Data Classification Template

Classify data by sensitivity and criticality to apply appropriate protection, retention, and access controls. Essential for GDPR compliance and information security.

4	GDPR	Protect	Free
CLASSIFICATION LEVELS	ALIGNED WITH UK GDPR	RIGHT DATA, RIGHT CONTROLS	CLASSIFICATION TEMPLATE

Why Data Classification Matters

Not all data is equal. Classifying data by sensitivity ensures you apply the right level of protection, encryption, access control, and retention to each category. Over-protecting everything is expensive; under-protecting sensitive data is dangerous.

1 Classification Levels

Define four classification levels with clear criteria and handling rules.

LEVEL	LABEL	DESCRIPTION	EXAMPLES	
1	**Public**	Information intended for public disclosure	Marketing materials, published reports, website content	No restrictions on sharing
2	**Internal**	General business information not for public release	Internal memos, meeting notes, org charts	Share within organisation only
3	**Confidential**	Sensitive business information with restricted access	Financial data, HR records, customer data, contracts	Need-to-know access, encrypted storage
4	**Restricted**	Highly sensitive data with legal/regulatory implications	Personal data (GDPR), medical records, payment card data	Strict access control, encrypted, logged access

2 Data Inventory

Document all data assets with their classification, location, and owner.

DATA ASSET	CLASSIFICATION	LOCATION	FORMAT				
Customer database	Confidential	Azure SQL	Digital	Sales Director	Sales team	Duration of relationship + 6yr	Yes
Employee HR records	Restricted	SharePoint (HR)	Digital	HR Director	HR team only	Employment + 6yr	Yes
Financial accounts	Confidential	Sage / SharePoint	Digital + Paper	Finance Director	Finance team	7 years (HMRC)	No
Marketing materials	Public	SharePoint	Digital	Marketing Manager	All staff	Superseded	No

3 Protection Controls by Classification

Define the security controls required for each classification level.

CONTROL	PUBLIC	INTERNAL	CONFIDENTIAL	
Encryption at rest	Optional	Recommended	Required	Required (AES-256)
Encryption in transit	Optional	Recommended	Required (TLS)	Required (TLS 1.2+)
Access control	None	AD group	Named individuals	Named + MFA + audit log
DLP policies	None	Basic	Email + endpoint DLP	Full DLP + sensitivity labels
Backup	Standard	Standard	Encrypted backup	Encrypted + immutable backup
Sharing (external)	Allowed	Link (internal only)	Approved recipients only	Prohibited (without approval)
Retention	Until superseded	3 years	Per regulation	Per regulation + legal hold
Disposal	No requirement	Delete	Secure delete + log	Secure delete + certificate

4 GDPR Personal Data Register

Document all personal data processing activities in line with UK GDPR Article 30 requirements.

PERSONAL DATA TYPE	LAWFUL BASIS	DATA SUBJECTS	PURPOSE			
Employee records	Contract + Legal obligation	Staff	Employment administration	HMRC, pension provider	6yr after leaving	No
Customer contact details	Legitimate interest	Customers	Service delivery, communication	None	Duration + 6yr	No
Marketing mailing list	Consent	Prospects	Email marketing	Mailchimp	Until consent withdrawn	No
CCTV footage	Legitimate interest	Staff, visitors	Security	Police (if required)	30 days	Yes

GDPR Accountability

Under UK GDPR, you must be able to demonstrate compliance. This data register is a legal requirement (Article 30) for most organisations. Keep it up to date and review it at least annually. The ICO can request to see this register at any time.

Notes

Prepared by: _____ Date: _____ Approved by: _____