GSDC
Global Skill Development Council

DATA PROTECTION OFFICER 7 PRIVACY AND **DATA PROTECTION TEMPLATES**

www.gsdcouncil.org

TEMPLATE 1 OF 7

TEMPLATE 1 — Data Breach Notification Template

A comprehensive, multi-part template for managing data breaches from initial discovery through regulatory notification, individual communication, and ongoing record-keeping.

1 Part A
Internal Breach Report

2 Part B
DPO Risk Assessment

3 Part C
Regulatory Notification

4 Part D
Individual Notification Letter

5 Part E
Breach Register

PART A — Internal Breach Report

Breach Reference Number	
Date & Time Discovered	
Reported By	
Department	
Date Reported to DPO	
Organization Name	
Jurisdictions Affected	

Type of Breach:

[ ]	Confidentiality — unauthorized disclosure
[ ]	Integrity — unauthorized alteration
[ ]	Availability — unauthorized loss of access

How It Occurred:

[ ]	Cyber attack
[ ]	Phishing
[ ]	Ransomware
[ ]	Lost/stolen device
[ ]	Wrong email recipient
[ ]	Unauthorized access
[ ]	Human error
[ ]	Other: _____

Data Affected:

Category	Details
Types of personal data involved	
Sensitive data involved?	[ ] Yes — specify: [ ] No
Approximate number of individuals	
Categories of individuals	
Systems affected	
Countries/regions affected	

Immediate Containment Actions:

Action	Taken By Whom	Date/Time

PART B — DPO Risk Assessment

Risk Level:

[ ]	No risk — document only, no notification required
[ ]	Risk identified — regulatory notification required
[ ]	High risk — regulatory notification AND individual notification required

Notification Deadlines — Check What Applies:

Jurisdiction	Law	Deadline
EU	GDPR	72 hours
UK	UK GDPR	72 hours
Brazil	LGPD	2 working days
Singapore	PDPA	3 calendar days
Canada	PIPEDA	Without unreasonable delay
Australia	Privacy Act	30 days
USA (varies)	State laws	30–90 days
South Africa	POPIA	As soon as reasonably possible

Applicable deadline for this breach: _____

PART C — Regulatory Notification

Authority Name:

_____

Notification Date & Time:

_____

Complete the following fields when notifying the relevant supervisory authority:

1 Nature of the breach

Describe what happened, data categories, and number of individuals affected

2 DPO contact details

Name, email, telephone, organization

3 Likely consequences

Describe impact on affected individuals

4 Measures taken

Describe containment and remediation steps

5 Phased notification?

[ ] Yes — further info by: ___ [ ] No

PART D — Individual Notification Letter

> **[Organization Letterhead]**
> **Date: _____**
> **Subject: Important Notice About Your Personal Information**

Dear [Name],

We are writing to inform you of a data security incident affecting your personal information.

What happened

On [date], we discovered [brief description]. We became aware on [date] and took immediate action.

Information affected

[List data categories clearly]

What we are doing

[List containment and remediation steps]

What you should do

[List recommended protective steps]

Contact us

[DPO name, email, telephone]

We sincerely apologize for this incident.

Yours sincerely,
[Name, Title, Organization]

PART E — Breach Register

Field	Details
Breach Reference	
Date Discovered	
Nature of Breach	
Data Affected	
Individuals Affected	
Risk Level	[ ] No Risk [ ] Risk [ ] High Risk
Authority Notified?	[ ] Yes — Date: [ ] No
Individuals Notified?	[ ] Yes — Date: [ ] No
Root Cause	
Preventive Measures	
DPO Sign-Off	
Date Closed	

TEMPLATE 2 OF 7

TEMPLATE 2 — Individual Rights / Privacy Request Response Template

A structured template for managing and responding to individual privacy rights requests across multiple jurisdictions, from intake through to final response and logging.

1 Part A
Request Intake

2 Part B
Data Search

3 Part C
Acknowledgement Letter

4 Part D
Response Letter

5 Part E
Request Log

PART A — Request Intake

Request Reference Number	
Date Received	
How Received	[ ] Email [ ] Letter [ ] Online Form [ ] Phone [ ] In Person
Requester Name	
Requester Email / Address	
Relationship	[ ] Customer [ ] Employee [ ] Former Employee [ ] Other:
Applicable Law / Jurisdiction	
Identity Verified?	[ ] Yes — Method: [ ] No — Action needed:
Response Deadline	
Extension Applied?	[ ] Yes — New deadline: [ ] No

Response Deadlines by Jurisdiction:

Jurisdiction	Law	Timeframe
EU / UK	GDPR / UK GDPR	1 month (extendable to 3)
California	CCPA / CPRA	45 days (extendable by 45)
Brazil	LGPD	15 days
Canada	PIPEDA	30 days
Singapore	PDPA	30 business days
Australia	Privacy Act	30 days

Type of Request

[ ] Access

Copy of personal data held

[ ] Correction

Fix inaccurate data

[ ] Deletion / Erasure

Delete personal data

[ ] Restriction

Limit how data is used

[ ] Portability

Receive data in portable format

[ ] Objection / Opt-Out

Stop certain processing

[ ] Automated Decision Making

Challenge automated decision

[ ] General Information

How data is used

PART B — Data Search

System / Location	Searched By	Date	Records Found?
CRM System			[ ] Yes [ ] No
HR System			[ ] Yes [ ] No
Email System			[ ] Yes [ ] No
Finance System			[ ] Yes [ ] No
Marketing Platform			[ ] Yes [ ] No
Cloud Storage			[ ] Yes [ ] No
Physical Files			[ ] Yes [ ] No
Third Party Systems			[ ] Yes [ ] No

Redactions required? [ ] Yes — reason: _____ [ ] No

PART C — Acknowledgement Letter

> **[Organization Letterhead]**
> **Date:** _____
> **Reference:** _____

Dear [Name],

Thank you for your privacy rights request received on [date].

We confirm receipt and are processing your request in line with applicable privacy law. We will respond by [deadline date]. If we need more time due to complexity, we will contact you in advance.

For questions, please contact our Privacy Officer:
Email: _____
Telephone: _____

Yours sincerely,
[Name, Title, Organization]

PART D — Response Letter & Request Log

> **[Organization Letterhead]**
> **Date:** _____
> **Reference:** _____

Dear [Name],

Thank you for your privacy rights request dated [date]. We have completed our review.

1. Data Held

We [do / do not] hold personal information about you.

2. Your Information

[Attach copy / describe what is enclosed. Explain any redactions.]

3. Purposes of Processing

[List clearly]

4. Legal Basis

[List applicable basis per jurisdiction]

5. Data Categories Held

[List]

6. Who We Share With

[List recipients]

7. International Transfers

[ ] No transfers outside your country [ ] Transfers to [country] — safeguard: [describe]

8. Retention

We keep your data for [period] because [reason].

9. Your Rights

You may have the right to correct, delete, restrict, or object to processing. Contact our Privacy Officer at [email] to exercise these rights.

10. Complaints

If unsatisfied, you may raise a complaint with the relevant privacy authority in your jurisdiction.

Yours sincerely,
[Name, Title, Organization]

PART E — Request Log

Ref	Date	Requester	Jurisdiction	Type	Deadline	Extension	Responded	Outcome
							[ ] Y [ ] N	

TEMPLATE 3 OF 7

TEMPLATE 3 — Data Processing Agreement (DPA)

A comprehensive, multi-jurisdictional Data Processing Agreement for use between Controllers and Processors, including all required schedules.

Main Agreement

Definitions, Scope, Obligations, Sub-Processing, Transfers, Breach Notification, Term

Schedule 1

Processing Details

Schedule 2

Security Measures

Schedule 3

Authorized Sub-Processors

Schedule 4

Transfer Mechanisms

DATA PROCESSING AGREEMENT — Parties & Definitions

Date: _____

Between: [Controller / Business Name], [jurisdiction], [address] — ("**Controller**")

And: [Processor / Service Provider Name], [jurisdiction], [address] — ("**Processor**")

1. DEFINITIONS

Personal Data / Personal Information

Any information relating to an identified or identifiable individual under applicable privacy law.

Processing

Any operation on personal data including collection, storage, use, sharing, or deletion.

Applicable Privacy Law

All privacy laws applicable in jurisdictions where the parties operate and where individuals are located.

Sub-Processor

Any third party engaged by the Processor to process data on behalf of the Controller.

Security Incident

Any breach leading to unauthorized access, loss, or disclosure of personal data.

Scope & Controller Obligations

2. SCOPE

This Agreement governs all processing of personal data by the Processor on behalf of the Controller in connection with: **[Describe services — e.g., cloud hosting, payroll processing, HR software]**

Full processing details are in **Schedule 1**.

3. CONTROLLER OBLIGATIONS

The Controller shall:

- → Ensure a valid legal basis exists for all processing
- → Provide clear written processing instructions
- → Ensure data provided is accurate
- → Comply with all applicable privacy law

4. Processor Obligations

1	**Instructions** Process data only on Controller's documented instructions unless required by law.
2	**Confidentiality** Ensure all staff with data access are bound by confidentiality obligations.
3	**Security** Implement and maintain appropriate technical and organizational security measures per Schedule 2.
4	**Sub-Processing** Do not engage sub-processors without prior written Controller authorization. See Schedule 3.
5	**Individual Rights** Assist the Controller in responding to individual rights requests within applicable timeframes.
6	**Compliance Support** Assist with breach notification, privacy impact assessments, and regulatory obligations.
7	**Data Return / Deletion** On termination, delete or return all personal data within [30] days and confirm in writing.
8	**Audit** Provide all information needed to demonstrate compliance and support Controller audits.

Sub-Processing & International Transfers

5. SUB-PROCESSING

- Requires prior written Controller authorization
- Sub-processors must be bound by equivalent obligations
- Processor remains liable for sub-processor performance
- Controller to be notified of changes with adequate notice to object

6. INTERNATIONAL TRANSFERS

No cross-border transfers without Controller authorization. Where transfers occur, appropriate safeguards must be in place per Schedule 4.

Breach Notification, Term & Signatures

7. BREACH NOTIFICATION

Notify Controller within **[24/48] hours** of becoming aware of any security incident, including:

- Nature and description of incident
- Categories and number of individuals affected
- Likely consequences
- Actions taken or planned

8. TERM AND TERMINATION

This Agreement lasts for the duration of the underlying services agreement. On termination, data is deleted or returned within [30] days.

SIGNATURES

Controller	**Processor**
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date:

Schedule 1 — Processing Details & Schedule 2 — Security Measures

SCHEDULE 1 — PROCESSING DETAILS

Field	Details
Purpose of processing	
Nature of processing	
Duration	
Data categories	
Categories of individuals	
Sensitive data involved?	[ ] Yes — specify: [ ] No
Jurisdictions of individuals	

SCHEDULE 2 — SECURITY MEASURES

Technical

- Encryption at rest and in transit
- Access controls
- MFA
- Security patching
- Backups
- Monitoring and logging

Organizational

- Privacy training
- Confidentiality obligations
- Incident response procedures
- Risk assessments
- Retention and deletion procedures

Schedule 3 — Authorized Sub-Processors & Schedule 4 — Transfer Mechanisms

SCHEDULE 3 — AUTHORIZED SUB-PROCESSORS

Sub-Processor	Country	Activity	Safeguard

SCHEDULE 4 — TRANSFER MECHANISMS

Destination	Law	Safeguard
		[ ] Adequacy Decision [ ] Standard Clauses [ ] BCRs [ ] Other:

TEMPLATE 4 OF 7

TEMPLATE 4 — Privacy Notice / Privacy Policy

A comprehensive, multi-jurisdictional privacy notice template covering all required disclosures for organizations operating globally.

1 Who We Are

2 Information We Collect

3 How We Collect

4 Why We Use It

5 Who We Share With

6 International Transfers

7 Retention

8 Your Rights

9 Security

10 Children

11 Changes

12 Contact

PRIVACY NOTICE — Sections 1 & 2

> **[Organization Name]**
> **Effective Date: _____ Last Updated: _____ Version: _____**

1. WHO WE ARE

[Organization Name] is [description] located at [address]. We act as the **Data Controller / Business** for the personal information described in this notice.

Privacy Officer / DPO:
Email: _____ Telephone: _____ Address: _____

2. INFORMATION WE COLLECT

Category	Examples
Identity	Name, date of birth, national ID
Contact	Email, address, phone number
Financial	Payment details, billing address
Transaction	Purchase and order history
Technical	IP address, device ID, cookies
Usage	How you use our website and services
Communications	Records of your correspondence with us
Preferences	Marketing and communication preferences
Employment *(if applicable)*	Job title, qualifications, payroll
Sensitive *(if applicable)*	[Specify what and why]

Sections 3 & 4 — How We Collect & Why We Use Your Information

3. HOW WE COLLECT YOUR INFORMATION

Directly

When you register, purchase, contact us, or apply for a job

Automatically

Through cookies and tracking technologies on our website

Third parties

From business partners, analytics providers, or public sources where permitted

4. WHY WE USE YOUR INFORMATION

Purpose	Data Used	Legal Basis
Account management	Identity, Contact	Contract
Order processing	Identity, Contact, Financial	Contract
Payment processing	Financial	Contract / Legal obligation
Service communications	Identity, Contact	Contract
Marketing	Contact, Preferences	Consent / Legitimate interest
Website improvement	Technical, Usage	Legitimate interest
Fraud prevention	Technical, Identity	Legitimate interest / Legal obligation
Legal compliance	Identity, Financial	Legal obligation
Customer support	Identity, Contact	Contract / Legitimate interest

Sections 5, 6 & 7 — Sharing, Transfers & Retention

5. WHO WE SHARE YOUR INFORMATION WITH

Recipient	Purpose
IT and hosting providers	System maintenance and support
Payment processors	Secure payment handling
Delivery partners	Order fulfilment
Analytics providers	Service improvement
Professional advisors	Legal, financial, audit
Regulatory authorities	Legal compliance

We do not sell your personal information for third-party marketing.

6. INTERNATIONAL TRANSFERS

Where we transfer data internationally, we ensure appropriate protections are in place such as standard contractual arrangements, adequacy decisions, or binding corporate rules. Contact our Privacy Officer for details.

7. HOW LONG WE KEEP YOUR INFORMATION

We retain data only as long as necessary for its stated purpose and to meet legal requirements. Retention periods vary by data type and jurisdiction. Once no longer needed, data is securely deleted or anonymized.

Sections 8, 9 & 10 — Your Rights, Security & Children

8. YOUR PRIVACY RIGHTS

Depending on your country, you may have the right to:

Right	Description
Access	Request a copy of your data
Correction	Fix inaccurate or incomplete data
Deletion	Request removal of your data
Restriction	Limit how your data is used
Portability	Receive data in a machine-readable format
Object / Opt-Out	Stop certain processing activities
Withdraw Consent	Withdraw consent at any time
Complain	Raise concerns with your local privacy authority

To exercise your rights, contact: [Privacy Officer email]

9. SECURITY

We implement appropriate technical and organizational measures to protect your data. No system is 100% secure — if you suspect a breach, contact us immediately at [email].

10. CHILDREN

Our services are not directed at children under [13/16 — specify]. We do not knowingly collect children's data without parental consent. Contact us if you believe we hold a child's data without proper authorization.

Sections 11 & 12 — Changes & Contact

11. CHANGES TO THIS NOTICE

We review this notice regularly. The current version is always at [website URL]. We will notify you of significant changes before they take effect.

12. CONTACT AND COMPLAINTS

Privacy Officer / DPO: [Name, Email, Telephone, Address]

If unsatisfied with how we handle your data, you may raise a complaint with your local data protection authority. A directory of global authorities is available at globalprivacyassembly.org.

TEMPLATE 5 OF 7

TEMPLATE 5 — Legitimate Interests Assessment (LIA)

A structured three-step assessment for determining whether legitimate interests can be relied upon as a legal basis for processing personal data.

Purpose Test

Necessity Test

Balancing Test

All three tests must be passed before legitimate interests can be relied upon as a legal basis for processing.

LIA Header & Step 1 — Purpose Test

LIA Reference Number	
Date Completed	
Completed By	
DPO Review	
Processing Activity	
Applicable Law / Jurisdiction	
Next Review Date	

STEP 1 — PURPOSE TEST

What is the processing activity?
[Describe what data is processed, by whom, and what is done with it]

What is the legitimate interest being pursued?
[Be specific — e.g., "To send marketing to existing customers about related services" or "To monitor network logs to detect cyber threats"]

Type of interest:

[ ]	Commercial
[ ]	Organizational / Operational
[ ]	Social
[ ]	Third party interest

Is the interest legitimate?

[ ]	Lawful — not prohibited by applicable law
[ ]	Clearly articulated — specific enough to be weighed against individual rights
[ ]	Real and present — not speculative

Purpose test outcome: [ ] Passed — proceed to Step 2 [ ] Failed — use alternative legal basis

Step 2 — Necessity Test

Is the processing necessary to achieve the purpose?
[Could the same outcome be achieved without processing personal data or with less data?]

Could the purpose be achieved less intrusively?

[ ]	No — this is the least privacy-invasive approach
[ ]	Yes — describe alternative: _____

Is the data proportionate to the purpose?

[ ]	Yes
[ ]	No — scope needs reducing before proceeding

Necessity test outcome: [ ] Passed — proceed to Step 3 [ ] Failed — adjust processing

Step 3 — Balancing Test (Parts A, B & C)

3A — Nature of Data

Sensitive / special category data involved?	[ ] Yes [ ] No
Children's data involved?	[ ] Yes [ ] No
Could cause harm or distress if misused?	[ ] Yes [ ] No

Data sensitivity: [ ] Low [ ] Medium [ ] High

3B — Individual Expectations

Would individuals reasonably expect this use?

[ ]	Yes — within reasonable expectations
[ ]	Possibly — not expected but not surprising
[ ]	No — would surprise or concern individuals

Is this processing communicated in the privacy notice?

[ ]	Yes
[ ]	No — needs to be added

3C — Impact on Individuals

Potential Impact	Likelihood	Severity
Privacy intrusion	[ ] Low [ ] Med [ ] High	[ ] Low [ ] Med [ ] High
Financial loss	[ ] Low [ ] Med [ ] High	[ ] Low [ ] Med [ ] High
Reputational damage	[ ] Low [ ] Med [ ] High	[ ] Low [ ] Med [ ] High
Discrimination	[ ] Low [ ] Med [ ] High	[ ] Low [ ] Med [ ] High
Loss of data control	[ ] Low [ ] Med [ ] High	[ ] Low [ ] Med [ ] High

Overall impact rating: [ ] Low [ ] Medium [ ] High

Step 3 — Balancing Test (Parts D & E)

3D — Safeguards in Place

Safeguard	In Place?
Clear opt-out / objection mechanism	[ ] Yes [ ] No
Data minimisation applied	[ ] Yes [ ] No
Communicated in privacy notice	[ ] Yes [ ] No
Rights easy to exercise	[ ] Yes [ ] No
Appropriate security measures	[ ] Yes [ ] No
Defined and proportionate retention period	[ ] Yes [ ] No

3E — Balancing Conclusion

Do the organization's legitimate interests outweigh individual rights?

[ ] Yes — legitimate interests prevail. Processing can proceed.

Reasons:

[ ] No — individual rights outweigh. Cannot rely on legitimate interests.

Reasons and next steps:

Step 4 — Overall Conclusion & Sign-Off

STEP 4 — OVERALL CONCLUSION

Test	Result
Purpose Test	[ ] Passed [ ] Failed
Necessity Test	[ ] Passed [ ] Failed
Balancing Test	[ ] Passed [ ] Failed
Overall Outcome	[ ] Legitimate interests can be relied upon [ ] Cannot be relied upon

SIGN-OFF

Completed By / Date	
DPO Review	[ ] Approved [ ] Not Approved
DPO Signature / Date	
Next Review Date	

TEMPLATE 6 OF 7

TEMPLATE 6 — Data Retention Schedule

A comprehensive data retention schedule covering all major data categories across HR, customer, financial, digital, supplier, security, privacy compliance, and sensitive data.

Section 1
HR & Employment Data

Section 2
Customer & Client Data

Section 3
Financial & Accounting Data

Section 4
Website & Digital Data

Section 5
Supplier & Contractor Data

Section 6
Security & Premises Data

Section 7
Privacy Compliance Data

Section 8
Sensitive / Special Category Data

DATA RETENTION SCHEDULE — Header

Organization Name	
DPO Approval	
Date Approved	
Version	
Applicable Jurisdictions	
Next Review Date	

Note: Retention periods below reflect commonly applied timeframes across major jurisdictions. Always verify specific legal requirements in every country where you operate.

Section 1 — HR and Employment Data

Data Category	Retention Period	Basis	Disposal
Job applications — unsuccessful	6–12 months	Legitimate interest	Secure deletion
Job applications — successful	Employment + 6–7 years	Legal obligation	Secure deletion
Employment contracts	Employment + 6–7 years	Legal obligation	Secure deletion
Personnel files	Employment + 6–7 years	Legal obligation	Secure deletion
Payroll records	5–7 years	Tax / legal obligation	Secure deletion
Pension records	10–12 years after benefits cease	Legal obligation	Secure deletion
Sickness / absence records	Employment + 6 years	Legal obligation	Secure deletion
Disciplinary — warnings	1–2 years	Legitimate interest	Secure deletion
Disciplinary — dismissal	Employment + 6–7 years	Legal obligation	Secure deletion
Performance appraisals	Employment + 5 years	Legitimate interest	Secure deletion
Training records	Employment + 3 years	Legitimate interest	Secure deletion
Background checks	6 months after decision	Legal obligation	Secure deletion
Accident / injury records	3–10 years (jurisdiction dependent)	Legal obligation	Secure deletion
Leaver records	6–7 years from departure	Legal obligation	Secure deletion

Section 2 — Customer and Client Data

Data Category	Retention Period	Basis	Disposal
Customer account data	Relationship + 5–7 years	Contract / legal claims	Secure deletion
Transaction records	5–7 years from transaction	Tax / legal obligation	Secure deletion
Customer service communications	2–3 years	Legitimate interest	Secure deletion
Complaint records	5–6 years from resolution	Legal claims	Secure deletion
Marketing consent records	Until withdrawn + 1 year	Privacy compliance	Secure deletion
Opt-out / unsubscribe records	Indefinitely	Privacy compliance	Maintained as suppression list
Online enquiry forms	1–2 years	Legitimate interest	Secure deletion

Sections 3 & 4 — Financial and Digital Data

SECTION 3 — FINANCIAL AND ACCOUNTING DATA

Data Category	Retention Period	Basis	Disposal
Invoices and purchase orders	5–7 years	Tax / legal obligation	Secure deletion
Bank and financial records	5–7 years	Legal obligation	Secure deletion
Expense claims	5–7 years	Tax obligation	Secure deletion
Tax records	5–7 years from end of period	Tax authority requirement	Secure deletion
Contracts and agreements	6–10 years from expiry	Legal claims	Secure deletion
Audit records	7–10 years	Legal / regulatory obligation	Secure deletion

SECTION 4 — WEBSITE AND DIGITAL DATA

Data Category	Retention Period	Basis	Disposal
Website analytics	13–26 months	Legitimate interest	Automatic deletion
Server access logs	3–6 months	Security	Secure deletion
Cookie consent records	1 year from consent	Privacy compliance	Secure deletion
Inactive user accounts	1–2 years from last login	Legitimate interest	Secure deletion after notice
Email marketing data	Until opt-out + 1 year	Consent	Secure deletion

Sections 5 & 6 — Supplier, Contractor & Security Data

SECTION 5 — SUPPLIER AND CONTRACTOR DATA

Data Category	Retention Period	Basis	Disposal
Supplier contracts	6–7 years from expiry	Legal claims	Secure deletion
Contractor personal data	Engagement + 6 years	Legal obligation	Secure deletion
Vendor due diligence	5–7 years from end of relationship	Legal obligation	Secure deletion

SECTION 6 — SECURITY AND PREMISES DATA

Data Category	Retention Period	Basis	Disposal
CCTV — general	7–31 days	Legitimate interest	Automatic overwrite
CCTV — incident recorded	Investigation + 6 months	Legal claims	Secure deletion
Access control logs	1–3 months	Security	Secure deletion
Visitor records	3–6 months	Security	Secure deletion

Sections 7 & 8 — Privacy Compliance & Sensitive Data

SECTION 7 — PRIVACY COMPLIANCE DATA

Data Category	Retention Period	Basis	Disposal
Data breach records	3–5 years	Privacy law	Secure deletion
Individual rights request records	3 years from response	Privacy law	Secure deletion
Privacy impact assessments	Activity + 3 years	Privacy law	Secure deletion
ROPA / processing records	Current version maintained — prior versions 3 years	Privacy law	Secure deletion
Consent records	Processing duration + 1 year	Privacy law	Secure deletion
Privacy authority correspondence	5–7 years	Legal obligation	Secure deletion

SECTION 8 — SENSITIVE / SPECIAL CATEGORY DATA

Data Category	Retention Period	Justification	Disposal
Health records — employees	Employment + 8–10 years	Health and safety law	Secure deletion
Health records — customers	Specify per applicable law	Specify justification	Secure deletion
Diversity monitoring data	2 years then anonymize	HR / legal	Anonymize then retain
Biometric data	Minimum period necessary	Specific legal justification required	Secure deletion
Children's data	Minimum necessary — review on reaching adulthood	Privacy law	Secure deletion

Key Principles & Sign-Off

KEY PRINCIPLES

Start the clock correctly

Start the clock from the **end** of the relationship or transaction — not the beginning

Employment data

Start from the date of leaving

Financial records

Start from the end of the relevant financial year

Disposal methods

Digital data — secure deletion. Physical documents — certified shredding. Cloud data — written confirmation from processor.

SIGN-OFF

Document Owner	
DPO Signature / Date	
Next Review Date	

TEMPLATE 7 OF 7

TEMPLATE 7 — Consent Form Template

Four consent form options for different contexts, plus a consent records log.

Option A

Online / Website Consent Form

Option B

Paper Consent Form

Option C

Employee Consent Form

Option D

Parental / Guardian Consent for Minors

Option A — Online / Website Consent Form

Global Note: Consent requirements vary by jurisdiction. GDPR requires freely given, specific, informed, unambiguous consent. CCPA focuses on opt-out mechanisms. PDPA (Singapore) recognizes deemed consent in some cases. Always confirm the appropriate standard in your jurisdiction before use.

> **[Organization Name] — Your Communication Preferences**
>
> We would like to keep you updated about [describe — e.g., our products, offers, and news]. Please tell us how you would like to hear from us:

[ ]	**Email** — I agree to receive [type] communications from [Organization Name] by email
[ ]	**SMS** — I agree to receive [type] communications by text message
[ ]	**Phone** — I agree to receive [type] communications by telephone
[ ]	**Post** — I agree to receive [type] communications by post

How we use your information: We use your contact details only to send the communications you have selected. We will not share your details for third-party marketing. You can withdraw consent at any time by clicking "unsubscribe", replying STOP, or contacting us at [email/phone].

Read our full [Privacy Policy — link].

Your Details:

First Name	Last Name	Email	Phone	Country

[ ] I confirm I meet the minimum age required in my country to provide consent

By submitting, you confirm you freely agree to the above uses. You can withdraw at any time.

[Submit Button]

Option B — Paper Consent Form

> **[Organization Name]**
> **CONSENT TO USE YOUR PERSONAL INFORMATION**
> **Form Reference: _____ Date: _____**

Your Details

Full Name	Date of Birth	Country of Residence	Email	Phone

I am being asked to consent to:

[Purpose 1] — [Plain-language description of use, data involved, and duration]

[Purpose 2] — [Plain-language description]

[Purpose 3] — [Plain-language description]

Tick each box separately. Ticking one does not mean agreeing to all.

How we protect your information: We store your data securely and use it only for ticked purposes. We do not share it with third parties without your knowledge except where required by law. See our Privacy Notice at [website] or on request.

Your rights: You may access, correct, delete, or restrict use of your data and withdraw consent at any time — contact us at:
Email: _____ Phone: _____ Address: _____

Declaration: *I freely give consent for the purposes I have ticked. I understand I can withdraw at any time.*

Signature	Print Name	Date	Country

Option C — Employee Consent Form

Important: Consent is rarely appropriate for employee data due to the inherent power imbalance in employment. Only use where the processing is genuinely voluntary and no other legal basis applies.

> **[Organization Name] — EMPLOYEE CONSENT FORM**

Employee Name:	_____
ID:	_____
Department:	_____
Country:	_____
Date:	_____

I am being asked to voluntarily consent to:

[ ]	**[Purpose 1]** — [e.g., "Use my photo and job title on the company's public website"]
[ ]	**[Purpose 2]** — [e.g., "Share my testimonial and name in company marketing materials"]
[ ]	**[Purpose 3]** — [e.g., "Refer my details to our wellness partner for optional support services"]

Important:

- This is completely voluntary — no impact on your employment either way
- You can withdraw at any time by contacting HR or the Privacy Officer
- Withdrawal does not affect anything done before withdrawal
- See our Employee Privacy Notice for full details

Declaration: *I freely consent to the purposes ticked. I understand this is voluntary and I can withdraw at any time.*

Employee Signature	Print Name	Date

HR / Privacy Officer Record:

Field	Details
Collected By	
Date	
Method	[ ] Paper [ ] Digital [ ] Email
Storage Location	
Withdrawal Date	
Action on Withdrawa	

Option D — Parental / Guardian Consent for Minors

Use where services may be used by children — adjust age threshold to applicable local law

[Organization Name] — PARENTAL CONSENT FORM

Children under [13/16/18 — specify] require parental or guardian consent.

Child's Details

Full Name	
Date of Birth	
Country	

Parent / Guardian Details

Full Name	
Relationship to Child	
Email	
Phone	

I consent on behalf of the child named above for [Organization Name] to:

[ ]	[Purpose 1 — plain language]
[ ]	[Purpose 2 — plain language]

Your Rights as Parent / Guardian: You may access, correct, or delete your child's data and withdraw consent at any time. Contact: [email]

Declaration: *I am the parent/guardian of the child named above. I freely give consent for the purposes ticked and understand I can withdraw at any time.*

Signature	Print Name	Date

Consent Records Log

Ref	Name	Date	Purpose	Jurisdiction	Method	Withdrawal Date	Action Taken

GSDC
Global Skill Development Council

DATA PROTECTION OFFICER CERTIFICATION

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain insights into autonomous decision-making processes
- Apply knowledge using ready-to-implement templates
- Demonstrate ability to work with Agentic AI models
- Validate your skills wit

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org