CLOUDSWITCHED

FREE RESOURCE — DATA CLASSIFICATION TEMPLATE

Data Classification Template

A practical framework to classify the data you hold by sensitivity, apply the right protection and access controls, and keep an audit-ready record. Aligned with UK GDPR Article 30, NCSC guidance and Cyber Essentials — the evidence regulators, insurers and certification bodies expect to see.

4	UK GDPR	25+	Fillable
CLASSIFICATION TIERS	ARTICLE 30 ALIGNED	HANDLING RULES PER TIER	TICK & TYPE IN ANY VIEWER

UK GDPR ALIGNED · CYBER ESSENTIALS · ARTICLE 30 RECORD · AUDIT-READY

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

01

Why classify data & how to use this template

Not all data is equal. The marketing brochure on your website needs no protection at all; the employee payroll spreadsheet on a finance laptop needs encryption, named access, an audit trail and a documented retention period. **Data classification** is the discipline of deciding which data sits in which category and then applying the right controls to each — no more, no less. Over-protecting everything is expensive and slows the business; under-protecting sensitive data is what gets you fined, sued and on the front page.

WHAT THIS TEMPLATE IS FOR

A practical, four-tier classification scheme aligned with UK GDPR, NCSC guidance and Cyber Essentials. Use it to (1) agree your tier definitions, (2) inventory the data you actually hold and assign each asset a tier, (3) record the protection controls each tier requires, and (4) maintain the Article 30 record of personal-data processing the ICO can request at any time. The whole document is **fillable** — tick boxes and type into the lines directly in any modern PDF viewer.

CLASSIFICATION IS A BUSINESS DECISION — NOT JUST IT

Tier definitions should be approved by an executive sponsor (typically the COO, CFO or DPO) and reviewed annually. IT enforces the controls, but only the business can decide what counts as "confidential" versus "restricted" for *your* organisation. Get sign-off on the scheme before you start tagging data — retro-fitting a tier change across thousands of files is painful.

The six sections of this template

- **01 Why & how to use** — the page you are on now: principles and walk-through.
- **02 Classification scheme** — the four tiers (Public / Internal / Confidential / Restricted), criteria for each, and your handling rules.
- **03 Data inventory** — every data asset you hold, its tier, where it lives, who owns it, and how long you keep it.
- **04 Protection controls reference** — the encryption, access, backup, sharing and disposal controls expected for each tier.
- **05 GDPR Article 30 register** — the personal-data processing record UK GDPR requires you to keep up to date.
- **06 Sign-off & review schedule** — named approver, date, next review trigger.

02

Classification scheme — 1 of 2

Tick the criteria that define each tier for *your* organisation, then write the specific handling rule you will apply (encryption, access, retention, disposal). Default examples are listed in section 04. Once approved, every data asset on the inventory must be tagged to exactly one of these four tiers. The first two tiers — **Public** and **Internal** — are covered below; the higher-sensitivity tiers continue on the next page.

LEVEL 1 Public

Information intended for unrestricted external disclosure. No harm if shared widely.

CRITERIA (TICK ALL THAT APPLY)

- ☐ Already published or approved for public release.
- ☐ No commercial, personal or regulatory sensitivity.
- ☐ Loss or disclosure causes no reputational or financial harm.

HANDLING RULES

Encryption	_____	**Access**	_____
Retention	_____	**Disposal**	_____

LEVEL 2 Internal

Routine business information not for external release. Default tier for most operational data.

CRITERIA (TICK ALL THAT APPLY)

- ☐ Intended for staff and contractors under NDA only.
- ☐ Disclosure would cause minor reputational or operational impact.
- ☐ No personal data and no regulator interest.

HANDLING RULES

Encryption	_____	**Access**	_____
Retention	_____	**Disposal**	_____

02

Classification scheme — 2 of 2

The two higher-sensitivity tiers. **Confidential** covers most personal data and commercially sensitive material; **Restricted** is reserved for special-category data, payment-card data, and anything under legal hold. Tier rules here should be approved at director level and reviewed at least annually.

LEVEL 3 Confidential

Sensitive business, commercial or personal data. Restricted to named individuals or roles on a need-to-know basis.

CRITERIA (TICK ALL THAT APPLY)

- ☐ Contains personal data (UK GDPR) or commercially sensitive information.
- ☐ Disclosure would cause material financial, legal or reputational harm.
- ☐ Covered by a contract, DPA or regulator-set retention rule.

HANDLING RULES

Encryption		**Access**	
Retention		**Disposal**	

LEVEL 4 Restricted

Highly sensitive data with legal or regulatory implications. Special-category personal data, payment-card data, legal hold, M&A.

CRITERIA (TICK ALL THAT APPLY)

- ☐ Special-category personal data (health, biometric), criminal-offence data, or PCI cardholder data.
- ☐ Disclosure would trigger ICO 72-hour notification, regulator action or contractual penalty.
- ☐ Subject to legal hold, court order or formal investigation.

HANDLING RULES

Encryption		**Access**	
Retention		**Disposal**	

03

Data inventory

List every data asset the organisation holds — databases, file shares, mailboxes, paper records, SaaS tenants. Assign each to one of the four tiers from section 02, record its location, owner and retention. This inventory is the foundation for everything downstream: encryption decisions, DLP rules, backup tiers, the GDPR Article 30 register and your Cyber Essentials evidence pack.

DATA ASSET	TIER	LOCATION / SYSTEM	FORMAT	OWNER	RETENTION	PII Y/N

EXAMPLES TO PROMPT THE INVENTORY

Customer CRM database · employee HR records · payroll · financial accounts · sales pipeline · tender responses · supplier contracts · marketing mailing list · CCTV footage · door-access logs · backups · archived email · product roadmap · source code · project files · paper records in the office · mobile devices · SaaS tenants (M365, Salesforce, Xero, etc.).

PII COLUMN TRIGGERS THE ARTICLE 30 REGISTER

Any row with **PII = Y** must also appear on the GDPR personal-data register in section 05. The two records must agree — an asset on this inventory but missing from the Article 30 register is the kind of gap the ICO singles out in enforcement notices.

04

Protection controls by classification

This is the reference baseline. For each control area, the table shows the minimum expected treatment for data at each tier. Your tier-specific rules on page 02 should align with or exceed these defaults — never weaken them. Treat any gap between this baseline and your actual environment as a candidate finding for the risk register.

CONTROL AREA	PUBLIC	INTERNAL	CONFIDENTIAL	RESTRICTED
Encryption at rest	Optional	Recommended	Required (AES-128+)	Required (AES-256 + KMS)
Encryption in transit	Optional	Recommended	Required (TLS 1.2+)	Required (TLS 1.3, mTLS where possible)
Access control	None	AD / Entra ID group	Named individuals, role-based	Named + MFA + audit log + JIT elevation
DLP policies	None	Basic (label-driven)	Email + endpoint DLP	Full DLP + sensitivity labels + watermarking
Backup	Standard	Standard	Encrypted backup, geo-redundant	Encrypted + immutable + 3-2-1-1-0
External sharing	Allowed	Link (internal only)	Approved recipients only, DPA in force	Prohibited without director approval
Mobile / removable media	Allowed	Allowed (encrypted)	Restricted, MDM-enforced	Prohibited unless ICO/director signed off
Logging & monitoring	None required	Standard system logs	Access logs reviewed monthly	Full audit log, SIEM alerts, 12mo+ retention
Retention	Until superseded	3 years (default)	Per contract / regulation	Per regulation + legal hold capability
Disposal	No requirement	Delete	Secure delete + log entry	Secure delete + certificate of destruction

HOW TO USE THIS REFERENCE

Walk every data asset on the inventory in section 03 against this table. Where the actual control is weaker than the tier requires, raise it as an action with a named owner. Where it is stronger, leave it — over-protection is fine, under-protection is the finding.

05

GDPR Article 30 personal-data register

UK GDPR Article 30 requires most controllers (and all controllers processing special-category data, or with 250+ employees) to keep a written record of personal-data processing activities. This page is your record. Every row on the data inventory in section 03 with **PII = Y** must have a matching entry here. Review and update at least annually, and after any new system, supplier or processing purpose goes live.

PROCESSING ACTIVITY	LAWFUL BASIS	DATA SUBJECTS	PURPOSE	RECIPIENTS	RETENTION	INTL. TRANSFER

LAWFUL-BASIS QUICK REFERENCE

Pick one per row from Article 6: **Consent** · **Contract** · **Legal obligation** · **Vital interests** · **Public task** · **Legitimate interest**. Special-category data (Article 9) needs a second condition — commonly explicit consent, employment law, or substantial public interest. Get the basis right at this row level; it dictates every downstream rights handling.

ARTICLE 30 IS A LEGAL REQUIREMENT — NOT A NICE-TO-HAVE

The ICO can request to see this register at any time. Missing or out-of-date Article 30 records are repeatedly cited in enforcement notices and monetary penalties. Update this page when a new processing activity goes live, a supplier changes, or a retention rule shifts — not once a year as a tidy-up exercise.

06

Sign-off & review schedule

A classification scheme is only enforceable when an executive sponsor has approved it and a date is in the calendar for the next review. Without those two things, this is a draft — not the policy the ICO, your insurer or your auditor expect to see.

Organisation & preparer

Organisation name _____

Prepared by (name & role) _____

Date prepared _____

Document version _____

Review schedule

Next full review (12 months) _____

Trigger events for early review _____

Calendar reminder set (Y/N) _____

Notes & outstanding actions

_____

_____

_____

PREPARED BY _____

DATE _____

APPROVED BY (DIRECTOR / DPO) _____

CLOUDSWITCHED

DATA CLASSIFICATION & COMPLIANCE

info@cloudswitched.com

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