Cross-border appointment and representative matrix

Situation	Initial assessment	Key caution
UK entity with processing in UK GDPR Article 37 categories	Determine UK DPO requirement, appointment and contact notification	UK statutory DPO duties still apply if appointment is outsourced
EU/EEA establishment with processing subject to EU GDPR	Assess EU GDPR Article 37 and relevant national provisions	UK-only DPO appointment does not automatically complete EU local requirements
Group wishes to use one DPO across UK and EEA entities	Consider duties under both regimes, accessibility, languages, resources, authority contact and local rules	Group-wide coverage is possible in some structures but must be demonstrably effective
UK organisation with no EU establishment offers goods/services to or monitors people in EU	Assess EU GDPR territorial scope and whether EU Article 27 representative appointment is required	EU representative is not the same as EU DPO; applicable exceptions require assessment
Non-UK organisation has relevant UK data-subject activity without UK establishment	Assess UK GDPR scope and potential UK Article 27 representative requirement	UK representative is not the UK statutory DPO role
Organisation transfers personal data internationally	Assess relevant UK/EU transfer rules and contractual safeguards	DPO designation and Article 27 representation are not transfer mechanisms
Multiple group entities share privacy staff and processors	Map controller/processor roles, entities, reporting lines and contracts	One global label does not override entity-by-entity accountability

The EU GDPR expressly permits one DPO for a group of undertakings if accessible from each establishment, while the EDPB's territorial-scope guidance distinguishes the Article 27 EU representative. It considers the EU representative function generally incompatible with acting as the same client's external DPO because of independence concerns. Apply a jurisdiction-specific conflict review rather than bundling the roles. [S2][S6][S7]

The UK regulator also distinguishes a UK representative obligation for certain organisations established outside the UK. The representative must be authorised in writing, with an assessment of exceptions. [S8]

Six questions for the multinational General Counsel

1. Which legal entity is the controller or processor for each material processing activity?
2. Which entities fall under UK GDPR, EU GDPR and any relevant national data protection laws?
3. For which entities is formal DPO designation compulsory, voluntary or not applicable?
4. If one DPO supports several entities, how will staff and individuals reach them and how will local supervisors be engaged?
5. Are UK or EU Article 27 representative appointments separately necessary, and who would provide them without conflicting with the DPO role?
6. Who owns the transfer assessment, applicable safeguards, operational compliance decisions and country-level legal advice?

7. Procurement RFP: 18 questions that separate a DPO appointment from a generic privacy subscription

Legal designation and independence

1. Which legal entities and jurisdictions are covered by the proposed DPO appointment?
2. Who will be the designated lead, who provides cover and what happens if that person leaves?
3. How do you establish independence and identify internal or external conflicts at appointment and during the engagement?
4. Can the DPO report to the highest management level and submit dissenting advice without contractual approval?
5. How are the DPO's statutory tasks protected if demand exceeds the routine service allowance?

Specialism and capacity

1. Which practitioners will actually deliver the service, and what sector and statutory DPO experience can be substantiated?
2. What availability, language coverage and continuity can be provided for our actual time zones and group entities?
3. How do you prioritise high-risk processing, complex DPIAs, sensitive health data and regulatory correspondence?
4. How will you involve the DPO early in projects, procurement, system changes and material incidents?

Operating evidence and governance

1. What does the first 30–90 days of mobilisation involve, subject to scoping, and what evidence would be produced? (Do not read this as a guaranteed delivery timetable.)
2. What is the normal board reporting and escalation mechanism, and how is advice documented?
3. How are outstanding findings, owner actions, risk acceptance and completion evidence recorded?
4. How are DPO monitoring and any provider-operated Privacy Office services independently challenged?

5. How will we publish DPO contact details and notify the relevant supervisory authority?

Commercial and security assurance

1. Which services are included in the retainer, separately scoped, or expressly excluded? Are statutory tasks unconditional?
2. What personnel or subcontractors can access information, where is it processed and what contractual protections apply?
3. How are conflicts, service deterioration, replacement, termination, records return and handover handled?
4. What specific client dependencies, capacity assumptions, response expectations and commercial change controls underlie the price?

Procurement rule: Require material answers and supporting documents, not only affirmative yes/no responses.

8. IG-Smart Enterprise DPO Service-Selection Matrix (100-point working tool)

Original proposed procurement worksheet. It ranks eligible provider proposals against your organisation's documented requirements; it does not certify a supplier, establish legal compliance or provide an independently validated market benchmark.

Step 1 — Apply four hard-stop qualification gates

A candidate is **not yet eligible for weighted scoring** if any of these checks fail and the deficiency is not remedied:

- **H1. Appointable mandate:** Can the engagement satisfy the required formal DPO appointment, scope and statutory duties where applicable?
- **H2. Genuine independence:** Is there a workable, documented solution to any material conflict of interests, with direct senior-management access?
- **H3. Effective resources:** Can the DPO actually perform the role with sufficient capacity, expertise, access and continuity for the organisation's risk?
- **H4. Jurisdiction and contact:** Is required coverage/territorial eligibility and accessible contact/regulatory liaison clearly provided, including separate handling of representative obligations?

Gate disposition: PASS / REMEDIABLE — obtain revised evidence and reassess / FAIL — exclude from formal DPO selection. An unknown answer is **not** a pass.

Step 2 — Score ten weighted criteria

Use the same documented evidence standard for every bidder. Rate each criterion from **0 to 4**:

- **0 — Absent:** no credible answer or material omission.
- **1 — Asserted:** broad claim with little verifiable detail.
- **2 — Partially evidenced:** workable outline, important material still missing.
- **3 — Evidenced:** specific roles, documents and workable contractual commitments.
- **4 — Strongly evidenced:** convincing, risk-proportionate arrangements verified through appropriate documents and discussion.

Weighted score = (rating ÷ 4) × criterion weight. Total possible = **100**. If evidence is missing, score the applicable criterion 0 rather than inventing assurances.

Criterion	Weight	What a strong answer demonstrates	Evidence to request	Rating 0–4	Weighted score
1. Legal and entity scope	12	Clear appointment type, entity/ jurisdiction analysis, statutory task completeness	Mandate, entity schedule, role specifications	—	—
2. Independence and conflicts	16	Direct senior access, separate decisions, conflict prevention and unfiltered challenge	Conflicts assessment, independence clauses	—	—
3. Practitioner competence	12	Confirmed named specialist expertise matched to the processing risks	Named CVs, relevant experience and references where authorised	—	—
4. Capacity and continuity	12	Realistic workload, responsiveness, cover and accessibility	Capacity/cover plan, response procedures	—	—
5. Board oversight and escalation	10	Timely senior reporting, challenge and documented risk acceptance	Sample report, escalation map	—	—
6. Day-to-day governance integration	10	Practical involvement in projects, monitoring and internal decision cycles	Operating cadence, example records	—	—
7. DPIA and incident advisory	8	Appropriate input on high-risk assessments and incident decisions without role confusion	DPIA workflow, incident advisory pathway	—	—
8. Contractual scope transparency	8	Non-optional statutory tasks, clear extra services, boundaries and exit arrangements	Statement of work, change-control and exit clauses	—	—
9. Information security and handling	6	Suitable controls for sensitive client information and appropriate subcontractors	Relevant security evidence and information-handling terms	—	—
10. Multijurisdictional fit	6	Realistic entity, language, supervisor and representative-role arrangements if applicable	Coverage matrix, local expertise plan	—	—

Criterion	Weight	What a strong answer demonstrates	Evidence to request	Rating 0–4	Weighted score
Total	100				___/100

Step 3 — Apply evidence confidence, not invented market thresholds

Before selection, separately document:

- **Mandatory appointment gates:** result and proof.
- **Evidence quality:** which ratings rely on commitments versus demonstrated working examples.
- **Red-flag exceptions:** unresolved conflicts, missing resources, inaccurate statutory claims, unverified service rights or poor access.
- **Value for money:** expected annual total cost, internal resources needed and separately priced projects — compared on like-for-like assumptions.
- **Management decision:** approved bidder, rejected alternatives, remaining conditions and accountable signatory.

There is **no universal pass score**. The buyer may define its own threshold before evaluating submissions, but an apparently high result cannot override a failed statutory safeguard or replace due diligence.

Illustrative example — why the lowest quote may lose

Fictional procurement scenario; the scores below are invented only to demonstrate the calculation and are not client evidence, market benchmarks or actual provider performance.

A HealthTech group compares four proposed arrangements. Provider A offers low-cost privacy helpdesk assistance but no board escalation and **fails H2**. Provider C offers experienced advisers but no workable group-coverage plan and **fails H4** unless remedied. Neither should be advanced solely on price. Providers B and D pass all four preliminary gates and can be scored.

Weighted selection illustration	Provider B	Provider D
Ratings in criterion order (1–10; each 0–4)	4, 4, 3, 4, 3, 3, 3, 4, 3, 2	3, 3, 4, 2, 4, 3, 4, 3, 3, 4
Independence criterion (weight 16)	$4 \div 4 \times 16 = 16$	$3 \div 4 \times 16 = 12$
Total weighted selection score	85.5/100	81/100
Next buyer action	Verify international-coverage limitations and overall commercial terms	Test capacity/continuity gaps and overall commercial terms

These illustrative numbers have **no statistical or evidential relationship to actual providers**. They demonstrate consistent application of the formula, not a regulatory pass mark. Procurement should document a material reason if it selects a lower-scored eligible bidder — for example, stronger contract terms or a substantially lower total cost with satisfactory required safeguards.

The lesson is not that the highest score always wins. It is that **procurement should not buy a statutory title based on price when the authority, independence or coverage behind that title is missing**.

9. Mobilisation: a defensible starting operating model

The first engagement phase should establish facts and routes for oversight, rather than claim to render an entire business compliant on appointment. A practical scoped mobilisation may include:

1. **Confirm designation and coverage** — entities, statutory rationale, appointed role and regulator communication.
2. **Protect mandate and access** — board sponsor, independence, conflicts, resources and confidential channels.
3. **Establish context** — key processing, systems, higher-risk projects, suppliers, international transfers and current data protection records.
4. **Set monitoring priorities** — review known material gaps, DPIA workflow, risk register and planned audit/assurance activity.
5. **Document operational ownership** — name internal and external owners for responses, complaints, records, incidents and remediation.
6. **Agree reporting and review triggers** — advice records, board escalation, management acceptance and material change notifications.

This is an illustrative delivery structure, not a guaranteed timeframe or pre-authorised contractual bundle. IG-Smart's approved delivery model is **Assess → Build → Manage → Assure → Improve**, adapted to the specific mandate while preserving DPO independence.

RACI-style responsibility snapshot

Key: A = accountable for business decision, R = responsible for performance, C = consulted/adviser/monitor, I = informed. Actual roles require tailoring.

Activity	Board / controller management	Operational Privacy Office	Independent DPO
Determine processing purposes and lawful basis	A	R / support as assigned	C, challenge
Approve funding and resource allocation	A	R / support	C, escalate inadequate resourcing
Compile DPIA and implement mitigations	A	R / delegated owner	C, advise and monitor
Independently monitor privacy compliance	Receives and responds to advice	Supplies records, executes actions	R for DPO monitoring function
Process access requests and rights workflows	A	R where assigned and resourced	C / monitor, unless separately scoped conflict-safe support
Assess and decide breach response	A	R / incident response team	C, advise, monitor and escalate
Issue board assurance or privacy risk acceptance	A	Supplies implementation evidence	C, independent findings
Maintain DPO contact and supervisory-authority liaison	Ensures publication/ communication	Administrative support	R for DPO contact and co-operation

RACI is a governance aid, not a reinterpretation of Article 39 responsibilities. An outsourced operational provider may undertake specific delegated tasks; this does not transfer the client's legal accountability.

10. A 16-point buyer readiness and contract checklist

Use this as an internal approval worksheet before signing a retained DPO contract.

Appointment and independence

- ☐ We have documented whether a formal DPO is required, voluntary or unnecessary, and for which entities.
- ☐ We have assessed our UK, EU/EEA and other jurisdictional obligations separately.
- ☐ We have identified the appointed DPO lead and credible cover arrangements.
- ☐ We have documented and mitigated independence and conflicts of interest.
- ☐ The DPO can access the highest management level without approval filtering.
- ☐ Statutory tasks cannot be omitted through package tiers or service-hour wording.

Operating readiness

- ☐ We have a named internal sponsor and operational decision owners.
- ☐ We have granted appropriate access to relevant personnel, records and processing activities.
- ☐ We have agreed regulator and data-subject contact arrangements and will publish/communicate required contact details.
- ☐ DPIA advice, monitoring, incident support and escalation routes are clearly described.
- ☐ We can record advice, exceptions, decisions and action follow-up.
- ☐ We have addressed continuity, capacity, specialist support and material-change triggers.

Commercial and information governance

- ☐ The DPO appointment, governance outputs and extra operational support have separate scope definitions.
- ☐ We have assessed information security, confidentiality, subcontractor arrangements and data processing roles.
- ☐ We have checked exit arrangements, evidence handover and responsibility for ongoing cases.
- ☐ We have evaluated selection using hard-stop safeguards and a documented, comparable scoring matrix.

11. One-page executive decision briefing – copyable template

Decision requested: Approve / conditionally approve / defer an outsourced DPO and associated Privacy Office operating model.

Field	Board or procurement entry
Entity / group scope	[Legal entities and locations]
Appointment basis	[UK GDPR Article 37 mandatory / voluntary / separate advisory role; EU/local law separately assessed]
Business trigger	[Vacancy, rapid growth, higher-risk processing, regulator scrutiny, procurement requirement]
Recommended model	[External DPO / hybrid DPO + internal Privacy Office / internal DPO / adviser only]
DPO independence	[Conflicts findings, reporting line and mitigation]
Coverage and resource	[Named lead, availability, entities and specialist back-up]

Field	Board or procurement entry
Statutory task support	[Complete / conditions to resolve]
Operational split	[DPO oversight / internal ownership / separately contracted support]
International issues	[EU DPO/Article 27, UK Article 27, local laws and transfer issues, where relevant]
Procurement assessment	[Hard-stop gate outcome; selection score and evidence limitations]
Total commercial commitment	[Provider costs, exclusions, separately scoped projects and internal resource needs]
Key unresolved risks	[Risk, owner, remedy and due date]
Proposed decision	[Approve / approve subject to conditions / defer]
Accountable sign-off	[Role, name and decision date]

Executive decision standard: Do not approve on the basis of a favourable fee or a high numeric matrix score if the proposed arrangement cannot demonstrate the required legal position, independent access or sufficient resources.

12. What should a well-run outsourced DPO relationship deliver?

A meaningful measure of value is not the volume of generic policy documents produced. Boards should expect a clear line of sight between material processing risk, professional advice, implementation ownership and recorded decisions.

Useful **operating indicators** (not regulatory compliance scores) include:

Indicator	What it tells management	Warning about interpretation
High-risk projects involving DPO input before major decisions	Whether the DPO is engaged in time	A count alone does not show advice quality
Significant DPIAs with recorded advice and outcomes	Whether independent advice affects governance	DPO opinion is not a substitute for the controller's decision
Material findings with owner, decision and evidence of follow-up	Whether issues are resolved or knowingly accepted	An unclosed item can reflect justified prioritisation or weak delivery
Board access and escalations documented	Whether independence works in practice	High escalation volume is not intrinsically good or bad
Entity/jurisdiction coverage kept current	Whether shared DPO arrangements match actual operations	Must be reviewed after acquisitions or geographic expansion
Contact, complaint and supervisory-authority paths exercised	Whether the designated function is reachable	A successful contact test is not proof of substantive compliance

A particularly relevant operational development in 2026 is the UK requirement for organisations to have a process for handling data protection complaints, including acknowledgement within the applicable 30-day rule and investigation without undue delay. **This is an organisational obligation, not a new power automatically transferred to the DPO.** [S9]

13. Common buying mistakes and the better question

Mistake	Better question
"We are buying twenty DPO hours, so anything else is extra."	Can this capacity actually support every statutory DPO function for our processing profile?
"Our cybersecurity consultant can also be the DPO."	Do the consultant's duties determine processing purposes/means or undermine independent privacy challenge?
"We want one global DPO and representative."	Which entity-specific DPO and Article 27 roles apply, and which roles must be separated?
"The provider will make us UK GDPR-compliant."	What decisions and controls will our organisation still own, and what evidence will the DPO monitor?
"We only need someone to draft policies."	Do we need a formal DPO, or is a defined-scope privacy project more appropriate?
"The provider has a recognised accreditation, so no further checks."	Is each claimed certification relevant, accurate, current and actually held by the contracting entity?
"The DPO will approve every DPIA and all our risks."	Who signs the DPIA, accepts risk and implements mitigation, and how is DPO advice recorded?
"One low-cost contract covers every country."	Which legal entities, languages, authorities, risk profiles and other legal duties are demonstrably covered?

14. Frequently asked enterprise buyer questions

Can we outsource a UK statutory DPO appointment?

Yes. UK GDPR Article 37 allows DPO tasks to be fulfilled through a service contract. The external DPO must have the competence, independence, access, resources and statutory functions required of the position. The client organisation retains responsibility for its compliance decisions. [S1][S2]

Is appointing a DPO mandatory for every business?

No. It is required for specified types of public body and processing activity, with possible additional legal obligations. Assess each organisation's circumstances. A voluntary formal appointment carries the same DPO-role safeguards. [S1]

Is a DPO the same as a Privacy Office?

No. The DPO's statutory purpose is independent advice, monitoring and contact. A Privacy Office may perform programme management and delegated operational work. One provider can potentially support both, but responsibilities and conflicts must be assessed and documented.

Can our external DPO write policies, administer subject access requests and conduct audits?

Some operational services may be contractually supplied in addition to the statutory appointment. The key is whether the DPO can still independently advise on and monitor the relevant work without an unacceptable conflict. A provider's ability to perform a task does not mean it is included in the DPO engagement.

Can one DPO serve several group companies?

Potentially, yes, subject to effective accessibility, expertise, resources and the relevant UK/EU/local legal requirements. A shared appointment is not automatically adequate for every entity or jurisdiction. [S1][S2]

Does our UK DPO also act as an EU Article 27 representative?

No such appointment follows automatically. Article 27 representation is a separate role and obligation. Under EDPB guidance, combining the EU representative function with the same client's external DPO raises an independence incompatibility concern. Assess each mandate independently. [S6][S7]

Does using a DPO guarantee that we will pass an audit or avoid regulatory action?

No. A DPO helps an organisation make better-informed decisions and monitor compliance, but cannot guarantee its legal compliance, regulatory outcome or audit result. Management remains accountable for decisions and implementation.

What should determine the fee?

The actual appointment and coverage scope, processing risk, entity count, complexity, necessary capacity, reporting requirements, required access, additional operational services and continuity. Demand itemised assumptions rather than comparing headline retainers alone.

What if the DPO's recommendation conflicts with a commercial objective?

The DPO must be able to provide advice free from instructions about its conclusion and escalate to senior management. Management should document its decision and reasons, particularly where it does not follow material advice. [S1][S5]

What happens when the appointed practitioner leaves?

Continuity should be contractually planned: temporary cover, named replacement criteria, regulator/contact updates where needed, advice records, open issues and an orderly handover. The organisation must avoid leaving a required appointment ineffective.

15. The next step: buy an accountable mandate, not a label

The strongest outsourced DPO procurement begins with the organisation's real processing, legal duties and decision structures. From there, the buyer can choose a defensible statutory appointment, a properly resourced Privacy Office, a hybrid arrangement or a narrower project — and make the contract explicit about how they differ.

For organisations that require an independent retained DPO: Explore IG-Smart's [DPO as a Service](#) to discuss appointment scope, senior-management access, governance cadence and contractual boundaries. **Talk to a Senior Practitioner** using the service's approved enquiry pathway.

If a formal DPO is not the immediate requirement: Consider [UK GDPR Consultancy](#) for defined privacy advisory needs or [International Data Transfer Assurance](#) where cross-border transfer assessment is the specific issue. These are distinct engagements and require appropriate scoping.

What to prepare for a useful first conversation: a group/entity map; a brief description of significant data processing; existing DPO arrangements; major privacy risks; required jurisdictions; and any procurement, audit or leadership deadlines. Do not send sensitive client or patient records through an ordinary enquiry form.

Primary source register and verification notes

Source labels distinguish official legislation and regulator guidance from the original IG-Smart working models in this guide. Check the current law and guidance for the date and scope of your decision.

Regulatory currency note — October 2026: The Data (Use and Access) Act 2025 amended UK data protection law, with the ICO reporting its data protection provisions in force as of June 2026. Some underlying ICO guidance was still being updated. Check the provisions and guidance current when making an appointment decision. A UK DPO is not automatically an EU DPO, Article 27 representative or unrestricted international legal adviser. [S1][S9]

Sources

- [S1] ICO — Data protection officers (UK GDPR accountability guidance). <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-officers/>
- [S2] EU GDPR — Articles 37, 38 and 39 (EUR-Lex). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [S3] ICO — Controllers and processors. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/>
- [S4] ICO — How do we do a DPIA? <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/>
- [S5] EDPB — Data Protection Officer guidance for organisations. https://www.edpb.europa.eu/sme/be-compliant/data-protection-officer_en
- [S6] EDPB — Final Guidelines 3/2018 on the territorial scope of the GDPR, Article 3. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
- [S7] EU GDPR — Articles 3 and 27 (EUR-Lex). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [S8] ICO - UK representatives. <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/uk-representatives/>
- [S9] ICO — What does the Data (Use and Access) Act 2025 mean for organisations?; How to deal with data protection complaints <https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-what-does-it-mean-for-organisations/>
- [S10] ICO — Add a Data Protection Officer. <https://ico.org.uk/for-organisations/data-protection-fee/your-data-protection-officer-is/>
- [S11] ICO - How to deal with data protection complaints. <https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/>