CLOUDSWITCHED

FREE RESOURCE — COMPLIANCE CHECKLIST

GDPR Compliance Checklist

Assess your organisation against ten domains of the UK GDPR and Data Protection Act 2018 — lawful basis, transparency, consent, individual rights, records of processing, security, breach response, processors, international transfers and governance. Tick every control that is fully in place, score each section and surface the gaps before the ICO does.

10	70+	/10	Fillable
COMPLIANCE DOMAINS	CONTROLS TO VERIFY	SCORE EACH SECTION	TICK & TYPE IN ANY VIEWER

UK GDPR · DPA 2018 · ICO READY · ACCOUNTABILITY

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this checklist

Work through each of the ten domains with your data protection lead, DPO or managed IT provider. Tick every control that is **fully in place** — documented, operating and evidenced today, not "in progress" or "on the roadmap". Then award each domain a score out of 10 based on how many controls you can confidently tick.

A score **below 6 in any domain** is a compliance gap that should be closed before it becomes a complaint, a data subject access request you cannot answer, or an ICO enquiry. Use the action page at the back to capture your top three priorities. This is an **interactive PDF** — tick the boxes and type your scores and notes directly in any modern PDF viewer.

WHAT THIS CHECKLIST IS

A practical accountability self-assessment for UK SMEs against the UK GDPR and the Data Protection Act 2018. It covers the day-to-day controls a competent data protection function should have running — lawful basis, privacy information, consent, individual rights, records of processing, security, breach response, processor contracts, international transfers and governance. It is not a substitute for legal advice or a formal ICO audit, but it is a fast way to surface the gaps those will pick up.

SCORING GUIDANCE

Award one point per control where you hold evidence it is in place — a policy, a register, a contract clause, a configuration, a training record. Half measures do not score. Round each domain to the nearest whole number out of 10 and carry it forward to the summary on page 12.

The ten domains

- **01 Lawful Basis & Processing Principles** — Article 6 basis, purpose limitation, minimisation.
- **02 Transparency & Privacy Information** — privacy notices, fair processing, cookies.
- **03 Consent Management** — valid consent, withdrawal, special category data.
- **04 Individual Rights & DSARs** — access, erasure, portability, one-month deadline.
- **05 Records of Processing & Accountability** — ROPA, retention, data mapping.
- **06 Data Security & Technical Controls** — encryption, access, MFA, pseudonymisation.
- **07 Personal Data Breach Management** — detection, 72-hour ICO reporting, log.
- **08 Processors, Contracts & Third Parties** — Article 28 contracts, due diligence.
- **09 International Data Transfers** — adequacy, SCCs, IDTA, transfer risk.
- **10 Governance, DPO & Training** — ownership, DPO, DPIAs, staff awareness.

01

Lawful Basis & Processing Principles

Every act of processing personal data needs a lawful basis under Article 6, and must respect the core principles. Check that you can name the basis for each processing activity and that you only hold what you genuinely need.

- ☐ A **lawful basis under Article 6** is identified and documented for every processing activity *(consent, contract, legal obligation, vital interests, public task or legitimate interests)*.
- ☐ Where **legitimate interests** is relied upon, a **Legitimate Interests Assessment (LIA)** has been completed and is on file.
- ☐ Personal data is processed only for the **specified, explicit purposes** it was collected for — no incompatible re-use without a new basis.
- ☐ **Data minimisation** is applied — you collect only the data that is adequate, relevant and necessary for the purpose.
- ☐ Personal data is kept **accurate and up to date**, with a process to correct or erase inaccurate records.
- ☐ **Retention periods** are defined for each data category and data is deleted or anonymised when no longer needed.
- ☐ A **lawful basis for any special category data** (Article 9) or criminal offence data (Article 10) is separately identified and documented.

WHAT GOOD LOOKS LIKE

You can point to a single register that names, for each processing activity, the purpose, the Article 6 basis and (where relevant) the Article 9 condition. If anyone asks “why do we hold this?” the answer is written down, not improvised.

SECTION 01 SCORE _____ / **10** *Aim for 8+. Below 6 = lawful basis gap.*

02

Transparency & Privacy Information

People have a right to know what you do with their data. Check that your privacy information is accurate, accessible and provided at the point of collection — not buried or out of date.

- ☐ A **privacy notice** is published and covers identity of the controller, purposes, lawful basis, retention, rights and how to complain to the ICO.
- ☐ Privacy information is provided **at the point data is collected** — on forms, sign-ups and contracts, not only on a hidden web page.
- ☐ The privacy notice is written in **clear, plain language** and is easy to find from every page that collects data.
- ☐ Where data is obtained **indirectly** (not from the individual), the source and the privacy information are provided within one month.
- ☐ A compliant **cookie consent banner** is in place — non-essential cookies are blocked until the user opts in *(PECR compliant)*.
- ☐ Privacy notices are **reviewed and version-controlled**, and updated whenever processing purposes change.
- ☐ Marketing communications include a **clear and working unsubscribe** mechanism in every message.

COOKIES ARE ENFORCED SEPARATELY

Cookie consent falls under PECR as well as UK GDPR. A pre-ticked box or “by using this site you agree” banner is not valid consent. Non-essential and analytics cookies must wait for an affirmative opt-in — the ICO has issued guidance and is actively reviewing UK websites.

SECTION 02 SCORE _____ / **10** *Aim for 8+. Below 6 = transparency gap.*

03

Consent Management

Where you rely on consent, it must be freely given, specific, informed and unambiguous — and as easy to withdraw as it was to give. Check that your consent records would survive scrutiny.

- ☐ Consent is captured through a **clear affirmative action** — no pre-ticked boxes, no consent bundled into terms and conditions.
- ☐ Consent requests are **granular** — separate opt-ins for separate purposes (e.g. email marketing vs. SMS vs. profiling).
- ☐ **Records of consent** are kept showing who consented, when, how and to exactly what they were told.
- ☐ Individuals can **withdraw consent at any time**, and withdrawal is as easy as giving it — with the route clearly signposted.
- ☐ **Explicit consent** is obtained where required for special category data or certain automated decision-making.
- ☐ Consent is **refreshed or reviewed** periodically, and stale or unverifiable consent is not relied upon.
- ☐ **Children's data** has appropriate age verification and parental consent where an online service is offered to under-13s.

CONSENT IS THE HARDEST BASIS TO RELY ON

If you cannot evidence valid, granular, withdrawable consent, you have no lawful basis and the processing is unlawful. Where another Article 6 basis fits better (contract or legitimate interests), use it — do not default to consent for everything.

SECTION 03 SCORE _____ / **10** *Aim for 8+. Below 6 = consent is unreliable.*

04

Individual Rights & DSARs

Individuals have eight rights under the UK GDPR. Check that you can recognise, log and fulfil a request — especially a data subject access request — within the statutory one-month deadline.

- ☐ Staff can **recognise a data subject request** in any form (email, phone, letter, social media) and know who to forward it to.
- ☐ A **documented process** exists to handle **data subject access requests (DSARs)** within one month, extendable by two months for complex cases.
- ☐ You can locate and export **all personal data held on an individual** across systems, email, files and backups.
- ☐ Processes exist to fulfil the rights to **rectification, erasure ('right to be forgotten') and restriction** of processing.
- ☐ The right to **data portability** can be met — relevant data provided in a structured, commonly used, machine-readable format.
- ☐ Individuals can **object to processing** (including direct marketing) and there is a process to action it promptly.
- ☐ Safeguards exist for **automated decision-making and profiling**, including the right to human review where it has legal or similar effects.
- ☐ Requests are **logged** with dates, actions and outcomes to evidence compliance with the deadline.

THE ONE-MONTH CLOCK STARTS ON RECEIPT

A DSAR does not need to mention “GDPR” or go to a particular inbox. The clock starts the day any member of staff receives it. Front-line training and a single logged intake route are the difference between a calm response and a missed statutory deadline.

SECTION 04 SCORE _____ / **10** *Aim for 8+. Below 6 = you risk missing deadlines.*

05

Records of Processing & Accountability

Accountability means being able to demonstrate compliance, not just claim it. Check that you maintain records of processing and can show the ICO how personal data flows through your organisation.

- ☐ A **Record of Processing Activities (ROPA)** is maintained under Article 30, covering purposes, categories, recipients, transfers and retention.
- ☐ A **data inventory / data map** records what personal data you hold, where it lives and which systems process it.
- ☐ A **retention schedule** is documented and enforced, with routine deletion or anonymisation of expired data.
- ☐ **Data protection policies** (data protection, retention, acceptable use, BYOD) are documented, approved and accessible to staff.
- ☐ Your organisation is **registered with the ICO** and the annual data protection fee is paid and current.
- ☐ Compliance is **reviewed at least annually**, with findings reported to senior management or the board.
- ☐ Decisions and assessments (LIAs, DPIAs, balancing tests) are **documented and retained** as evidence of accountability.

ACCOUNTABILITY IS THE PRINCIPLE THAT TIES IT TOGETHER

The ICO does not just ask whether you comply — it asks you to demonstrate it. A current ROPA, a retention schedule and a file of documented decisions are the artefacts that turn “we take privacy seriously” into evidence.

SECTION 05 SCORE _____ / **10** *Aim for 8+. Below 6 = accountability gap.*

06

Data Security & Technical Controls

Article 32 requires appropriate technical and organisational measures to keep personal data secure. Check that the controls protecting the data are proportionate to the risk and actually in operation.

- ☐ Personal data is **encrypted** at rest and in transit — device encryption, TLS, and encrypted backups.
- ☐ **Access to personal data is role-based** and limited to staff who need it, with access reviewed regularly.
- ☐ **Multi-factor authentication (MFA)** is enforced on email, cloud services and any system holding personal data.
- ☐ **Pseudonymisation or anonymisation** is used where it reduces risk without defeating the purpose.
- ☐ **Endpoint protection, patching and secure configuration** are maintained across all devices that process personal data.
- ☐ **Backups** of personal data are taken, encrypted and test-restored, supporting the integrity and availability principle.
- ☐ **Physical security** protects paper records and on-premise systems — locked storage, clear-desk, controlled access.
- ☐ Security measures are **reviewed and tested** (e.g. vulnerability scans, Cyber Essentials) and improved over time.

SECURITY IS JUDGED ON APPROPRIATENESS, NOT PERFECTION

Article 32 asks for measures appropriate to the risk and the state of the art. A small charity and a fintech are held to different standards — but both must be able to show they assessed the risk and acted on it. Undocumented controls are hard to defend after a breach.

SECTION 06 SCORE _____ / **10** *Aim for 9+. Below 6 = serious security risk.*

07

Personal Data Breach Management

A personal data breach must be detected, contained and — where it is likely to risk people's rights — reported to the ICO within 72 hours. Check that you could meet that deadline under pressure.

- ☐ A **documented breach response plan** defines roles, containment steps, assessment and escalation.
- ☐ Staff know **how to recognise and report a suspected breach** immediately, to a named owner or inbox.
- ☐ A process exists to **assess the risk to individuals** and decide whether ICO notification within 72 hours is required.
- ☐ A process exists to **notify affected individuals without undue delay** where the breach is likely to result in a high risk to them.
- ☐ A **breach log / register** records all incidents — including those not reported — with facts, effects and remedial action.
- ☐ Breach scenarios are **rehearsed or tabletop-tested** so the 72-hour clock does not catch the team unprepared.
- ☐ **Lessons learned** from incidents and near-misses feed back into security controls and training.

72 HOURS IS FROM AWARENESS, NOT FROM CERTAINTY

The clock starts when you become aware a breach has likely occurred — not when the investigation is finished. You can submit an initial ICO report and follow up with detail. Failing to report a reportable breach is itself an infringement.

SECTION 07 SCORE _____ / **10** *Aim for 8+. Below 6 = you cannot meet 72 hours.*

08

Processors, Contracts & Third Parties

When others process personal data on your behalf, you remain accountable. Check that every processor is under a compliant Article 28 contract and has been through basic due diligence.

- ☐ All **processors and sub-processors** are identified and listed *(cloud, payroll, marketing, IT support, SaaS vendors)*.
- ☐ A **written contract meeting Article 28** is in place with every processor, setting out subject matter, duration, purpose and obligations.
- ☐ **Due diligence** is performed on processors' security and compliance before sharing personal data with them.
- ☐ Contracts require processors to **assist with breaches, DSARs and audits**, and to delete or return data at the end of the contract.
- ☐ **Sub-processors** are only engaged with your authorisation and under equivalent contractual terms.
- ☐ Where you are a **joint controller**, a documented arrangement sets out respective responsibilities.
- ☐ Third-party data sharing is governed by a **data sharing agreement** and a clear lawful basis.

YOU STAY ON THE HOOK FOR YOUR PROCESSORS

Outsourcing the processing does not outsource the accountability. If your payroll provider or marketing agency suffers a breach of your data, it is still your incident to assess and, where required, report. A signed Article 28 contract and basic due diligence are the minimum defence.

SECTION 08 SCORE _____ / **10** *Aim for 8+. Below 6 = processor exposure.*

09

International Data Transfers

Transferring personal data outside the UK needs a valid transfer mechanism. Check that every flow of data abroad — including via cloud services — is covered and risk-assessed.

- ☐ All **transfers of personal data outside the UK** are identified, including those via cloud hosting and SaaS providers.
- ☐ Each transfer relies on a **valid mechanism** — UK adequacy regulations, the **IDTA**, or the **UK Addendum to the EU SCCs**.
- ☐ A **Transfer Risk Assessment (TRA)** is completed where required, considering the laws of the destination country.
- ☐ **Supplementary measures** (such as encryption) are applied where the destination's protections are inadequate.
- ☐ The **data hosting locations** of your key cloud providers are known and documented.
- ☐ **Onward transfers** by processors to third countries are controlled and contractually restricted.
- ☐ Transfer mechanisms are **reviewed** when adequacy decisions, vendors or regulations change.

"IT'S IN THE CLOUD" IS A TRANSFER QUESTION

Many everyday SaaS tools store or replicate data in the US or elsewhere. Each is an international transfer that needs a mechanism — usually the IDTA or the UK Addendum to the EU SCCs, plus a transfer risk assessment. Map where your data actually lives before you assume you are covered.

SECTION 09 SCORE _____ / **10** *Aim for 8+. Below 6 = transfer exposure.*

10

Governance, DPO & Training

Data protection needs an owner, a culture and a way of building privacy into new projects. Check that responsibility is clear, staff are trained and DPIAs happen before high-risk processing begins.

- ☐ **Clear responsibility** for data protection is assigned — a **Data Protection Officer (DPO)** where required, or a named accountable lead.
- ☐ All staff receive **data protection training** at induction and at least annually, with completion recorded.
- ☐ **Data Protection by Design and by Default** is embedded — privacy is considered at the start of new projects and systems.
- ☐ **Data Protection Impact Assessments (DPIAs)** are conducted before high-risk processing, with the ICO consulted where residual risk is high.
- ☐ Senior management or the board receive **regular reporting** on data protection risk and compliance.
- ☐ A **complaints handling process** exists for individuals, signposting their right to complain to the ICO.
- ☐ Data protection performance is **reviewed and improved** — audits, metrics and corrective actions are tracked.

PRIVACY BY DESIGN IS THE CHEAPEST CONTROL YOU HAVE

Fixing a privacy problem after launch is expensive and visible; designing it out at the requirements stage is almost free. A short DPIA at the start of any new system or data use is the single highest-leverage governance habit a small organisation can build.

SECTION 10 SCORE _____ / **10**

Aim for 8+. Below 6 = no clear ownership.

Σ

Compliance score summary

Transfer the score for each domain into the table. Set a priority (H/M/L) based on the gap to target. Anything below 6 is a candidate for the top-3 actions on the next page.

#	COMPLIANCE DOMAIN	SCORE / 10	PRIORITY
01	Lawful Basis & Processing Principles	_____ / 10	☐ H ☐ M ☐ L
02	Transparency & Privacy Information	_____ / 10	☐ H ☐ M ☐ L
03	Consent Management	_____ / 10	☐ H ☐ M ☐ L
04	Individual Rights & DSARs	_____ / 10	☐ H ☐ M ☐ L
05	Records of Processing & Accountability	_____ / 10	☐ H ☐ M ☐ L
06	Data Security & Technical Controls	_____ / 10	☐ H ☐ M ☐ L
07	Personal Data Breach Management	_____ / 10	☐ H ☐ M ☐ L
08	Processors, Contracts & Third Parties	_____ / 10	☐ H ☐ M ☐ L
09	International Data Transfers	_____ / 10	☐ H ☐ M ☐ L
10	Governance, DPO & Training	_____ / 10	☐ H ☐ M ☐ L
Σ	**TOTAL SCORE**	_____ / 100	—

¶

Interpretation & priority actions

Translate your total score into a risk band, then commit to a small number of next steps. The goal is one page of decisions, not a wish list.

Score interpretation

80–100	**Strong compliance posture.** Accountability is evidenced — focus on continuous review and emerging risks.
60–79	**Good foundation, gaps exist.** Prioritise any domain scoring below 6 with named owners and deadlines.
Below 60	**Significant exposure.** Seek a formal data protection review without delay.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

_____

ASSESSMENT COMPLETED BY _____

DATE _____

NEXT REVIEW DUE _____

Need help closing the gaps?

Cloudswitched helps UK SMEs operationalise GDPR — ROPA, retention, DSAR and breach processes, processor contracts and training, with fixed-price remediation.

info@cloudswitched.com

cloudswitched.com/services/compliance

CLOUDSWITCHED

IT, SECURITY & COMPLIANCE SERVICES

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom