
Definitions


Overview


Purpose


Scope


Applicable Laws


Roles and Responsibilities


Data Protection Principles


Legal Basis for Processing


Right of Individuals


Transfer of Personal Data


Privacy by Design and Default


Records of Processing Activities


Data Breach Response


Training and Awareness


Related Documents


Policy Ownership and Maintenance

M2

GROUP DATA PROTECTION POLICY

Owner	Group Legal Department
Version	2.0
Effective Date	October 2025
Next Review	October 2026
Classification	Public
Approver	Board of Directors
Applies to	M42 Ltd and its subsidiaries

Table of Contents

1. DEFINITIONS 3
2. OVERVIEW 4
3. PURPOSE 4
4. SCOPE 5
5. APPLICABLE LAWS 5
6. ROLES AND RESPONSIBILITIES 6
7. DATA PROTECTION PRINCIPLES 7
8. LEGAL BASES FOR PROCESSING 8
9. RIGHTS OF INDIVIDUALS 8
10. TRANSFER OF PERSONAL DATA 10
11. PRIVACY BY DESIGN AND DEFAULT 11
12. RECORDS OF PROCESSING ACTIVITIES 11
13. DATA BREACH RESPONSE 12
14. TRAINING AND AWARENESS 12
15. RELATED DOCUMENTS 13
16. POLICY OWNERSHIP AND MAITENANCE 13

ANNEX 1 – USE CASES 15

PART I: INTRODUCTION

1. DEFINITIONS

Applicable Data Protection Laws	The privacy laws that M42 must follow where applicable - including the UAE Data Protection Law (PDPL), ADGM Data Protection Regulations 2021 (the 'ADGM DPR') and the EU's General Data Protection Regulation (GDPR), and all other national privacy laws where M42 operates.
Information Asset	A business application or system that creates, receives, stores (digitally or physically) or transmits Personal Data.
Data Controller	An organisation (such as M42 or an external partner) that decides why Personal Data is being processed and how it will be done. The Data Controller is responsible for ensuring that data Processing complies with the law.
Data Breach	A security incident in which Personal Data is lost, stolen, accessed without permission, or shared in error. This includes both accidental and deliberate incidents.
Data Protection Impact Assessment (DPIA)	A structured risk assessment required when a planned project or Processing activity could pose high risks to individuals' privacy. It helps identify and minimise those risks before the activity goes live.
Data Subject	The person whose Personal Data is being processed. This could be a patient, employee, job applicant, contractor, or customer.
High-Risk Processing	Any use of Personal Data that is likely to result in high risk to individuals' rights and freedoms. Examples include large-scale use of Sensitive Data, automated decision-making, or cross-border transfers of Personal Data (referred to also as 'High-Risk').
M42 Connect	Means the M42 Intranet where all M42 Group Data Protection Policies and Procedures are stored and accessible for M42 Group Personnel.
M42 Group	Includes all entities and personnel of M42.
M42 Group Personnel	All individuals who work directly for or represent the M42 Group, including directors, employees, consultants, and long-term contractors or any other person or entity whose transactions are directed by, or subject to, your influence or control.
Personal Data	Any information that relates to a person who can be identified directly or indirectly. This includes names, ID numbers, contact details, health data, employee files, and online identifiers.

PIA	Means Privacy Impact Assessment.
Privacy Management Platform	The technical platform selected by M42 to facilitate the management of day-to-day protection practices, including Records of Processing Activities, DPIAs and data protection training.
Processing	Any action performed on Personal Data - such as collecting, storing, using, analysing, sharing, or deleting it - whether done manually or using automated systems.
Data Processor	An organisation or person that processes Personal Data on behalf of a Data Controller and only according to the Data Controller's instructions (example: a payroll service provider Processing employee salary for M42).
ROPA	Means Records of Processing Activities.
Special Categories of Personal Data (Sensitive Data)	Types of Personal Data that are considered sensitive and require additional protection under the law. This information includes racial or ethnic origin, nationality/passport, political opinions, religious or similar beliefs, trade union membership, physical and/or mental health information, data concerning a natural person's private life, and criminal convictions, allegations, court proceedings, and/or sentences.
Supervisory Authority	A government agency responsible for overseeing data protection compliance, handling complaints, and enforcing privacy laws (example: the UAE Data Office, or a national Data Protection Authority in the EU).
Vendor	An entity providing goods and/or services to M42 with which M42 enters into a legally binding agreement (including a Purchase Order).

2. OVERVIEW

M42 is committed to collecting, using and sharing Personal Data with care, accountability, and respect for individual privacy. Across all platforms and business units, we recognize the importance of protecting the Personal Data entrusted to us by patients, employees, clients, and partners.

We view data protection as a core element of operational excellence and trust. This policy sets out the principles, roles, and requirements that govern how M42 handles Personal Data- ensuring that it is protected from unauthorised access, misuse, or loss in line with best practice and applicable Data Protection Laws.

In an increasingly data-driven and digitally connected world, M42 recognizes the growing privacy risks and responsibilities that come with collecting, using, and sharing Personal Data- especially in the context of healthcare, research, and advanced technologies.

3. PURPOSE

This Policy is designed to ensure that:

- Personal Data is handled lawfully, fairly, and transparently across the M42 Group
- Individuals' privacy rights are understood and respected by all employees and stakeholders
- All data Processing activities meet the requirements of applicable Data Protection Laws
- M42 employees, contractors, and business partners understand their role in protecting data and maintaining trust

It applies to all Personal Data processed by or on behalf of M42, in any format and in any location, and should be followed alongside M42's supporting data protection and information security frameworks, policies, procedures, standards, and guidance. For more information, please go to section 15. **Related Documents** of this Policy.

4. SCOPE

This Policy applies to all Personal Data processed by or on behalf of M42 Ltd and its subsidiaries, including entities operating in the United Arab Emirates, Europe and other jurisdictions. It covers all employees, contractors, and third parties who process Personal Data for M42, regardless of location, system, or format.

5. APPLICABLE LAWS

M42 is subject to a range of data protection laws depending on the nature and location of its activities. The UAE has a patchwork of laws and regulations which relate to health data and Personal Data. There are separate regimes that exist at the federal level (i.e. that apply across the whole country), and in different economic zones and Emirates. Generally, the applicable regime(s) depend on the jurisdiction in which an entity has been established / is operating.

As an Abu Dhabi-headquartered company, the principal data protection laws applicable to M42's activities in the UAE include the PDPL and the ADGM DPR for the Abu Dhabi Global Market ('ADGM'), together, the 'UAE Data Protection Laws'.

In addition, the M42 Group's activities which relate to health data will likely fall within the remit of the Federal Law No. 2 of 2019, and its related regulations Cabinet Resolution No. 32 of 2020 and Ministerial Resolution 51 of 2021 (collectively, the 'Health Data Law'), as well as:

- the applicable **Abu Dhabi Department of Health policies and standards** ('DoH Standards'),
- The **Abu Dhabi Healthcare Information and Cyber Security** (ADHICS) standard, where applicable.

This Policy is primarily based on the requirements of the PDPL, ADGM DPR and the EU General Data Protection Regulation (GDPR), where applicable.

M42 will also comply with any other local data protection or privacy laws in jurisdictions where it operates, to the extent they apply to its Processing of Personal Data.

PART II: GOVERNANCE

6. ROLES AND RESPONSIBILITIES

Group Level

Platform Level

All Levels

Group Data Protection Officer (DPO)

Provides oversight of M42's data protection programme across the Group. Advises on compliance, reviews high-risk Processing, and is the main contact for supervisory authorities. Maintains this policy and supporting procedures.

The Group DPO sets the overall privacy strategy and ensures M42 meets legal requirements. Platform Privacy Officers apply this strategy locally and handle day-to-day privacy tasks.

They work together to make sure privacy is managed consistently across the Group.

Platform Privacy Officer

Leads day-to-day privacy compliance within their business unit or platform. Coordinates local activities, ensures policy implementation, and serves as a contact point for internal teams and the Group DPO.

Privacy Champion

Supports awareness and implementation of data protection in a specific department. Helps ensure local teams follow the policy, escalate issues when needed, and apply privacy practices in daily operations.

Process Owner

Oversees a defined business process (e.g., onboarding, billing) and ensures that Personal Data is handled in line with privacy requirements at every step.

System Owner

Manages technical systems and applications that process Personal Data. Works with relevant stakeholders to apply appropriate security measures and controls.

Contract Owner

Oversees third-party vendor relationships. Ensures privacy clauses and data processing terms are in place before any vendor processes Personal Data on M42's behalf.

All M42 Employees

Must follow this policy and complete training on data protection. Responsible for reporting privacy concerns, using Personal Data appropriately, and protecting confidential information.

PART III: OPERATIONS

7. DATA PROTECTION PRINCIPLES

M42 follows core privacy principles when Processing Personal Data. These principles come from Applicable Data Protection Laws. They guide how we collect, use, store, and share Personal Data across the M42 Group.

All employees, contractors, and third parties working with M42 must follow these principles in their daily work.

The Principle	What Does It Mean?	How Do We Comply?
Lawfulness, Fairness & Transparency	M42 must only collect and use Personal Data when there is a valid legal reason (known as a legal basis) under laws like the PDPL or GDPR, and we must be open and honest with individuals about how their data is handled. For more information, refer to our **privacy notices** or speak to your Platform Privacy Officer or Privacy Champion.	• We identify and document the legal basis before collecting Personal Data. • We provide a clear and accessible Privacy Notice at the point of collection. • Privacy Notices explain what data we collect, why, who we share it with, and how long we keep it. • We do not collect or use Personal Data in misleading or hidden ways.

Purpose Limitation	M42 must only use Personal Data for the specific purpose we told the individual at the time of collection. If we want to use it for a different reason, we must update the privacy notice and have a valid legal basis.	• We only use data for the purposes listed in our **privacy notices**.
		• Common purposes at M42 include:
		  ○ Employee administration.
		  ○ Marketing and communications.
		  ○ Patient registration and appointment scheduling.
		  ○ Diagnosis, treatment, and medical care delivery.
		• If the purpose changes, we update the privacy notice and confirm the legal basis again.

Data Minimisation	We must only collect the Personal Data we truly need- no more, no less. Collecting unnecessary data increases privacy risk and may be unlawful.	• We only collect data that is essential for a defined purpose. • Our systems and forms are designed to avoid collecting “nice-to-have” data. • We regularly review what we collect and remove anything that is no longer needed.
Data Accuracy	Personal Data must be correct, complete, and kept up to date. Using inaccurate information can lead to mistakes or unfair outcomes.	• We update Personal Data when notified of changes. • We avoid relying on outdated or incomplete data. • Where relevant, we give individuals a way to correct their information.
Storage Limitation	We must not keep Personal Data longer than necessary. Once it’s no longer needed for its original purpose, it should be securely deleted or anonymised. Refer to the **M42 Group Personal Data Retention Procedure** or speak to your Platform Privacy Officer or Privacy Champion for guidance.	• We apply defined retention periods based on purpose and legal need. • Personal Data is securely deleted or anonymised when no longer required. • Where data must be kept for legal, audit, or regulatory reasons, access is restricted and documented.

Integrity and Confidentiality (Security)	Personal Data must be protected from unauthorised access, loss, misuse, or disclosure- whether it's stored digitally or on paper. For more information, refer to the **M42 Group Data Breach Notification Procedure** or contact the Group DPO.	• We follow M42 security policies, including role-based access and secure systems. • Sensitive Data is encrypted where required and access is restricted. • All data incidents must be reported immediately and handled under M42's response procedures. • Third party vendors must meet equivalent security standards.
Accountability	M42 must be able to demonstrate that it complies with data protection laws. It's not enough to follow the rules- we must be able to show how.	• We maintain up-to-date RoPAs. • We conduct DPIAs for High-Risk Processing. • Roles and responsibilities are clearly assigned through our governance framework. • All employees complete mandatory privacy training and follow documented procedures.

8. LEGAL BASES FOR PROCESSING

Before collecting or using Personal Data, we must always have a valid legal reason to do so under the applicable law- either the PDPL or the GDPR.

This is called a **legal basis**. We must choose the correct legal basis depending on the nature of the activity, the type of Personal Data, and where the activity takes place.

The PDPL treats consent as the main reason for Processing Personal Data but also allows Personal Data to be used without consent in certain situations, for example in contracts, legal obligations, or protecting someone's safety. The GDPR takes a slightly different approach- there are six possible legal reasons we can rely on to use someone's Personal Data – consent, contractual obligation, legal obligation, vital interests, public interests and legitimate interests.

M42 must always identify a valid legal basis before Processing Personal Data. Guidance on how to determine the appropriate legal basis is provided in the **M42 Group Legal Basis Procedure**.

9. RIGHTS OF INDIVIDUALS

The Applicable Data Protection Laws that M42 must follow- depending on jurisdiction and context- may grant individuals (including patients, employees, job applicants, contractors, and customers) certain rights in relation to their Personal Data. Although the specific terminology and scope may vary across laws, individuals may be entitled to exercise one or more of the following rights:

Right **to know** if their Personal Data is being Processed and **to access** that Personal Data	Right **to withdraw consent** for Processing their Personal Data at any time and for any reason

Right **to correct** inaccurate Personal Data and complete any incomplete Personal Data	Right **to restrict** or **stop** the Processing of their Personal Data in specific circumstances, such as when the Personal Data's accuracy is contested, or the Processing is unlawful
Right to request the **deletion** of their Personal Data in certain situations, like when it is no longer needed, or they withdraw their consent	Right to **file a complaint** with a Supervisory Authority if they believe their Data Subject rights are being violated
Right **to receive** their Personal Data in a format that allows them **to transfer** it to another service or company easily	Right **to object** to any **decision based solely on automated Processing** (like automated credit scoring), including profiling, which produces legal consequences or significantly affects the individual, and to require such decisions to be reviewed manually

These rights may not apply in the same way everywhere- it depends on which Applicable Data Protection Law that applies in each country and what role M42 plays in handling the Personal Data. M42 will always respect the rights that apply in each situation, based on the relevant legal requirements.

M42 must always be receptive to any requests made by individuals in connection with their Data Subject rights and Personal Data. It is our duty to identify such requests, to respond to them appropriately, and maintain a register of all such requests along with the corresponding M42 responses.

You can read more about rights of individuals and how to handle them in our **M42 Group Data Subject Rights Procedure** - in the meantime, please find below a short summary:

Ways individuals submit requests for Data Subject rights:	Examples of Data Subject rights requests:	Response Timing – Best Practice:
• Job applicants, employees, or contractors contacting Human Capital • Patients and customers submitting inquiries via email, telephone, or in-app channels • Website visitors using the web form • Any individual contacting M42 through other available channels, even if not specifically designated for privacy inquiries (e.g. through Social Media channels)	• 'I don't want to receive your marketing letters and promotions' • 'Did I agree to that? I didn't see a privacy notice when I typed in my details' • 'Does the right to be forgotten apply to me?' • 'I want to find out what data you have about me'	1. Acknowledgement must be sent to the individual within 10 days of their request submission date 2. Requests must be fulfilled within 30 days of the request submission 3. If needed, M42 can extend response period by an additional 30 days, provided the individual is informed of the extension

Note: All Data Subject that submits a request to M42 must receive a response!

When interacting with Data Subjects- whether directly or indirectly by supporting the Platform Privacy Officer in fulfilling a Data Subject request- it is important to keep the following in mind:

- If someone contacts you, be aware they may be making a request regarding their Personal Data, regardless of your role
- Never ignore a Data Subject request, but seek clearance internally before responding
- Remain professional, and escalate any issues to your Privacy Champion or Platform Privacy Officer

If you are a Process Owner, System Owner, or Contract Owner looking for guidance on handling data subject requests as they pertain to your process, system, or contract, please refer to the **Data Subject Rights Procedure** - It includes email templates and workflow charts to support you through each step, or contact your Platform Privacy Officer.

To help communicate with data subjects clearly and consistently, use the approved **Guidance and Response Templates**.

10. TRANSFER OF PERSONAL DATA

M42 may, from time to time, transfer Personal Data across borders in order to deliver services, manage operations, or work with partners and vendors internationally. These transfers must be conducted in strict compliance with Applicable Data Protection Laws.

Depending on the law and the location, different conditions must be met before a transfer can happen. These may include (but are not limited to):

- Ensuring the destination country has an adequate level of data protection
- Showing that the transfer is necessary- for example, to carry out a contract or protect someone's vital interests
- Including specific privacy safeguards in contracts (such as standard clauses or binding rules)
- Completing a risk assessment to evaluate and reduce risks to rights and freedoms of individuals
- Getting clear and informed consent from the individuals
- Keeping records of the transfer, including why it's happening, who will receive the data, and what protections are in place

M42 Group Controls for International Transfers

To ensure compliance across all jurisdictions:

- M42 maintains an internal **Data Transfer Procedure** and requires completion of a **Transfer Impact Assessment** (TIA) for non-adequate jurisdictions
- Cross-border transfers must be documented, including legal basis, recipient details, purpose, and risk mitigation
- Contracts with external parties must include appropriate data protection clauses, ensuring enforceability of data subject rights
- M42 conducts regular reviews to assess transfer mechanisms in light of changes to law, supervisory guidance, or risk environment

M42 employees must consult with their Platform Privacy Officer or the Group DPO prior to initiating any new international data transfer. The use of secure transfer methods and minimisation of exported data volumes are always encouraged.

For more information, refer to the **M42 Group Data Transfer Procedure** or contact your Platform Privacy Officer.

11. PRIVACY BY DESIGN AND DEFAULT

When planning new systems, services, or processes that involve Personal Data- or making significant changes to existing ones- M42 applies the principles of Privacy by Design and Default. **This means privacy must be considered from the start**, not added later.

In line with this, M42 may carry out a **Data Protection Impact Assessment** (DPIA) to assess potential privacy risks and ensure that Personal Data is handled lawfully and responsibly.

A DPIA typically includes:

- A review of how and why Personal Data will be processed
- An assessment of whether the Processing is necessary and proportionate
- An evaluation of the risks to individuals
- Identification of safeguards and controls to reduce those risks

We may also use techniques such as:

- Data minimisation – only collecting what's needed
- Anonymisation – removing personal identifiers
- Pseudonymisation – replacing identifiers with codes when full anonymity isn't possible

Before starting any new project, system, process, or making significant changes to existing ones, you should always refer to the **Data Protection by Design and Default Policy** and procedure. If required under that policy, a DPIA must also be completed using provided template.

12. RECORDS OF PROCESSING ACTIVITIES

M42 maintains detailed records of all Personal Data Processing activities carried out across the M42 Group. These records are required under applicable Data Protection Laws and may be provided to Supervisory Authorities upon request.

Each record includes:

- The name and contact details of the relevant M42 entity and the Group DPO
- The purpose(s) for Processing Personal Data
- The types of data subjects and Personal Data involved
- Who has access to the data and any recipients (including third parties or international transfers)
- How long the data is kept and when it will be deleted
- The legal basis for Processing and any restrictions
- The technical and organisational measures used to keep data secure

These records are maintained and regularly updated in line with the **M42 Record of Processing Activities Procedure**, which outlines roles, responsibilities, and the steps for keeping these records accurate and up to date.

13. DATA BREACH RESPONSE

M42 must act quickly and responsibly in the event of a Personal Data breach. A breach can include accidental loss, unauthorised access, misuse, or theft of Personal Data.

When a breach occurs:

- M42 may be required to notify the relevant authority within 72 hours of becoming aware of the breach
- In some jurisdictions, notification may be required immediately upon becoming aware of the breach - there is no specific time window
- If the breach could cause serious harm to individuals (such as identity theft or financial loss), M42 may also need to notify the affected individuals without undue delay
- If a third-party service provider (e.g., a vendor or partner) causes or discovers the breach, they must notify M42 immediately
- In some situations, notification to individuals may not be required if strong protective measures were in place (e.g., encryption or pseudonymisation)

Note: the rules and deadlines for breach notification vary depending on the country and the law that applies to the processing. For full details, please refer to the **M42 Group Data Breach Notification Procedure**.

What to do:

All suspected or confirmed breaches must be reported immediately to your **Platform Privacy Officer** and **Chief Information Officer**, who will coordinate the response in line with the **M42 Group Data Breach Notification Procedure**.

Employees should use the **Data Breach Notification Form, Data Breach Assessment and Data Breach Register** template to document the event and ensure all required information is captured for review and reporting.

14. TRAINING AND AWARENESS

M42 is committed to building a strong culture of data protection across the Group.

- All employees, contractors, and relevant third parties must complete privacy training when they join M42 and at regular intervals afterwards
- Training will cover the Applicable Data Protection Laws, and M42's internal privacy policies, procedures, and responsibilities
- Training may be delivered in different formats, such as online modules, live sessions, or recorded presentations, depending on role and location

- M42 may also provide targeted workshops, reminders, or awareness campaigns to help embed privacy into daily practice
- Participation in training will be tracked, and records of completion will be maintained. Repeated failure to complete mandatory training may lead to disciplinary action

Everyone at M42 is expected to understand and follow this policy, and to stay informed through the resources and guidance provided by the Group DPO and Platform Privacy Officers.

PART IV: MAINTANCE AND QUERIES

15. RELATED DOCUMENTS

Data Protection Related Documents	
Procedures	**Instructions, Guidelines, Forms & Templates**
• Records of Processing Activities Procedure	• Group Records of Processing Activities
• Privacy Risk Assessment Procedure	• PIA & DPIA templates
• Data Subject Rights Procedure	• Guidance and Response Templates
• Procedure to Determine the Legal Basis	• Consent Withdrawal Form Template
• Data Retention Policy	• Retention Schedules
• Transfer Impact Assessment Procedure	• Transfer Impact Assessment Template
• Third Party Management Procedure	• DPA Templates
• Breach Notification Procedure	• Data Breach Reporting Templates
• Privacy by Design and Default Policy	• Privacy by Design and Default Guidance

Information Security Related Documents	
• Information Security Policy	• Information Security Governance Framework
• IT Operations Security Policy	• Information Security Incident Management Policy
• Information Classification and Handling Guidelines	

16. POLICY OWNERSHIP AND MAITENANCE

This Policy is owned by the **M42 Legal & Governance**. It will be reviewed at least once a year, or sooner if triggered by relevant changes. Examples of triggers for incidental review include:

- Changes to applicable laws or regulatory guidance (e.g., updates to the PDPL, ADGM DPR or GDPR)
- Introduction of new systems or technologies that affect how Personal Data is processed
- Organisational changes, such as mergers, acquisitions, or internal restructuring
- Material changes to M42's Processing activities or risk profile
- Findings from audits, assessments, or supervisory authority guidance
- Lessons learned from significant Data Breaches or incidents

The current version of this Policy is available on the M42 Internet and M42 Connect.

Updates must be reviewed by the **Group Data Protection Officer** and approved by the **M42 Board of Directors**.

Version history:

Date	Version	Responsible
August 2024	Version 1.0	Group DPO
October 2025	Version 2.0	Group DPO

Reviewed by:

Date	Version	Reviewer

Approved by:

Date	Version	Approver
October 2025	Version 2.0	Board of Directors

CONTACT DETAILS

For any questions, concerns, or requests related to this Policy or the processing of Personal Data by M42, please contact the **M42 Privacy Team** at: privacy@m42.ae

ANNEX 1 – USE CASES

TRANSPARENCY IN MARKETING- USE CASE TABLE

Scenario	What You Must Tell the Data Subject	How M42 Ensures Compliance
Marketing email campaigns	Purpose, legal basis, how to opt out	Clear unsubscribe links; consent records maintained
Telemarketing (UAE)	Explicit consent required by law	Follow national do-not-call registry; pre-check consents
Website form collecting contact details	Purpose, data collected, how it will be used	Embedded privacy notice with link to full
Internal employee survey	Purpose, optional/mandatory, who sees data	Intro blurb includes data use and access rights
Using a vendor to send newsletters	That data will be shared with a third party	Listed in privacy notice + covered in vendor contract

Under UAE law, prior consent is especially critical in marketing communications - this applies to email, SMS, general messaging providers (e.g., WhatsApp), and phone calls.