GSDC
Global Skill Development Council

DATA PROTECTION CHECKLIST

www.gsdcouncil.org

Data Protection — Essential Checklists

Quick Reference for Data Protection Officers and Privacy Professionals

GDPR Compliance

Checklist 1 — Core compliance obligations for every organisation processing personal data.

DPO Onboarding

Checklist 2 — Essential first steps for a newly appointed Data Protection Officer.

Vendor Due Diligence

Checklist 3 — Third-party risk assessment before engaging any data processor.

Data Breach Response

Checklist 4 — Step-by-step actions from identification through to remediation.

DPIA

Checklist 5 — Determine whether a DPIA is required and how to conduct one.

Privacy by Design

Checklist 6 — Embed privacy into every new project and system from the start.

CHECKLIST 1 — GDPR Compliance Checklist

#	Item	Status	
1	Valid legal basis identified for every processing activity	Done	In Progress / Not Started
2	Record of Processing Activities (ROPA) is maintained and current	Done	In Progress / Not Started
3	DPO / Privacy Officer appointed where required	Done	In Progress / Not Started
4	Privacy Notice is up to date and accessible at all data collection points	Done	In Progress / Not Started
5	Cookie notice and consent mechanism are in place on the website	Done	In Progress / Not Started
6	Consent records are maintained with date, purpose, and method	Done	In Progress / Not Started
7	Process in place to receive and respond to individual rights requests on time	Done	In Progress / Not Started

CHECKLIST 1 — GDPR Compliance Checklist *(continued)*

#	Item	Status	
8	Data Processing Agreements in place with all third-party processors	Done	In Progress / Not Started
9	International data transfers have appropriate safeguards	Done	In Progress / Not Started
10	Technical security measures in place — encryption, access controls, MFA	Done	In Progress / Not Started
11	Data breach response procedure is documented and tested	Done	In Progress / Not Started
12	Data retention schedule is documented and applied	Done	In Progress / Not Started
13	DPIAs conducted for all high-risk processing activities	Done	In Progress / Not Started
14	Privacy by design applied to all new projects and systems	Done	In Progress / Not Started
15	All staff have completed data protection awareness training	Done	In Progress / Not Started

Completed by: _____ Date: _____ Next Review: _____

CHECKLIST 2 — DPO Onboarding Checklist

#	Task	Done?
1	Obtain formal written DPO appointment with defined scope and authority	
2	Confirm direct reporting line to senior leadership	
3	Confirm independence — no conflicting roles or responsibilities	
4	Gain access to key systems — HR, IT, Legal, Finance, Procurement	
5	Review existing privacy policies, notices, and procedures	
6	Review previous audit reports, breach records, and regulatory correspondence	
7	Review the ROPA — assess completeness and accuracy	
8	Review all Data Processing Agreements with vendors	

CHECKLIST 2 — DPO Onboarding Checklist *(continued)*

#	Task	Done?
9	Assess the individual rights request process	
10	Review data breach response procedure — when was it last tested?	
11	Identify high-risk processing activities requiring a DPIA	
12	Review staff training records — when was last training done?	
13	Conduct a privacy gap assessment and present findings to leadership	
14	Deliver initial staff data protection awareness training	
15	Register with relevant supervisory authority where required	
16	Set up a calendar for audits, reviews, and training cycles	
17	Subscribe to updates from relevant supervisory authorities	

DPO Name: _____ Start Date: _____ Jurisdiction: _____

CHECKLIST 3 — Vendor / Third Party Due Diligence Checklist

#	Item	Status
1	Confirm whether the vendor will process personal data	Yes / No
2	Identify what personal data categories will be processed	Done
3	Identify countries where data will be stored or processed	Done
4	Confirm whether sensitive or children's data is involved	Yes / No
5	Vendor has a Privacy Policy and can confirm regulatory compliance	Yes / No
6	Vendor has a designated Privacy Officer or DPO	Yes / No
7	Vendor holds relevant security certifications — ISO 27001, SOC 2, or equivalent	Yes / No
8	Data is encrypted at rest and in transit	Yes / No

CHECKLIST 3 — Vendor / Third Party Due Diligence Checklist *(continued)*

#	Item	Status
9	Vendor has a documented breach notification procedure	Yes / No
10	Vendor can notify breaches within the required regulatory timeframe	Yes / No
11	Data Processing Agreement is in place and covers all required elements	Yes / No
12	Audit rights are included in the contract	Yes / No
13	Sub-processor arrangements are identified and require authorization	Yes / No
14	International transfer mechanism is identified and in place	Yes / No
15	Data deletion / return on termination is specified in the contract	Yes / No

Vendor Risk Rating: High / Medium / Low

Approved for Engagement: Yes / No / Conditional

Completed by: _____ **Date:** _____ **DPO Review:** _____

CHECKLIST 4 — Data Breach Response Checklist

IDENTIFY AND CONTAIN

#	Action	Done?	Time
1	Confirm a breach has occurred or is suspected		
2	Isolate affected systems to prevent further data loss		
3	Preserve evidence — do not delete logs or affected files		
4	Notify the DPO / Privacy Officer immediately		
5	Record date and time the organization became aware		

ASSESS

#	Action	Done?	Time
6	Identify what personal data was involved and its sensitivity		
7	Identify how many individuals are affected and in which countries		
8	Assess likely consequences for affected individuals		
9	Determine overall risk level — no risk / risk / high risk		

#	Action	Done?	Time
10	Determine whether regulatory notification is required		
11	Determine whether individual notification is required		

CHECKLIST 4 — Data Breach Response Checklist *(continued)*

NOTIFY

#	Action	Done?	Time
12	Identify applicable notification deadline for each jurisdiction		
13	Submit regulatory notification if required — within deadline		
14	Send individual notifications if high risk confirmed		
15	Document all notification decisions including decisions NOT to notify		

REMEDIATE AND LEARN

#	Action	Done?	Time
16	Implement technical fixes to close the vulnerability		
17	Complete the breach register entry in full		
18	Identify root cause and implement preventive measures		
19	Report findings to senior management		
20	Conduct targeted staff training if human error was a factor		

Breach Reference: _____ DPO Sign-Off: _____ Date Closed: _____

CHECKLIST 5 — DPIA Checklist

STEP 1 — Is a DPIA Required?

#	Trigger	Applies?
1	Systematic profiling with significant effects on individuals	Yes / No
2	Large-scale processing of sensitive / special category data	Yes / No
3	Systematic monitoring of publicly accessible areas	Yes / No
4	Processing children's data at scale	Yes / No
5	New technology with unknown or high privacy risks	Yes / No
6	Automated decision-making with significant effects	Yes / No
7	Large-scale matching or combining of datasets	Yes / No

DPIA Required? Yes — proceed / No — document reason

CHECKLIST 5 — DPIA Checklist

STEP 2 — Conduct the DPIA

#	Item	Status
1	Describe the processing — what data, whose data, why, how long, where	Done
2	Confirm a valid legal basis exists for the processing	Done
3	Confirm only minimum necessary data is collected	Done
4	Confirm individuals will be informed of the processing	Done
5	Identify all privacy risks — unauthorized access, misuse, discrimination, breach	Done
6	Assess likelihood and severity of each risk	Done
7	Identify mitigation measures for each risk with owner and deadline	Done
8	Assess residual risk after mitigation	Done
9	Confirm whether supervisory authority consultation is required	Done
10	DPO has reviewed and approved the DPIA	Done
11	ROPA has been updated to include this processing activity	Done

DPIA Outcome: Approved / Approved with conditions / Not approved

DPO Sign-Off: _____ **Date:** _____ **Review Date:** _____

CHECKLIST 6 — Privacy by Design Checklist

PROJECT INITIATION

#	Item	Status
1	DPO consulted at the start of the project	Yes / No
2	Privacy screening completed to assess data protection implications	Yes / No
3	DPIA screening completed — decision documented	Yes / No

DATA MINIMISATION

#	Item	Status
4	Only minimum necessary data is collected	Yes / No
5	Anonymisation or pseudonymisation applied where identification is not needed	Yes / No
6	Automatic deletion or archiving built into the system	Yes / No

SECURITY BY DEFAULT

#	Item	Status
7	Data encrypted at rest and in transit	Yes / No
8	Access controls and MFA in place	Yes / No
9	Activity logs and audit trails enabled	Yes / No
10	Security review or penetration test conducted	Yes / No

CHECKLIST 6 — Privacy by Design Checklist *(continued)*

PRIVACY AS THE DEFAULT

#	Item	Status
11	Default settings are the most privacy-protective option	Yes / No
12	Marketing preferences default to opt-out	Yes / No
13	Cookies default to essential only	Yes / No

TRANSPARENCY AND RIGHTS

#	Item	Status
14	Privacy notice linked at every data collection point	Yes / No
15	Individuals can easily access, correct, or delete their data	Yes / No

DOCUMENTATION

#	Item	Status
16	ROPA updated to include this processing activity	Yes / No
17	DPO has reviewed and signed off	Yes / No

Project Name: _____ DPO Sign-Off: _____ Date: _____

CHECKLIST 7 — Annual Data Protection Audit Checklist

GOVERNANCE

#	Audit Item	Status	Action Needed
1	DPO is appointed, independent, and resourced adequately	Compliant	Gap
2	Senior management is actively engaged in data protection oversight	Compliant	Gap

ROPA

#	Audit Item	Status	Action Needed
3	ROPA reviewed and updated in the last 12 months	Compliant	Gap
4	Every processing activity has a documented legal basis	Compliant	Gap

PRIVACY NOTICE

#	Audit Item	Status	Action Needed
5	Privacy Notice reviewed and updated in the last 12 months	Compliant	Gap
6	Cookie notice and consent mechanism are current and functional	Compliant	Gap

CHECKLIST 7 — Annual Data Protection Audit Checklist *(continued)*

INDIVIDUAL RIGHTS

#	Audit Item	Status	Action Needed
7	All rights requests received this year were responded to on time	Compliant	Gap
8	Rights request log is maintained and complete	Compliant	Gap

DATA SECURITY

#	Audit Item	Status	Action Needed
9	Security review or testing conducted during the year	Compliant	Gap

#	Audit Item	Status	Action Needed
10	Access controls reviewed — unnecessary access removed	Compliant	Gap
11	Breach register is up to date and all incidents documented	Compliant	Gap

CHECKLIST 7 — Annual Data Protection Audit Checklist *(continued)*

DATA RETENTION

#	Audit Item	Status	Action Needed
12	Retention schedule reviewed and applied in practice	Compliant	Gap
13	Data exceeding retention period deleted or anonymized	Compliant	Gap

VENDORS

#	Audit Item	Status	Action Needed
14	DPAs reviewed and up to date with all processors	Compliant	Gap
15	New vendors onboarded this year have been assessed	Compliant	Gap

PRIVACY BY DESIGN AND DPIA

#	Audit Item	Status	Action Needed
16	DPIAs conducted for all high-risk processing this year	Compliant	Gap
17	DPO consulted on all new projects involving personal data	Compliant	Gap

CHECKLIST 7 — Annual Data Protection Audit Checklist *(continued)*

TRAINING

#	Audit Item	Status	Action Needed
18	All staff completed data protection training in the last 12 months	Compliant	Gap
19	New joiners received data protection training during onboarding	Compliant	Gap
20	Training content reviewed and updated to reflect current requirements	Compliant	Gap

Annual Audit Summary

Area	Status	Priority Action
Governance	Compliant / Partial / Gap	
ROPA	Compliant / Partial / Gap	
Privacy Notice	Compliant / Partial / Gap	
Individual Rights	Compliant / Partial / Gap	
Data Security	Compliant / Partial / Gap	
Data Retention	Compliant / Partial / Gap	
Vendors	Compliant / Partial / Gap	
Privacy by Design	Compliant / Partial / Gap	
Training	Compliant / Partial / Gap	

Audit Conducted By: _____ **Date:** _____

Presented to Senior Management: Yes — Date: _____ / No

Next Audit Due: _____

Annual Audit Summary

Area	Status	Priority Action
Governance	Compliant / Partial / Gap	
ROPA	Compliant / Partial / Gap	
Privacy Notice	Compliant / Partial / Gap	
Individual Rights	Compliant / Partial / Gap	
Data Security	Compliant / Partial / Gap	
Data Retention	Compliant / Partial / Gap	
Vendors	Compliant / Partial / Gap	
Privacy by Design	Compliant / Partial / Gap	
Training	Compliant / Partial / Gap	

Audit Conducted By: _____ **Date:** _____

Presented to Senior Management: Yes — Date: _____ / No

Next Audit Due: _____