NYMITY
innovating compliance

Framework for Demonstrable GDPR Compliance

A mapping of the Nymity's Privacy Management Accountability Framework™ to GDPR Compliance Obligations

Overview

The concept of accountability is a common principle for organisations across many disciplines. It embodies the notion that organisations live up to expectations, for example, in their behavior toward data subjects or in the delivery of their products and services. The General Data Protection Regulation (GDPR) integrates accountability as a principle in Article 5(2) which requires organisations to demonstrate compliance with the principles of the GDPR. Article 24 sets out how organisations can do this by requiring the implementation of appropriate technical and organisational measures to ensure that organisations can demonstrate that the processing of personal data is performed in accordance with the GDPR.

Nymity Research™ has identified 39 Articles under the GDPR that require evidence of a technical or organisational measure to demonstrate compliance and has mapped these to the Nymity Privacy Management Accountability Framework™. The result is the identification of 55 "primary" technical and organisational measures that, if implemented, may produce documentation that will help demonstrate ongoing compliance with your GDPR compliance obligations (some activities may not apply to your organisation). The document also identifies additional technical and organisational measures that, while not considered mandatory for demonstrating compliance with the GDPR, if implemented, may produce additional documentation to help demonstrate compliance.

To get started using this document:

1. Begin by reviewing Part 1, "Overview of Nymity's Privacy Management Accountability Framework™ mapped to the Articles in the GDPR that Require Evidence to Demonstrate Compliance." This will provide you with an outline of the 55 "primary" technical and organisational measures that map to the 39 Articles in the GDPR that require evidence to demonstrate compliance.
2. In Part 2, review all primary technical and organisational measures listed in Column 2.
3. For each mandatory technical and organisational measure, refer to the relevant Article listed in Column 3 and then read the GDPR Article description in Column 4 to determine if the activity applies to your organisation.
4. If the technical and organisational measure applies to your organisation, refer to Column 5 to read how this activity may help your organisation comply with the obligation set out in the Article and see a list of sample evidence to demonstrate compliance.
5. After determining your organisation's "primary" technical and organisational measures and creating your unique organizational Framework for compliance, refer to the additional technical and organisational measures identified that if implemented may produce additional documentation to help demonstrate compliance.

PART 1 Overview of Nymity's Privacy Management Framework™ Mapped to the Articles in the GDPR that Require Evidence to Demonstrate Compliance

Privacy Management Categories	Technical and Organisational Measures	GDPR Article Reference
1. Maintain Governance Structure	Assign responsibility for data privacy to an individual (e.g. Privacy Officer, General Counsel, CPO, CISO, EU Representative)	27
	Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)	
	Appoint a Data Protection Officer (DPO) in an independent oversight role	37, 38
	Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)	
	Maintain roles and responsibilities for individuals responsible for data privacy (e.g. Job descriptions)	39
	Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy	38
	Engage stakeholders throughout the organization on data privacy matters (e.g., information security, marketing, etc.)	
	Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)	
	Report to external stakeholders on the status of privacy management (e.g., regulators, third–parties, clients)	
	Conduct an Enterprise Privacy Risk Assessment	24, 39
	Integrate data privacy into business risk assessments/reporting	
	Maintain a privacy strategy	
	Maintain a privacy program charter/mission statement	
	Require employees to acknowledge and agree to adhere to the data privacy policies	
2. Maintain Personal Data Inventory and Data Transfer Mechanisms	Maintain an inventory of personal data and/or processing activities	30
	Classify personal data by type (e.g. sensitive, confidential, public)	
	Obtain Regulator approval for data processing (where prior approval is required)	
	Register databases with regulators (where registration is required)	

Privacy Management Categories	Technical and Organisational Measures	GDPR Article Reference
	Maintain documentation of data flows (e.g. between systems, between processes, between countries)	
	Maintain documentation of the transfer mechanism used for cross–border data flows (e.g., model clauses, BCRs, Regulator approvals)	45, 46, 49
	Use Binding Corporate Rules as a data transfer mechanism	46, 47
	Use contracts as a data transfer mechanism (e.g., Standard Contractual Clauses)	46
	Use APEC Cross Border Privacy Rules as a data transfer mechanism	
	Use Regulator approval as a data transfer mechanism	46
	Use adequacy or one of the derogations (e.g. consent, performance of a contract, public interest) as a data transfer mechanism	45, 49, 48
	Use the Privacy Shield as a data transfer mechanism	46
3. Maintain Internal Data Privacy Policy	Maintain a data privacy policy	5, 24, 91
	Maintain an employee data privacy policy	
	Document legal basis for processing personal data	6, 9, 10
	Integrate ethics into data processing (Codes of Conduct, policies and other measures)	
	Maintain an organizational code of conduct that includes privacy	
4. Embed Data Privacy Into Operations	Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)	9
	Maintain policies/procedures for collection and use of children and minors' personal data	8, 12
	Maintain policies/procedures for maintaining data quality	5
	Maintain policies/procedures for the de–identification of personal data	89
	Maintain policies/procedures to review processing conducted wholly or partially by automated means	12, 22
	Maintain policies/procedures for secondary uses of personal data	6, 13, 14
	Maintain policies/procedures for obtaining valid consent	6, 7, 8
	Maintain policies/procedures for secure destruction of personal data	
	Integrate data privacy into use of cookies and tracking mechanisms	
	Integrate data privacy into records retention practices	5
	Integrate data privacy into direct marketing practices	21
	Integrate data privacy into e–mail marketing practices	
	Integrate data privacy into telemarketing practices	
	Integrate data privacy into digital advertising practices (e.g., online, mobile)	
	Integrate data privacy into hiring practices	

Privacy Management Categories	Technical and Organisational Measures	GDPR Article Reference
	Integrate data privacy into the organization's use of social media practices	8
	Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures	
	Integrate data privacy into health & safety practices	
	Integrate data privacy into interactions with works councils	
	Integrate data privacy into practices for monitoring employees	
	Integrate data privacy into use of CCTV/video surveillance	
	Integrate data privacy into use of geo–location (tracking and or location) devices	
	Integrate data privacy into delegate access to employees' company e–mail accounts (e.g. vacation, LOA, termination)	
	Integrate data privacy into e–discovery practices	
	Integrate data privacy into conducting internal investigations	
	Integrate data privacy into practices for disclosure to and for law enforcement purposes	
	Integrate data privacy into research practices (e.g., scientific and historical research)	21, 89
5. Maintain Training and Awareness Program	Conduct privacy training	39
	Conduct privacy training reflecting job specific content	
	Conduct regular refresher training	
	Incorporate data privacy into operational training (e.g. HR, marketing, call centre)	
	Deliver training/awareness in response to timely issues/topics	
	Deliver a privacy newsletter, or incorporate privacy into existing corporate communications	
	Provide a repository of privacy information, e.g. an internal data privacy intranet	
	Maintain privacy awareness material (e.g. posters and videos)	
	Conduct privacy awareness events (e.g. an annual data privacy day/week)	
	Measure participation in data privacy training activities (e.g. numbers of participants, scoring)	
	Enforce the Requirement to Complete Privacy Training	
	Provide ongoing education and training for the Privacy Office and/or DPOs	
	Maintain qualifications for individuals responsible for data privacy, including certifications	
6. Manage Information Security Risk	Integrate data privacy risk into security risk assessments	32
	Integrate data privacy into an information security policy	5, 32
	Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)	32
	Maintain measures to encrypt personal data	32

Privacy Management Categories	Technical and Organisational Measures	GDPR Article Reference
	Maintain an acceptable use of information resources policy	
	Maintain procedures to restrict access to personal data (e.g. role–based access, segregation of duties)	32
	Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)	
	Maintain human resource security measures (e.g. pre–screening, performance appraisals)	
	Maintain backup and business continuity plans	
	Maintain a data–loss prevention strategy	
	Conduct regular testing of data security posture	32
	Maintain a security certification (e.g. ISO)	
7. Manage Third–Party Risk	Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)	28, 32
	Maintain procedures to execute contracts or agreements with all processors	28, 29
	Conduct due diligence around the data privacy and security posture of potential vendors/processors	28
	Conduct due diligence on third party data sources	
	Maintain a vendor data privacy risk assessment process	
	Maintain a policy governing use of cloud providers	
	Maintain procedures to address instances of non–compliance with contracts and agreements	
	Conduct due diligence around the data privacy and security posture of existing vendors/processors	
	Review long–term contracts for new or evolving data privacy risks	
8. Maintain Notices	Maintain a data privacy notice	8, 13, 14
	Provide data privacy notice at all points where personal data is collected	13, 14, 21
	Provide notice by means of on–location signage, posters	
	Provide notice in marketing communications (e.g. emails, flyers, offers)	
	Provide notice in contracts and terms	
	Maintain scripts for use by employees to explain or provide the data privacy notice	
	Maintain a privacy Seal or Trustmark to increase customer trust	
9. Respond to Requests and Complaints from Individuals	Maintain procedures to address complaints	
	Maintain procedures to respond to requests for access to personal data	15
	Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data	16, 19

Privacy Management Categories	Technical and Organisational Measures	GDPR Article Reference
	Maintain procedures to respond to requests to opt–out of, restrict or object to processing	7, 18, 21
	Maintain procedures to respond to requests for information	
	Maintain procedures to respond to requests for data portability	20
	Maintain procedures to respond to requests to be forgotten or for erasure of data	17, 19
	Maintain Frequently Asked Questions to respond to queries from individuals	
	Investigate root causes of data protection complaints	
	Monitor and report metrics for data privacy complaints (e.g. number, root cause)	
10. Monitor for New Operational Practices	Integrate Privacy by Design into data processing operations	25
	Maintain PIA/DPIA guidelines and templates	35
	Conduct PIAs/DPIAs for new programs, systems, processes	5, 6, 25, 35
	Conduct PIAs or DPIAs for changes to existing programs, systems, or processes	5, 6, 25, 35
	Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process	35
	Track and address data protection issues identified during PIAs/DPIAs	35
	Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)	36
11. Maintain Data Privacy Breach Management Program	Maintain a data privacy incident/breach response plan	33, 34
	Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol	12, 33, 34
	Maintain a log to track data privacy incidents/breaches	33
	Monitor and Report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)	
	Conduct periodic testing of data privacy incident/breach plan	
	Engage a breach response remediation provider	
	Engage a forensic investigation team	
	Obtain data privacy breach insurance coverage	
12. Monitor Data Handling Practices	Conduct self–assessments of privacy management	25, 39
	Conduct Internal Audits of the privacy program (i.e., operational audit of the Privacy Office)	
	Conduct ad–hoc walk-throughs	
	Conduct ad–hoc assessments based on external events, such as complaints/breaches	
	Engage a third–party to conduct audits/assessments	
	Monitor and report privacy management metrics	
	Maintain documentation as evidence to demonstrate compliance and/or accountability	5, 24

Privacy Management Categories	Technical and Organisational Measures	GDPR Article Reference
	Maintain certifications, accreditations, or data protection seals for demonstrating compliance to regulators	
13. Track External Criteria	Identify ongoing privacy compliance requirements, e.g., law, case law, codes, etc.	39
	Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments	
	Attend/participate in privacy conferences, industry associations, or think–tank events	
	Record/report on the tracking of new laws, regulations, amendments or other rule sources	
	Seek legal opinions regarding recent developments in law	
	Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes	
	Identify and manage conflicts in law	

PART 2 Framework for Demonstrable GDPR Compliance – Detailed Mapping of Nymity's Privacy Management

Explanation of the Framework for GDPR Compliance Table:

Privacy Management Categories	Primary Technical and Organisational Measures (Primary measures are highlighted)	Relevant GDPR Article(s)	Article Description	How the Primary Technical and Organisational Measures may help Achieve Compliance with GDPR Obligations
Identifies the Privacy Management Category in the Nymity Framework™ e.g. Maintain Governance Structure	A list of technical and organisational measures in the Nymity Privacy Management Accountability Framework™. "Mandatory" technical and organisational measures are highlighted and represent those activities that that once implemented may help: 1. Achieve ongoing compliance with the GDPR 2. Produce documentation that will help demonstrate compliance In some cases, the technical and organisational measure may not be applicable for your organisation.	A list of GDPR Article(s) that require evidence to demonstrate compliance, mapped to the specific technical and organisational measure.	A brief annotation explaining the meaning and impact of the Article.	A description of how the technical and organisational measure may help organisations demonstrate compliance with the obligations set out in the related Article(s) and a list of sample evidence to demonstrate compliance.
		The merged columns are not shaded and identify technical and organisational measures that, while not considered mandatory for demonstrating compliance with the GDPR, if implemented, may produce additional documentation to help demonstrate compliance.		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
1. Maintain Governance Structure	**Assign Responsibility for data privacy to an individual (e.g. Privacy Officer, General Counsel, CPO, CISO, EU Representative)**	27	**Article 27** – Representatives of controllers or processors not established in the Union This Article states that in cases where a non–EU Data Controller or Data Processor is offering goods or services (paid or free) to EU data subjects, or is monitoring the behaviour of data subjects within the EU, the Data Controller or processor must designate in writing a representative in the EU. Exceptions apply.	This technical and organisational measure addresses how organisations assign responsibility for the operational aspects of a privacy programme to an individual. Example evidence to demonstrate compliance: 1. Written mandate for the Representative to act on behalf of the controller or processor; or 2. Evidence of communication of the Representative, e.g. within a privacy notice or via a website.
	Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data.		
	Appoint a Data Protection Officer (DPO) in an independent oversight role	37, 38	**Article 37** – Designation of the Data Protection Officer This Article provides that the Data Controller or the Data Processor shall designate a Data Protection Officer ("DPO") in three circumstances. If they:	This technical and organisational measure addresses the appointment of a Data Protection Officer, including assignment of tasks. In order to achieve GDPR compliance, the assignment of responsibility for privacy includes the broader organisation, guaranteeing the independence of the office, funding and resourcing the office, addressing the resolution of conflicts of interest,

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			1. Are a public sector body; 2. Are a body which processes large amounts of special data (Articles 9 & 10); or 3. Undertake large scale, regular & systematic.	and stressing the DPO's responsibility for oversight of all processing activities.
			Additionally, the appointment may be required by specific Union or Member State law. The DPO must have expert knowledge of data protection law. They may be an employee or third party under contract. Their contact details must be published and given to the Supervisory Authority. **Article 38** – Position of the Data Protection Officer. This Article positions the DPO within the organisation, requiring involvement in all issues relating to processing personal data, with sufficient resources, acting in an independent manner, and with direct reporting to the highest management level. They shall also be available to be contacted by data subjects.	Example evidence to demonstrate compliance: 1. Privacy notice including the DPO's contact details; 2. Evidence that the DPO's contact details have been communicated to the Supervisory Authority; 3. Evidence of DPO qualifications, e.g. CV, Certifications; 4. An organisational chart showing the DPO reports to the highest level of management; 5. A job description or mandate for the DPO role; and 6. Budget and resources allocated for the DPO role.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Assign responsibility for data privacy throughout the organisation (e.g. Privacy Network)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data. • **Article 24** – Responsibility of the controller		
	Maintain roles and responsibilities for individuals responsible for data privacy (e.g. Job descriptions)	39	**Article 39** – Tasks of the Data Protection Officer This Article sets out the tasks of the DPO: advise the Controller or Processor and its employees of data protection obligations; monitor compliance, including assigning responsibilities, training and audits; advising on & monitoring DP impact assessments; cooperating and contacting the supervisory authority as required; and reviewing processing risk.	This technical and organisational measure addresses defining the privacy roles in an organisation through job descriptions, by contract or other methods. A job description or mandate for the DPO role addressing the specific tasks set out by Article 39.
	Conduct regular communication between the privacy office, privacy network and others responsible/accountable for data privacy	38	**Article 38** – Position of the Data Protection Officer Article 38 positions the DPO within the organisation, requiring involvement in all issues relating to processing personal data, with sufficient resources, acting in an independent manner, and with direct reporting to the highest	This technical and organisational measure addresses how individuals who are accountable and responsible for data privacy regularly communicate with each other. This communication is essential for the DPO to be involved in all issues relating to the processing of personal data. Example evidence to demonstrate compliance:

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			management level. They shall also be available to be contacted by data subjects.	1. Provide evidence of regular communication between the DPO and stakeholders in the privacy office and throughout the organisation; 2. Meeting agendas and minutes; 3. Membership on committees, boards or working groups; or 4. Workflows or procedures indicating the requirement for DPO involvement in certain processing activities (e.g. DPIAs, vendor selection, complaints).
	Engage stakeholders throughout the organisation on data privacy matters (e.g., Information Security, Marketing, etc.)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
	Report to internal stakeholders on the status of privacy management (e.g. Board of Directors, Management)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
	Report to external stakeholders on the status of privacy management (e.g., Regulators, third-parties, clients)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
	Conduct an Enterprise Privacy Risk Assessment	24, 39	**Article 24** – Responsibility of the controller	This technical and organisational measure enables the privacy office to identify issues and

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			This Article requires the Data Controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR. The appropriateness of these measures is based on a risk assessment that takes into account the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals. There is a specific reference that, where proportionate in relation to the processing activities, data protection policies shall be implemented. **Article 39** – Tasks of the Data Protection Officer This Article sets out the tasks of the DPO including having due regard to the risk associated with processing operations, taking into account the nature, scope, context, and purposes of processing.	risks and determine, based on the likelihood and impact, where to prioritise resources to mitigate the risks. Note that this technical and organisational measure refers to high level risk assessments, not project or initiative-based risk assessments which are addressed in privacy management category 10 - Monitor for New Operational Practices. Example evidence to demonstrate compliance: 1. Enterprise Risk Assessment which includes data privacy; or 2. Privacy Risk Assessment and mitigation plan.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Integrate data privacy into business risk assessments/reporting	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to take into consideration the risks associated with processing operations in the performance of his or her tasks)		
	Maintain a privacy strategy	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data		
	Maintain a privacy charter/mission statement	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data		
	Require employees to acknowledge and agree to adhere to the data privacy policies	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
2.Maintain Personal Data Inventory and Data Transfer Mechanisms	**Maintain an inventory of personal data and/or processing activities**	30	The obligation applies to both controllers and processors. **Article 30** – Records of processing activities This Article sets out a detailed list of information that must be maintained as records of processing activities carried out by and on behalf of the	This technical and organisational measure will help the privacy office develop an inventory of processing activities that addresses the information required to be maintained. 1. A listing of categories of data and data subjects, the purposes for which the data was collected, categories of recipients and the country they are

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			controller, as well as the requirement to make the records available to data subjects and Supervisory Authorities upon request. Exceptions apply.	located in, retention periods, and other details set out in Article 30.
	Classify personal data by type (e.g. sensitive, confidential, public)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 9** – Processing of special categories of personal data		
	Obtain Regulator approval for data processing (where prior approval is required)			
	Register databases with regulators (where registration is required)			
	Maintain documentation of data flows (e.g. between systems, between processes, between countries)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 46** – Transfers subject to appropriate safeguards		
	Maintain documentation of the transfer mechanism used for cross-border data flows (e.g., model clauses, BCRs, Regulator approvals)	45, 46, 49	**Article 45** – Transfers on the basis of an adequacy decision This Article provides that personal data may not be transferred to a third country or international	This technical and organisational measure supports the privacy office managing international data flows and tracking their use of cross–border transfer mechanisms.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			organisation without a specific authorization where the Commission has decided the country or organisation ensures an adequate level of protection. Exceptions apply. **Article 46** – Transfers subject to appropriate safeguards. This Article states that in cases where a third country has not been assessed as providing an adequate level of data protection by the Commission, the Data Controller or processor may transfer personal data to a third country provided there are appropriate safeguards in place, enforceable data subject rights and legal remedies. **Article 49 –** Derogations for specific situations This Article outlines derogations for specific situations and enumerates circumstances in which personal	Example evidence to demonstrate compliance: 1. A personal data inventory which identifies international data transfers and indicates the basis for each transfer; or 2. Evidence of the assessment of non–adequate third countries prior to a transfer.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			data may be transferred to a third country even in the absence of an adequacy decision or other appropriate safeguards. Examples include: • With explicit consent of the data subject; • For performance of a contract or implementation of pre–contractual measures; • For important reasons of public interest; • For establishment, exercise or defence of legal claims; • In order to protect the vital interests of a person; • For transfers made from public registers in certain cases; or • In the compelling legitimate interests of the Data Controller.	
	Use Binding Corporate Rules as a data transfer mechanism	46, 47	**Article 46 –** Transfers subject to appropriate safeguards	This technical and organisational measure addresses the implementation, approval and monitoring of binding corporate rules, which govern data transfers among members of a

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			This Article states that in cases where a third country has not been assessed as providing an adequate level of data protection by the European Commission, the Data Controller or processor may transfer personal data to a third country provided there are in place appropriate safeguards including binding corporate rules. **Article 47** – Binding corporate rules. This Article provides the requirements for approval of binding corporate rules as a data transfer mechanism.	corporate group and can be used as a legal mechanism for international data transfers. Example evidence to demonstrate compliance: 1. Approved binding corporate rules; 2. Results of BCR monitoring activities (e.g. Data Privacy Accountability Scorecard, Audits); or 3. Up to date listing of the scope and coverage of the BCR.
	Use contracts as a data transfer mechanism (e.g., Standard Contractual Clauses)	46	**Article 46** – Transfers subject to appropriate safeguards. This Article states that in cases where a third country has not been assessed as providing an adequate level of data protection by the European Commission, the Data Controller or Processor may transfer personal data to a third country provided there are appropriate safeguards in place such as standard data protection clauses.	This technical and organisational measure addresses the use of Standard Contractual Clauses to facilitate the transfer of personal data to a third country. Example evidence to demonstrate compliance: 1. Contracts with data importers/ exporters that include the Standard Contractual Clauses.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Use APEC Cross Border Privacy Rules as a data transfer mechanism			
	Use Regulator approval as a data transfer mechanism	46	**Article 46** – Transfers subject to appropriate safeguards. This Article states that in cases where a third country has not been assessed as providing an adequate level of data protection by the European Commission, the Data Controller or processor may transfer personal data to a third country provided there are appropriate safeguards in place such as authorisation by a Member State or supervisory authority.	This technical and organisational measure addresses the use of Regulator approval to facilitate the transfer of personal data to a third country. Example evidence to demonstrate compliance: 1. Decisions of the supervisory authority approving the transfer (e.g. approving contractual safeguards in contracts with data importers/ exporters).
	Use adequacy or one of the derogations (e.g. consent, performance of a contract, public interest) as a data transfer mechanism	45, 48, 49	**Article 45** – Transfers on the basis of an adequacy decision This Article provides that personal data may not be transferred to a third country or international organisation without a specific authorization where the Commission has decided the country or organisation ensures an adequate level of protection. Exceptions apply.	This technical and organisational measure addresses relying on derogations to the requirement to send personal data to third countries which provide an "adequate" level of protection for personal data. Example evidence to demonstrate compliance: 1. A personal data inventory which identifies international data transfers and indicates the basis for each transfer;

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			Article 48 – Transfers or disclosures not authorised by Union law This Article addresses when Data Controllers or processors may rely on a court judgment or tribunal decision in order to transfer personal data to a third country. **Article 49** – Derogations for specific situations This Article enumerates derogations for specific situations that may support the transfer of personal data to a third country even in the absence of an adequacy decision or other appropriate safeguards. Among others, examples of derogations include explicit consent of the data subject or for the performance of a contract.	2. Consent forms from data subjects, including an explanation of the possible risk posed by a lack of appropriate safeguards); and 3. An assessment balancing the legitimate interests of the Data Controller against the rights and freedoms of the data subjects.
	Use Privacy Shield as a data transfer mechanism	46	**Article 46** – Transfers subject to appropriate safeguards This article states that in cases where a third country has not been assessed as providing an adequate level of data protection by the	This technical and organisational measure addresses the requirements for using the Privacy Shield as a data transfer mechanism. Sample evidence to demonstrate compliance:

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			European Commission, the Data Controllers or processor may transfer personal data to a third country provided there are in place appropriate safeguards, enforceable data subject rights and legal remedies.	1. Maintain a privacy policy that explicitly refers to the Privacy Shield, contains the relevant contact details and refer to an independent recourse mechanism; or 2. Ensure annual renewal of the self–certification to the Privacy Shield principles.
3.Maintain Internal Data Privacy Policy	**Maintain a data privacy policy**	5, 24, 91	**Article 5** – Principles relating to processing of personal data This Article sets out the general principles that all processing activities must abide by, including: • Lawfulness, fairness and transparency; • Purpose limitation; • Data minimisation; • Accuracy; • Storage or retention limitation; • Integrity and confidentiality; and • Accountability. The accountability principle states that Data Controllers are responsible for and able to demonstrate	This privacy management helps the organisation create and maintain an organisational–level privacy policy to provide guidance to employees regarding the processing and protection of personal data to ensure that such processing aligns with the obligations of the GDPR. Where relevant (Article 91) it will also address specific data processing obligations that apply to organisations such as churches and other religious associations. Example evidence to demonstrate compliance: 1. Privacy policy setting out how the organisation processes personal data; and 2. Where applicable, a copy of the church or religious association's data protection rules or policy.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			compliance with the data processing principles. One of the most notable changes from obligations under the Directive is the explicit requirement to make organisations more accountable for their data practices. **Article 24** – Responsibility of the Controller This Article requires the Data Controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR. The appropriateness of these measures is based on a risk assessment that takes into account the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals. There is a specific reference that, where proportionate in relation to the processing	

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			activities, data protection policies shall be implemented. **Article 91** – Existing data protection rules of churches and religious associations This Article provides that churches and religious associations and communities that apply comprehensive rules relating to processing personal data may continue to apply such rules, provided the rules are brought in line with the GDPR.	
	Maintain an employee data privacy policy	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 13** – Information to be provided where personal data are collected from the data subject • **Article 14** – Information to be provided where personal data have not been obtained from the data subject		
	Document legal basis for processing personal data	6, 9, 10	**Article 6** – Lawfulness of processing This Article provides legal grounds on which personal data can be processed, as well as how to determine when further processing is compatible with the original purposes for processing.	This technical and organisational measure addresses how the organisation determines the legal basis on which processing takes place and ensuring a record of this analysis. Example evidence to demonstrate compliance:

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			Article 9 – Processing of special categories of personal data This article sets out a general prohibition on the processing of sensitive data, followed by legal grounds on which sensitive personal data can be processed. **Article 10** – Processing of personal data relating to criminal convictions and offences This Article provides the legal basis upon which personal data relating to Criminal convictions and offences may be processed.	1. Log for recording the legal basis for processing personal data, including where applicable a detailed log of the provided unambiguous consent; or 2. Results from DPIAs showing how determinations were made balancing the legitimate interests of the Data Controller against the interests or fundamental rights and freedoms of data subjects.
	Integrate ethics into data processing (Codes of Conduct, policies and other measures)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 6** – Lawfulness of processing		
	Maintain an organizational code of conduct that includes privacy	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data		
4.Embed Data Privacy Into Operations	**Maintain policies/procedures for collection and use of**	9	**Article 9** – Processing of special categories of personal data	This technical and organisational measure helps the organisation put in place in place policies and procedures to ensure that that special categories of personal data are processed only in

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	sensitive personal data (including biometric data)		This Article sets out a general prohibition on the processing of special categories of data, followed by legal grounds on which this data can be processed. Special categories of data include: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade–union membership; genetic data; biometric data; data concerning health or sex life; and sexual orientation.	accordance with the legal grounds set out in Article 9. Example evidence to demonstrate compliance: 1. Organisational policy on handling special categories of personal data; 2. Sample data classification guides; 3. Consent forms/evidence of explicit consent; 4. Collective agreements that set out processing of sensitive data of employees; 5. Details or proof that special categories of personal data were obtained from a publicly available source; or 6. Privacy policy language covering the processing of special categories of personal data.
	Maintain policies/procedures for collection and use of children and minors' personal data	8, 12	**Article 8** – Conditions applicable to child's consent in relation to information society services This article states that where the legal basis of consent is being relied on in relation to offering information society services to minors under the age of 16 (or to younger children not younger than 13, if the age threshold is lowered by Member State Law),	This technical and organisational measure helps the organisation put in place certain policies and procedures to ensure that consent is given or authorised by the holder of parental responsibility over the child when information services are offered directly to a child. Example evidence to demonstrate compliance: 1. Policy for obtaining parental consent; or

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			verifiable parental consent must be obtained. **Article 12** – Transparent information, communication and modalities for the exercise of the rights of the data subject This Article requires that when Data Controllers are providing information to data subjects, whether through privacy notices, in communications regarding access, rectification, correction, and objection rights, or as part of breach notifications, the communication must be in a concise, transparent, intelligible, and easily accessible form, use clear and plain language.	2. Evidence of technological method used to obtain parental consent.
	Maintain policies/procedures for maintaining data quality	5	**Article 5** – Principles relating to processing of personal data This Article sets out the general principles that all processing activities must abide by, including: • Lawfulness, fairness and transparency; • Purpose limitation;	This technical and organisational measure relates to putting in place policies and procedures to ensure data is accurate and, where necessary, kept up–to–date, and for data that is inaccurate in light of the purposes for which they are processed, the data is erased or rectified. Example evidence to demonstrate compliance:

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			• Data minimisation; • Accuracy; • Storage or retention limitation; and • Integrity and confidentiality.	Refer to example evidence under the following Articles: • Lawfulness – see Articles 6, 9 and 10; • Transparency – see Articles 13 and 14; • Purpose limitation – see Article 6; • Integrity and confidentiality – see Article 32; • Accountability – see Article 24.
	Maintain policies/ procedures for the de-identification of personal data	89	**Article 89** – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes This Article provides that processing for archiving purposes in the public interest, or for scientific or historical research, or for statistical purposes is subject to appropriate safeguards, including data minimisation. Thus, processing should use pseudonymised or anonymised data to the extent possible.	This technical and organisational measure addresses how organisations put in place a specific technical and organisational measure to ensure respect for the principle of data minimisation. Example evidence to demonstrate compliance: 1. Policies and procedures around data minimisation, pseudonymisation, or anonymisation of data; 2. Research Ethics Board approvals that address data minimisation and privacy protections; and 3. Technical solutions that result in the pseudonymisation or anonymisation of personal data.
	Maintain policies/ procedures to review	12, 22	**Article 22** – Automated individual decision–making, including profiling	This technical and organisational measure supports determining whether processing

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	processing conducted wholly or partially by automated means		This Article addresses the right of data subjects to not be subject to a decision based solely on automated processing, where such decision would have a legal or significant effect concerning him or her. **Article 12** – Transparent information, communication and modalities for the exercise of the rights of the data subject This Article requires that when Data Controllers are providing information to data subjects, whether through privacy notices, in communications regarding access, rectification, correction, and objection rights, or as part of breach notifications, the communication must be in a concise, transparent, intelligible and easily accessible form, use clear and plain language.	activities are captured by the restriction on automated decision–making and presents options for achieving compliance. As part of this activity, Data Controllers must implement measures to safeguard the data subject's rights and freedoms and legitimate interests. These measures (e.g., providing a right to express a point of view and contest the decision) would need to adhere to Article 12's requirements around clarity of communication, time frames and appropriate responses. Example evidence to demonstrate compliance: 1. Policy or procedures related to automated decision–making; 2. Data inventory identifying automated processing and stating a legal basis for such processing; and 3. Evidence of a manual intervention/human check in decision making processes.
	Maintain policies/procedures for secondary uses of personal data	6, 13, 14	**Article 6** – Lawfulness of processing This Article provides for the legal grounds upon which personal data can be processed, as well as how to determine when further processing	This technical and organisational measure addresses having policies and procedures that define how to handle situations when the organisation wishes to use personal data beyond the primary purpose.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			is compatible with the original purposes for processing. **Article 13** – Information to be provided where personal data are collected from the data subject This Article provides that where personal data relating to data subjects are collected, controllers must provide certain minimum information to those data subjects through an information notice. It also sets out requirements for timing of the notice and identifies when exemptions may apply. **Article 14** – Information to be provided where personal data have not been obtained from the data subjects This Article specifies what information is required to be provided to data subjects when that information is not obtained by the controller.	Secondary uses of data must be disclosed in information notices under Article 13 and 14. Example evidence to demonstrate compliance: 1. Log for recording the legal basis for processing personal data.
	Maintain policies/procedures for obtaining valid consent	6, 7, 8	**Article 6** – Lawfulness of processing. This Article provides legal grounds on which personal data can be	This technical and organisational measure addresses the different components that makes consent valid (e.g., freely given, specific and

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			processed including the data subject has given consent to the processing of his or her personal data for one or more specific purposes. **Article 7** – Conditions for Consent This Article sets out the standard for consent when relying on consent as a legal basis for processing personal data (demonstrable consent) and sensitive personal data (explicit consent). **Article 8** – Conditions applicable to child's consent in relation to information society services This Article provides that where the legal basis of consent is being relied on in relation to offering information society services to minors under the age of 16 (or to younger children not younger than 13, if the age threshold is lowered by Member State law), verifiable parental consent must be obtained.	unambiguous) and how to update consent forms and mechanisms to ensure GDPR compliance. Example evidence to demonstrate compliance: 1. Evidence that web forms used opt–in consent check boxes or buttons; 2. Copies of signed consent forms (written or electronic); or 3. Call–centre recordings.
	Maintain policies/procedures for	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with:		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	secure destruction of personal data	• **Article 32** – Security of processing		
	Integrate data privacy into use of cookies and tracking mechanisms	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 21**– Right to object		
	Integrate data privacy into records retention practices	5	**Article 5** – Principles relating to processing of personal data This Article sets out the general principles that all processing activities must abide by, including: • Lawfulness, fairness and transparency; • Purpose limitation; • Data minimisation; • Accuracy; • ***Storage or retention limitation***; • Integrity and confidentiality; and • Accountability.	This technical and organisational measure helps the organisation embed data privacy into the records retention policy and procedure to ensure proper storage of personal data. It helps organisations put in place policies and procedures to ensure data is not kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which it was processed unless the data is being archived for public interest, scientific, statistical, or historical purposes. Example evidence to demonstrate compliance: 1. Records retention policy.
	Integrate data privacy into direct marketing practices		**Article 21** – Right to object This Article addresses the right of data subjects to object to the processing of his or her personal data. The grounds for objecting must	This technical and organisational measure addresses the policies/ procedures that organisations put in place to ensure that the right of the data subject to object to direct marketing are honoured in an organisation's practices respecting direct marketing.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			relate to the particular situation of the data subject and the right to object only applies to processing, including profiling, that is for: • Performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; • Purposes of the legitimate interests pursued by the Data Controller or a third party; • ***Direct marketing purposes***; or • Scientific or historical research or statistical purposes.	Example evidence to demonstrate compliance: 1. Internal guidance for analysing and responding to data subject objections to processing.
	Integrate data privacy into e-mail marketing practices	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 21** – Right to object		
	Integrate data privacy into telemarketing practices	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 21** – Right to object		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Integrate data privacy into digital advertising practices (e.g., online, mobile)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 21** – Right to object		
	Integrate data privacy into hiring practices	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 9** – Processing of special categories of personal data • **Article 10** – Processing of personal data relating to criminal convictions and offences		
	Integrate data privacy into the organization's use of social media practices	8	**Article 8** – Conditions applicable to child's consent in relation to information society services This Article provides that where the legal basis of consent is being relied on in relation to offering information society services to minors under the age of 16 (or to younger children not younger than 13, if the age threshold is lowered by Member State law), consent must be obtained by the holder of parental responsibility over the child.	This technical and organisational measure addresses how the organisation uses social media to collect and disseminate information. Policies around social network use may address the collection and processing of personal data for children and minors to ensure such collection and processing adheres to the GDPR requirement that such consent be obtained by the holder of parental responsibility over the child. Example evidence to demonstrate compliance: 1. Online Privacy and Data Use Policy; 2. Policy for obtaining and documenting parental consent; 3. Social Media Privacy and Confidentiality Policy; or 4. Guidelines for authorized social media users.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 21** – Right to object • **Article 32** – Security of processing		
	Integrate data privacy into health & safety practices	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data		
	Integrate data privacy into practices for monitoring employees	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 6** – Lawfulness of processing • **Article 21** – Right to object		
	Integrate data privacy into use of CCTV/video surveillance	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 6** – Lawfulness of processing • **Article 21** – Right to object		
	Integrate data privacy into use of geo-location (tracking and or location) devices	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 6** – Lawfulness of processing • **Article 21** – Right to object		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Integrate data privacy into delegated access to employees' company e-mail accounts (e.g. vacation, LOA, termination)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 6** – Lawfulness of processing • **Article 21** – Right to object		
	Integrate data privacy into e-discovery practices	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 6** – Lawfulness of processing • **Article 21** – Right to object		
	Integrate data privacy into conducting internal investigations	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 6** – Lawfulness of processing • **Article 21** – Right to object		
	Integrate data privacy into practices for disclosure to and for law enforcement purposes	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 6** – Lawfulness of processing • **Article 21** – Right to object		
	Integrate data privacy into research practices (e.g., scientific and historical research)	21, 89	**Article 21** – Right to object This Article addresses the right of data subjects to object to the processing of his or her personal data. The grounds for objecting must relate to the particular situation of the data subject and the right to object only applies to processing,	This technical and organisational measure generally deals with how an organization maintains procedures for research practices including processes to obtain personal data for research purposes, ensuring valid consents are obtained, de–identifying data where possible, and taking measures to ensure that research data maintained for scientific, historical or

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			including profiling that is for scientific or historical research or statistical purposes. **Article 89** – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes This Article provides that processing for archiving purposes in the public interest, or for scientific or historical research, or for statistical purposes is subject to appropriate safeguards, including data minimisation. Thus, processing should use pseudonymised or anonymised data to the extent possible.	statistical research is safeguarded against improper use.
5. Maintain Training and Awareness Program	**Conduct privacy training**	39	**Article 39** –Tasks of the Data Protection Officer This Article sets out the tasks of the DPO which include the obligation to provide awareness–raising and training of staff involved in processing operations.	This privacy management addresses the need for the DPO to provide awareness–raising and training of staff involved in processing operations and implementing such activities would produce documentation that could serve as evidence of compliance with this requirement. Example evidence to demonstrate compliance:

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
				1. Documentation showing the content and delivery of a training and awareness programme.
	Conduct privacy training reflecting job specific content	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and provide training to staff involved in processing operations)		
	Conduct regular refresher training	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and provide training to staff involved in processing operations)		
	Incorporate data privacy into operational training (e.g. HR, Marketing, Call Centre)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and provide training to staff involved in processing operations)		
	Deliver training/awareness in response to timely issues/topics	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and provide training to staff involved in processing operations)		
	Deliver a privacy newsletter, or incorporate privacy into existing corporate communications	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and to staff involved in processing operations)		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Provide a repository of privacy information, e.g., an internal data privacy intranet	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and to staff involved in processing operations)		
	Maintain privacy awareness material (e.g. posters and videos)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and to staff involved in processing operations)		
	Measure participation in data privacy training activities (e.g. numbers of participants, scoring)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and to staff involved in processing operations)		
	Enforce the Requirement to Complete Privacy Training	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and to staff involved in processing operations)		
	Provide ongoing education and training for the Privacy Office and/or DPOs)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and to staff involved in processing operations)		
	Maintain qualifications for individuals responsible for data privacy, including certifications	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with:		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
		• **Article 39** – Tasks of the Data Protection Officer (requiring the DPO to raise awareness and to staff involved in processing operations)		
6. Manage Information Security Risk	**Integrate data privacy risk into security risk assessments**	32	**Article 32** – Security of processing This Article states that organisations must implement an "appropriate" level of security based on the state of the art and costs of implementation, processing activities, ***and risk of varying likelihood and severity to individuals' rights and freedoms***.	This technical and organisational measure addresses the role of the privacy officer in ensuring privacy and data protection are taken into account as part of security risk assessments. Example evidence to demonstrate compliance: 1. DPIAs or other form or security risk assessment that demonstrates measures were based on an assessment of risk.
	Integrate data privacy into an information security policy	5, 32	**Article 5** – Principles relating to processing of personal data This Article sets out the general principles that all processing activities must abide by, including: • Lawfulness, fairness and transparency; • Purpose limitation; • Data minimisation; • Accuracy; • Storage or retention limitation; • Integrity and confidentiality; and	This technical and organisational measure helps the privacy office insert privacy and data protection consideration into the information security policy. Example evidence to demonstrate compliance: 1. Information security programme policies and procedures; or 2. Details of security measures that are in place.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			• Accountability. **Article 32** – Security of processing This Article states that organisations must implement an "appropriate" level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms.	
	Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)	32	**Article 32** – Security of processing The GDPR requires organisations to implement an "appropriate" level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms. Examples are provided of measures that might be appropriate depending on the level of risk including regular tests of the effectiveness of security measures.	This technical and organisational measure helps the privacy office assess what technical security measures are in place to ensure an appropriate level of security based on the considerations set out in Article 32. Example evidence to demonstrate compliance: 1. Details of security measures that are in place; or 2. Policy on review and update of technical security measures.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Maintain measures to encrypt personal data	32	**Article 32** – Security of processing The GDPR requires organisations to implement an "appropriate" level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms. Examples are provided of measures that might be appropriate depending on the level of risk including encryption (32.1.a)	This technical and organisational measure helps the privacy office put in place encryption practices as an appropriate technical and organisational measure to ensure an appropriate level of security.
	Maintain an acceptable use of information resources policy	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 32** – Security of processing		
	Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)	32	**Article 32** – Security of processing The GDPR requires organisations to implement an "appropriate" level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms.	This technical and organisational measure helps the organisation address how organisations restrict access to personal data to those employees and users who have a legitimate business need to access the data. Example evidence to demonstrate compliance: 1. Contracts with employees and contractors limit the processing of personal data;

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
				2. Register of employees and contractors detailing access rights to IT systems and data; or 3. Audits of access to personal data to determine if existing procedures are appropriate based on the purpose for which the data was collected and the nature of the access.
	Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 32** – Security of processing		
	Maintain human resource security measures (e.g. pre-screening, performance appraisals)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 32** – Security of processing		
	Maintain backup and business continuity plans	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 32** – Security of processing		
	Maintain a data-loss prevention strategy	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 32** – Security of processing		
	Conduct regular testing of data security posture	32	**Article 32** – Security of processing This Article requires an "appropriate" level of security including a process for regularly	This technical and organisational measure helps the organisation address the requirement to put in place a technical or organisational measure to ensure the security of the processing of personal data.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			testing, assessing and evaluating the effectiveness of technical organisational measures for ensuring the security of the processing (32.1.d).	
	Maintain a security certification (e.g., ISO)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 32** – Security of processing		
7. Manage Third–Party Risk	**Maintain data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates)**	28, 32	**Article 28** – Processor This Article creates an obligation on Data Controllers to only outsource processing to those entities that have sufficient guarantees to implement appropriate measures to guarantee GDPR compliance and to have a contract or binding act that governs the relationship. The contents of such a contract are set out. The Article also limits the ability of processors to subcontract without consent of the Data Controller, and what guarantees need to be in place in this arrangement.	This technical and organisational measure helps the organisation determine what data protection requirements are needed for contracts with third–parties who receive and use the personal data on behalf of the organisation. Example evidence of compliance: 1. Screening questions for potential vendors and other processors; 2. Privacy and security contractual clauses (inserted data processing agreements); 3. Data protection questionnaire for outsourcing personal data processing; 4. Vendor data protection risk assessment scorecard; 5. Contractor data protection requirements.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			Article 32 – Security of Processing This Article requires an "appropriate" level of security and also requires that any person with access to personal data only processes such data in accordance with instructions from the Data Controller.	6. Adherence of the processor to an approved code of conduct or certification mechanism; or 7. Agreements with contractors or vendors that include the standard contractual clauses.
	Maintain procedures to execute contracts or agreements with all processors	28, 29	**Article 28** – Processor This Article creates an obligation on Data Controllers to only outsource processing to those entities that have sufficient guarantees to implement appropriate measures to guarantee GDPR compliance and to have a contract or binding act that governs the relationship. The contents of such a contract are set out. The Article also limits the ability of processors to subcontract without consent of the Data Controller, and what guarantees need to be in place in this arrangement.	This technical and organisational measure addresses steps taken to ensure written or electronic contracts are in place with processors. Example evidence of compliance: 1. Data processing agreements or contracts that show consistency with legal obligations and privacy risk management activities; 2. Adherence of the processor to an approved code of conduct or certification mechanism; or 3. Standard contractual clauses between the controller and processor.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			Article 29 – Processor This Article indicates that processors and staff of controllers and processors must only process personal data in accordance with either Data Controller instructions or a requirement of Union or Member State law.	
	Conduct due diligence around the data privacy and security posture of potential vendors/processors	28	**Article 28** – Processor This Article creates an obligation on Data Controllers to only outsource processing to those entities that have sufficient guarantees to implement appropriate measures to guarantee GDPR compliance.	This privacy management addresses that requirement that due diligence is necessary as part of ensuring that processing is only done by entities with sufficient data protection guarantees. Example evidence of compliance: 1. Checklist of screening questions for potential vendors and processors; 2. Vendor privacy questionnaire; or 3. Vendor privacy risk assessment scorecard.
	Conduct due diligence on third party data sources	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 28** – Processor (requiring Data Controllers to use only processors providing sufficient guarantees)		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Maintain a vendor data privacy risk assessment process	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 28** – Processor (requiring Data Controllers to use only processors providing sufficient guarantees)		
	Maintain a policy governing use of cloud providers	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 28** – Processor (requiring Data Controllers to use only processors providing sufficient guarantees)		
	Maintain procedures to address instances of non–compliance with contracts and agreements	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 28** – Processor (requiring Data Controllers to use only processors providing sufficient guarantees)		
	Conduct due diligence around the data privacy and security posture of existing vendors/processors	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 28** – Processor (requiring Data Controllers to use only processors providing sufficient guarantees)		
	Review long–term contracts for new or evolving data privacy risks	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 28** – Processor (requiring Data Controllers to use only processors providing sufficient guarantees)		
8. Maintain Notices	**Maintain a data privacy notice**	8, 13, 14	**Article 8** provides that where the legal basis of consent is being relied on in relation to offering information society services to minors under the	This technical and organisational measure ensures that controllers put in place policies and procedures to ensure that the required

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			age of 16 (or to younger children not younger than 13, if the age threshold is lowered by Member State Law), verifiable parental consent must be obtained. **Article 13** – Information to be provided where personal data are collected from the data subject This Article provides that where personal data relating to data subjects are collected, controllers must provide certain minimum information to those data subjects through an information notice. It also sets out requirements for timing of the notice and identifies when exemptions may apply. **Article 14** – Controllers obligations to provide notice where personal data have not been obtained from the data subject Article 14 specifies what information is required to be provided to data subjects when that information is not obtained by the controller.	information is provided to data subjects when their information is collected. Example evidence to demonstrate compliance: 1. Copy of the information notice provided to data subjects; or 2. Documentation showing that privacy notice is aligned to legal requirements.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Provide data privacy notice at all points where personal data is collected	13, 14, 21	**Article 13** – Information to be provided where personal data are collected from the data subject This Article provides that where personal data relating to data subjects are collected, controllers must provide certain minimum information to those data subjects through an information notice. It also sets out requirements for timing of the notice and identifies when exemptions may apply. **Article 14** – Controllers obligations to provide notice where personal data have not been obtained from the data subject Article 14 specifies what information is required to be provided to data subjects when that information is not obtained by the controller. **Article 21** – Right to object This Article addresses the right of data subjects to object to the processing of his or her personal data.	This technical and organisational measure addresses how an organisation provides an opportunity for data subjects to review the organisations privacy notice at the point of data collection. Example evidence to demonstrate compliance: 1. Details on the placement and timing of the notice.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Provide notice by means of on–location signage, posters	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 13** – Information to be provided where personal data are collected from the data subject • **Article 14** – Information to be provided where personal data have not been obtained from the data subject		
	Provide notice in marketing communications (e.g. emails, flyers, offers)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 13** – Information to be provided where personal data are collected from the data subject • **Article 14** – Information to be provided where personal data have not been obtained from the data subject		
	Provide notice in contracts and terms	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 13** – Information to be provided where personal data are collected from the data subject • **Article 14** – Information to be provided where personal data have not been obtained from the data subject		
	Maintain scripts for use by employees to explain or provide the data privacy notice	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 13** – Information to be provided where personal data are collected from the data subject • **Article 14** – Information to be provided where personal data have not been obtained from the data subject		
	Maintain a privacy Seal or Trustmark to increase customer trust	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 13** – Information to be provided where personal data are collected from the data subject		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
		• **Article 14** – Information to be provided where personal data have not been obtained from the data subject		
	Maintain procedures to address complaints	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 15** – Right of access by the data subject • **Article 16** – Right to rectification • **Article 17** – Right to erasure ('right to be forgotten') • **Article 18** – Right to restriction of processing • **Article 19** – Notification obligation regarding rectification or erasure of personal data or restriction of processing • **Article 20** – Right to data portability		
9. Respond to Requests and Complaints from Individuals	**Maintain procedures to respond to requests for access to personal data**	15	**Article 15** – Right of access by the data subject This Article addresses the right of data subjects to: obtain confirmation of whether their personal is being processed, where it is being processed and have access to the data. Additionally, it lists further information that should be supplied: • Purpose of processing; • Categories of data; • Recipients of data; • Data storage period; • Rights to rectification & complaint;	This technical and organisational measure addresses the primary process and procedures needed to ensure that an organisation can respond to access requests in a timely and appropriate manner, providing the data held on the data subject. If implanted this activity may demonstrate that the right to access is understood and provided for. Example evidence to demonstrate compliance: 1. Protocol or procedure for responding to access requests in a timely manner; 2. Form for the supply of additional data required for access requests; or 3. Log of recording access requests.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			• Source of data; • Existence of automated processing, associated logic and consequences; and • Safeguards for transfer to third countries or international organisations. Exception may apply (Article 23)	
	Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data	16, 19	**Article 16** – Right to rectification This Article addresses the right of data subjects to obtain rectification of inaccurate data or completion of incomplete data. **Article 19** – Notification obligation regarding rectification or erasure of personal data or restriction of processing This Article creates an obligation to notify each recipient to whom data has been disclosed of any rectification, erasure or restriction of processing. There is also an obligation to provide information to the data subject about these recipients upon request. Exception may apply (Article 23)	This technical and organisational measure helps put in place mechanisms to ensure that appropriate corrections to records of personal data are made in a timely and effective manner. Example evidence to demonstrate compliance: 1. Protocol or procedure for responding to rectification requests in a timely manner.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Maintain procedures to respond to requests to opt–out of, restrict or object to processing	7, 18, 21	**Article 7** – Conditions for consent This Article sets out the standard for consent when relying on consent as a legal basis for processing personal data (demonstrable consent) and sensitive personal data (explicit consent). **Article 18** – Right to restriction of processing This Article addresses the right of a data subject to obtain a restriction (i.e., marking stored personal data for the purpose of limiting their processing in the future) on the processing of personal data in cases such as pending verification of a legal ground to process or where accuracy of the data is disputed. **Article 21** – Right to object This Article addresses the right of data subjects to object to the processing of his or her personal data. Exception may apply (Article 23)	Implementing this technical and organisational measure will help organisations put in place processes to ensure that records of personal data are used in line with any restrictions as well as, including not only uses by the Data Controller but also any restrictions on use by downstream recipients. Example evidence to demonstrate compliance: 1. Policy or procedure for responding to requests to restrict processing of data in a timely manner; or 2. Guidance for analysing and responding to data subject objections to processing (e.g. operating procedures or technical processes).

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Maintain procedures to respond to requests for information	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 24** – Responsibility of the controller		
	Maintain procedures to respond to requests for data portability	20	**Article 20** – Right to data portability This Article provides data subjects with a right to, in certain circumstances, receive personal data concerning him or her, in a structured and commonly used and machine–readable format, and to transmit such data to another Data Controller.	This technical and organisational measure addresses the concept of data portability and how to operationalise that concept within the organisation. Example evidence to demonstrate compliance: 1. Procedure or technical process for handling data portability requests.
	Maintain procedures to respond to requests to be forgotten or for erasure of data	17, 19	**Article 17** – Right to erasure ('right to be forgotten') This Article addresses the right of data subjects to obtain from the Data Controller the erasure of personal data based on certain grounds **Article 19** – Notification obligation regarding rectification or erasure of personal data or restriction of processing	This technical and organisational measure outlines possible steps to take when assessing requests for erasure, and the subsequent actions necessary when a request is granted. Example evidence to demonstrate compliance: 1. Protocol or procedure for responding to right to be forgotten / erasure requests.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			This Article creates an obligation to notify each recipient to whom data has been disclosed of any rectification, erasure or restriction of processing. There is also an obligation to provide information to the data subject about these recipients upon request. Exception may apply (Article 23)	
	Maintain Frequently Asked Questions to respond to queries from individuals	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 15** – Right of access by the data subject • **Article 16** – Right to rectification • **Article 17** – Right to erasure ('right to be forgotten') • **Article 18** – Right to restriction of processing • **Article 19** – Notification obligation regarding rectification or erasure of personal data or restriction of processing • **Article 20** – Right to data portability		
	Investigate root causes of data protection complaints	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 15** – Right of access by the data subject • **Article 16** – Right to rectification • **Article 17** – Right to erasure ('right to be forgotten') • **Article 18** – Right to restriction of processing		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
		• **Article 19** – Notification obligation regarding rectification or erasure of personal data or restriction of processing • **Article 20** – Right to data portability		
	Monitor and report metrics for data privacy complaints (e.g. number, root cause)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 15** – Right of access by the data subject • **Article 16** – Right to rectification • **Article 17** – Right to erasure ('right to be forgotten') • **Article 18** – Right to restriction of processing • **Article 19** – Notification obligation regarding rectification or erasure of personal data or restriction of processing • **Article 20** – Right to data portability		
10. Monitor for New Operational Practices	**Integrate Privacy by Design into data processing operations**	25	**Article 25** – Data protection by design and by default The GDPR introduces responsibilities for the controller and requires data protection by design and by default. Data Controllers must, at the time of determining the means of processing as well as when actually processing, implement appropriate technical and organisational measures (e.g., pseudonymisation) to implement the data protection principles set out in **Article 5** (such as data minimisation) and integrate	This technical and organisational measure addresses frameworks to help engineers and application developers embed privacy–protective mechanisms into the fundamental design of processing activities. Example evidence to demonstrate compliance: 1. Policies and procedures demonstrating that privacy requirements shall be included in the technical specifications of new IT tools 2. DPIAs demonstrating that the necessary safeguards were integrated into the data processing;

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			necessary safeguards into the processing to meet the GDPR requirements. Data Controllers must also implement data protection by default, i.e. implement appropriate technical and organisational measures to ensure that, by default, only personal data necessary for each specific purpose are processed. The concept of "necessary" informs the amount of data collected, extent of processing, and retention and accessibility of data.	3. Incorporating data protection by design principles into: a) IT systems; b) accountable business practices; and c) physical design and networked infrastructure; or 4. Policies, procedures, methodologies, and other measures for anonymizing or pseudonymizing data.
	Maintain PIA/DPIA guidelines and templates	35	**Article 35** – Data protection impact assessment This Article requires Data Controllers to assess the impact of processing operations on the protection of personal data where the processing is likely to result in a high risk for the rights and freedoms of data subjects. When carrying out the DPIA, the controller must seek the advice of the Data Protection Officer (when designated). DPIAs should contain:	This technical and organisational measure addresses guidelines on how to conduct a DPIA to analyse the processing of personal data and determine risks to such personal data. It helps organisations ask questions during the development of their processing programs to take into account the available technology, cost of implementation, nature, scope, context, and purposes of processing, and measures that could be applied to protect the rights of data subjects (e.g., pseudonymisation). Example evidence to demonstrate compliance: DPIA templates covering required content;

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			• A description of the processing activities being assessed; • An assessment of the risks to data subjects; and • A description of the measures the controller will take to address these risks, including the safeguards, security measures and mechanisms that the controller will implement to ensure compliance with the GDPR. If the risks posed by the processing change, a review must be conducted to assess whether processing still complies with the DPIA	Guidelines, policies or assessments around when DPIAs are required; Officer's opinion and advice was sought as part of the DPIA process; Evidence that consultations were held with affected populations or their representatives where appropriate (e.g., advocates, community groups); Assessments/reviews of processing activities in light of new or changes to risks; or Guidelines and policies on when to reach out to the data protection authorities to assess risk mitigation.
	Conduct PIAs/DPIAs for new programs, systems, processes	5, 6, 25, 35	**Article 5** – Principles relating to processing of personal data This Article sets out the general principles that all processing activities must abide by including: • Lawfulness, fairness and transparency;	This technical and organisational measure addresses guidelines on when a DPIA is required as part of the development process for new processing. Example evidence to demonstrate compliance:

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			• Purpose limitation; • Data minimisation; • Accuracy; • Storage or retention limitation; • Integrity and confidentiality; and • Accountability **Article 6** – Lawfulness of processing This Article provides legal grounds on which personal data can be processed, as well as how to determine when further processing is compatible with the original purposes for processing. **Article 25** – Data protection by design and by default This Article introduces responsibilities for the controller and requires data protection by design and by default. **Article 35** – Data protection impact assessment	1. DPIAs demonstrating that the necessary safeguards were integrated into the data processing; 2. Results from DPIAs showing how determinations were made balancing the legitimate interests of the Data Controller against the interests or fundamental rights and freedoms of data subjects; 3. Guidelines, policies or assessments around when DPIAs are required; 4. Evidence that the Data Protection Officer's opinion and advice was sought as part of the DPIA process; 5. Evidence that consultations were held with affected populations or their representatives where appropriate (e.g., advocates, community groups); or 6. Assessments/reviews of processing activities in light of new or changes to risks.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			This Article requires Data Controllers to assess the impact of processing operations on the protection of personal data where the processing is likely to result in a high risk for the rights and freedoms of data subjects.	
	Conduct PIAs or DPIAs for changes to existing programs, systems, or processes	5, 6, 25, 35	**Article 5** – Principles relating to processing of personal data This Article sets out the general principles that all processing activities must abide by, including: • Lawfulness, fairness and transparency; • Purpose limitation; • Data minimisation; • Accuracy; • Storage or retention limitation; • Integrity and confidentiality; and • Accountability. **Article 6** – Lawfulness of processing This Article provides legal grounds on which personal data can be processed, as well as how to determine when further processing	This technical and organisational measure addresses having policies and procedures to follow when there is a change to existing processes, programs or systems to ensure that data protection risks are measured, analysed and mitigated. Example evidence to demonstrate compliance: DPIA templates covering required content; 1. Guidelines, policies or assessments around when DPIAs are required; 2. Evidence that the Data Protection Officer's opinion and advice was sought as part of the DPIA process; 3. Evidence that consultations were held with affected populations or their representatives where appropriate (e.g., advocates, community groups); or 4. Assessments/reviews of processing activities in light of new or changes to risks. DPIAs demonstrating that the

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			is compatible with the original purposes for processing. **Article 25** – Data protection by design and by default	necessary safeguards were integrated into the data processing.
	Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process	35	**Article 35.9** – states that, where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.	This technical and organisational measure helps the organisation develop guidance on how to consult with external parties as part of the DPIA process. Example evidence to demonstrate compliance: 1. Evidence that consultations were held with affected populations or their representatives where appropriate (e.g., advocates, community groups).
	Track and address data protection issues identified during PIAs/DPIAs	35	**Article 35** – Data Protection Impact Assessment This Article requires Data Controllers to assess the impact of processing operations on the protection of personal data where the processing is likely to result in a high risk for the rights and freedoms of data subjects.	This technical and organisational measure ensures the organisation treats similar data protection issues consistently and allows for learning from one PIA/DPIA to be applied to subsequent PIAs/DPIAs. Example evidence to demonstrate compliance:
	Report PIA/DPIA analysis and results to regulators (where required) and	36	**Article 36** – Prior consultation	This technical and organisational measure addresses when and how to report PIAs/DPIAs to supervisory authorities. Determinations around

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	external stakeholders (if appropriate)		This Article requires Data Controllers to consult with the supervisory authority when a PIA indicates that processing would result in a high risk to data subjects and lists the minimum information the Data Controller needs to provide to the supervisory authority.	whether such reporting is required and documentation that consultations were executed would demonstrate compliance with the GDPR. Example evidence to demonstrate compliance: 1. DPIAs identifying high risk processing; or 2. Correspondence with the supervisory authority seeking advice regarding the intended processing. Responses from the supervisory authority providing advice regarding the processing.
11. Maintain Data Privacy Breach Management Program	**Maintain a data privacy incident/breach response plan**	33, 34	**Article 33** – Notification of a personal data breach to the supervisory authority This Article makes it mandatory to notify supervisory authorities in the event of a data breach that poses a "risk of harm". The notification is expected without undue delay and where feasible within 72 hours. As well, detailed content requirements are set out for the notification letter.	This technical and organisational measure helps organisations create a breach response infrastructure that will facilitate compliance with the specific requirements under Article 33 respecting timing requirements for notification and the content of a notification letter. It further ensures that recordkeeping requirements are captured. Example evidence to demonstrate compliance: 1. Incident and breach response protocol; 2. Contact list for breach response team; 3. Breach notification letters;

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			The circumstances of the data breaches must also be documented. **Article 34** – Communication of a personal data breach to the data subject This Article requires notification to data subjects of breaches that result in a "high risk" for the rights and freedoms of individuals.	4. Log for recording data protection incidents and breaches; 5. Incident summary form; or 6. Information loss report and management form.
	Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol	12, 33, 34	**Article 12** – Transparent information, communication and modalities for the exercise of the rights of the data subject This Article requires that when Data Controllers are providing information to data subjects as part of breach notifications, the communication must be in a concise, transparent, intelligible, and easily accessible form, use clear and plain language. Information may be provided in writing, electronically (where appropriate), or orally (as long as identity of the data subject is verified).	This technical and organisational measure helps the organisation identify items that need to be addressed in determining timing and content of notifications to DPAs. Example evidence to demonstrate compliance: 1. Contact list for breach response team; 2. Breach notification letters; or 3. Notification protocols that provide for notification to DPAs and individuals in the event a high risk of harm is found to exist.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			Article 33 – Notification of a personal data breach to the supervisory authority This Article makes it mandatory to notify supervisory authorities in the event of a data breach that poses a "risk of harm". The notification is expected without undue delay and where feasible within 72 hours. As well, detailed content requirements are set out for the notification letter. The circumstances of the data breaches must also be documented. **Article 34 –** Communication of a personal data breach to the data subject This Article requires notification to data subjects of breaches that result in a "high risk" for the rights and freedoms of individuals. Template letters.	
	Maintain a log to track data privacy incidents/breaches	33	**Article 33.5** – States that the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the	This technical and organisational measure helps the organisation address the specific requirement under Article 33.5 requiring that a controller document personal data breaches. Example evidence to demonstrate compliance:

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.	1. Log for recording data protection incidents and breaches; 2. Incident summary form; or 3. Information loss report and management form.
	Conduct periodic testing of data privacy incident/breach plan	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 33** – Notification of a personal data breach to the supervisory authority		
	Engage a breach response remediation provider	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 33** – Notification of a personal data breach to the supervisory authority		
	Engage a forensic investigation team	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 33** – Notification of a personal data breach to the supervisory authority		
	Obtain data privacy breach insurance coverage			
12. Monitor Data Handling Practices	**Conduct self–assessments of privacy management**	24, 39	**Article 24** –Responsibility of the controller This Article requires the Data Controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR.	This technical and organisational measure helps the privacy office establish a procedure to ensure the ability to demonstrate that appropriate technical and organisational measures have been put in place for compliance with the GDPR. Example evidence to demonstrate compliance: 1. Readiness Assessments; or

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			Article 39 – Tasks of the DPO This Article sets out the tasks of the DPO including: advise the Controller or Processor and its employees of data protection obligations; monitor compliance, including assigning responsibilities, training and audits; advising on & monitoring DP impact assessments, cooperating and contacting the supervisory authority as required, and reviewing processing risk.	2. Data Privacy Accountability Scorecard.
	Conduct Internal Audits of the privacy program (i.e., operational audit of the Privacy Office)	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
	Conduct ad–hoc walk-throughs	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
	Conduct ad–hoc assessments based on external events, such as complaints/breaches	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Engage a third–party to conduct audits/assessments	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
	Monitor and report privacy management metrics	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
	Maintain documentation as evidence to demonstrate compliance and/or accountability	5, 24	**Article 5** – Principles relating to processing of personal data This Article sets out the general principles that all processing activities must abide by, including: • Lawfulness, fairness and transparency; • Purpose limitation; • Data minimisation; • Accuracy; • Storage or retention limitation; • Integrity and confidentiality; and • Accountability.	This technical and organisational measure supports the organisation creating a process for maintaining documentation of the technical and organisational measures it has put in place in order to demonstrate compliance with the GDPR. Example evidence to demonstrate compliance: 1. Register of all data processing operations within the organisation, including underlying decisions on interpretation of the relevant legal provisions and grounds for processing.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
			The accountability principle states that Data Controllers are responsible for and able to demonstrate compliance with the data processing principles. **Article 24** – Responsibility of the Data Controller This Article requires the Data Controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR.	
	Maintain certifications, accreditations, or data protection seals for demonstrating compliance to regulators	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the controller		
13. Track External Criteria	**Identify ongoing privacy compliance requirements, e.g., law, case law, codes, etc.**	39	**Article 39 –**Tasks of the DPO This Article sets out the tasks of the DPO which include an obligation to monitor compliance with the GDPR and with other Union or Member State data protection provisions.	This technical and organisational measure addresses how the DPO conducts research regularly to maintain expert knowledge with respect to privacy and data protection law and practices and to determine what, if any, changes to the privacy program need to be made as a result of any legal or regulatory developments.

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
				Example evidence to demonstrate compliance: 1. Subscriptions (free or paid) to privacy law research reporting services; 2. Certification of attendance at privacy and data protection conferences; or 3. Evidence of consultations with law firms.
	Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** –Tasks of the DPO		
	Attend/participate in privacy conferences, industry associations, or think–tank events	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** –Tasks of the DPO		
	Record/report on the tracking of new laws, regulations, amendments or other rule sources	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** –Tasks of the DPO		
	Seek legal opinions regarding recent developments in law	While not considered mandatory for demonstrating compliance with the GDPR, if implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with: • **Article 39** –Tasks of the DPO		

Privacy Management Categories	Technical and organisational measures (Mandatory Privacy management Activities are highlighted)	Relevant GDPR Article(s)	Article Description	How the Mandatory Technical and Organisational Measure may help Achieve Compliance with GDPR Obligations
	Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes	If implemented, this technical and organisational measure may produce additional documentation to help demonstrate compliance with the following Articles: • **Article 39 –**Tasks of the DPO • **Article 35** – Data Protection Impact Assessment • **Article 5** – Principles relating to processing of personal data • **Article 24** – Responsibility of the Controller		
	Identify and manage conflicts in law	• **Article 39 –**Tasks of the DPO		