World Medical Card®
For safer medical treatment

Security & Data Protection Overview

World Medical Card | worldmedicalcard.io

Confidential | For enterprise and partner use

Document version	1.0
Date	June 2026
Classification	Confidential
Legal entity	Wmc Technologies AS (Company No. 984 653 689)
Prepared by	World Medical Card — Operations & Compliance
Intended audience	Enterprise clients, partners, procurement & due diligence teams

This document provides an overview of World Medical Card's data protection practices, infrastructure security, and GDPR compliance posture. It is intended to support enterprise procurement, partner onboarding, and due diligence processes. For additional information or a formal Data Processing Agreement, please contact **compliance@worldmedicalcard.io**.

Table of Contents

1. About World Medical Card
2. Data We Hold and How We Use It
3. Infrastructure & Platform Architecture
4. Access Controls & Security Practices
5. GDPR & Data Protection Compliance
6. Vendor & Third-Party Management
7. Incident Response & Business Continuity
8. Summary & Contact Information

1 About World Medical Card

World Medical Card (WMC) is a Norway-based digital health record platform with global reach. WMC enables individuals to store, manage, and share their critical health information securely — including diagnoses, medications, allergies, vaccination history, and insurance details — so that authorised healthcare providers and emergency responders can access it when it matters most.

The platform serves individual members, corporate clients, insurance partners, and healthcare organisations worldwide. As a custodian of sensitive personal health data, WMC takes its data protection and security obligations with the utmost seriousness.

Key facts

Headquarters	Norway
Legal entity	Wmc Technologies AS (Company No. 984 653 689)
Geographic reach	Global — members and enterprise partners across multiple continents
Platform type	Digital health record platform (SaaS)
Primary regulation	GDPR (EU/EEA) — Norway as EEA member state
Infrastructure	Google Cloud Platform (GCP)
Data categories	Health records, personal identity, insurance/policy data, contact & payment data

2 Data We Hold and How We Use It

WMC processes several categories of personal data, all collected with the explicit, informed consent of each member. The table below summarises each category, its purpose, and the legal basis under GDPR.

Data categories and processing purposes

Category	Examples	Purpose	Legal basis (GDPR)
Health & medical records	Diagnoses, medications, allergies, vaccinations, conditions	Enable emergency access and health management by member and authorised providers	Explicit consent (Art. 9(2)(a)); Vital interests (Art. 9(2)(c))
Personal identity	Name, date of birth, nationality, passport/ID number	Member identification and verification	Contract performance (Art. 6(1)(b))
Insurance & policy data	Insurer name, policy number, coverage details	Facilitate insurance-related services and partner integrations	Contract performance; legitimate interests (Art. 6(1)(f))
Contact & payment data	Email, phone, address, billing information	Account management, service delivery, billing	Contract performance (Art. 6(1)(b))

Data minimisation and retention

WMC adheres to the principle of data minimisation: only data that is strictly necessary for the stated purpose is collected. Data is retained only for as long as required by the service relationship or applicable law, after which it is securely deleted or anonymised in accordance with our documented retention schedule.

Member control and data subject rights

Members retain full control over their data. WMC supports the exercise of all GDPR data subject rights, including:

- ✓ Right of access — members can view all data held about them at any time
- ✓ Right to rectification — members can correct inaccurate records
- ✓ Right to erasure — members can request deletion of their account and associated data
- ✓ Right to data portability — members can export their health record in a standard format
- ✓ Right to withdraw consent — health data processing can be stopped at any time
- ✓ Right to object — members can object to any processing based on legitimate interests

3 Infrastructure & Platform Architecture

WMC's platform is built on Google Cloud Platform (GCP), one of the world's leading enterprise cloud providers and a recognised leader in security and compliance. GCP provides WMC with enterprise-grade physical security, redundancy, and a broad portfolio of compliance certifications including ISO 27001, SOC 2, and GDPR data processing agreements.

GCP infrastructure highlights

Cloud provider	Google Cloud Platform (GCP)
Data residency	EEA-based regions (data stored within the European Economic Area)
Physical security	GCP data centres are ISO 27001 certified with 24/7 physical access controls, CCTV, and multi-factor entry
Network security	Google's private global fibre network; DDoS protection via Google Cloud Armor; VPC isolation between environments
High availability	Multi-zone deployment with automated failover; target 99.9%+ uptime SLA
Disaster recovery	Automated daily backups with point-in-time recovery; geographically redundant storage
Encryption at rest	All data encrypted at rest using AES-256 by default via GCP-managed keys
Encryption in transit	All communications encrypted via TLS 1.2+ with HTTPS enforced across all endpoints

Environment separation

Production, staging, and development environments are strictly separated using separate GCP projects with independent IAM policies. No real member data is ever used in non-production environments. Access to production infrastructure is limited to authorised engineers on a need-to-know basis and is subject to audit logging.

Scalability and availability

The platform is designed for elastic scalability using GCP-native managed services. Auto-scaling policies ensure consistent performance under load, and health checks with automated remediation reduce dependency on manual intervention.

4 Access Controls & Security Practices

Identity and access management

Access to WMC systems follows the principle of least privilege. Every team member is granted the minimum level of access required to perform their role, and access rights are reviewed periodically and revoked promptly upon any change in role or departure from the organisation.

- ✓ Multi-factor authentication (MFA) is mandatory for all staff accessing internal systems and cloud infrastructure
- ✓ Role-based access control (RBAC) is enforced across all platforms and services
- ✓ Privileged access to production systems requires additional approval and is time-limited
- ✓ All access to production data is logged and subject to audit review
- ✓ Shared accounts and credentials are prohibited

Application security

WMC follows secure software development lifecycle (SSDLC) practices to embed security throughout the development process:

- ✓ Code is reviewed by a second engineer before merging to main branches
- ✓ Dependency scanning is run automatically as part of the CI/CD pipeline to identify known vulnerabilities
- ✓ Static application security testing (SAST) is integrated into the development workflow
- ✓ API endpoints are protected with authentication, rate limiting, and input validation
- ✓ Security-relevant changes are flagged for additional review

Internal security policies

WMC maintains a set of internal security policies that govern how staff interact with systems and data. These include:

Acceptable use policy	Defines permitted and prohibited uses of WMC systems and data by all staff
Password & credential policy	Enforces strong password standards and prohibits credential sharing; password manager use is required
Device management policy	All work devices are enrolled in device management with remote wipe capability; full-disk encryption required
Remote working policy	Defines secure practices for remote access including mandatory VPN usage for accessing internal resources
Data classification policy	Data is classified by sensitivity; handling requirements are defined for each classification level

Joiner/mover/leaver process	Access provisioning and de-provisioning is tied to HR processes with same-day revocation on departure

Security awareness training

All WMC staff complete security awareness training upon onboarding and annually thereafter. Training covers phishing awareness, data handling best practices, incident reporting, and social engineering. Phishing simulation exercises are conducted periodically.

5 GDPR & Data Protection Compliance

As a Norwegian company operating within the EEA and processing health data of individuals worldwide, WMC is subject to the General Data Protection Regulation (GDPR) and the Norwegian Personal Data Act (Personopplysningsloven). Health data is classified as a special category of personal data under GDPR Article 9 and is afforded the highest level of protection.

GDPR compliance posture

Data controller	Wmc Technologies AS acts as data controller for all member personal data
Data processors	Third-party processors (e.g. GCP) are engaged under signed Data Processing Agreements (DPAs) compliant with GDPR Art. 28
Legal bases	Explicit consent (Art. 9(2)(a)) for health data; contract performance (Art. 6(1)(b)) for service delivery; vital interests (Art. 9(2)(c)) for emergency access scenarios
Privacy policy	A clear and accessible privacy policy is provided to all members at the point of data collection
Records of processing	WMC maintains a Record of Processing Activities (ROPA) as required by GDPR Art. 30
DPO / Data protection contact	A designated data protection contact is responsible for GDPR compliance and can be reached at compliance@worldmedicalcard.io
International transfers	Where data is transferred outside the EEA, appropriate safeguards (e.g. EU Standard Contractual Clauses) are in place
Data subject requests	Processes are in place to handle all data subject rights requests within the statutory 30-day period

Data Processing Agreements

WMC is prepared to enter into a Data Processing Agreement (DPA) with enterprise clients and partners where WMC processes personal data on their behalf or jointly with them. Our DPA template reflects GDPR requirements and can be adapted to client-specific requirements. Please contact compliance@worldmedicalcard.io to initiate this process.

> **Special category data:** Health data is classified as special category data under GDPR Art. 9. WMC processes this data only on the basis of explicit, informed consent from each member. Members can withdraw consent at any time, and their data will be deleted upon request.

6 Vendor & Third-Party Management

WMC maintains a vendor management programme to ensure that all third parties who access or process WMC data on our behalf meet appropriate security and data protection standards.

Vendor assessment process

- ✓ All new vendors are assessed for security and data protection compliance before onboarding
- ✓ Vendors who process personal data must sign a Data Processing Agreement (DPA) prior to engagement
- ✓ Vendors handling sensitive data are subject to enhanced due diligence, including review of their own certifications and security practices
- ✓ Vendor relationships are reviewed annually, and critical vendors are assessed more frequently
- ✓ A register of all data processors is maintained and updated as the vendor landscape changes

Key platform vendors

Vendor	Role	Key certifications
Google Cloud Platform	Primary cloud infrastructure provider	ISO 27001, SOC 2 Type II, GDPR DPA, CSA STAR
Payment processor (PCI-DSS compliant)	Billing and payment processing	PCI DSS Level 1, SOC 2
Email / communications provider	Transactional email and notifications	SOC 2, GDPR DPA

7 Incident Response & Business Continuity

Incident response

WMC maintains a documented Incident Response Plan (IRP) covering detection, containment, eradication, recovery, and post-incident review. All staff are trained to recognise and report security incidents promptly.

Detection	Automated alerting via GCP Security Command Center, Cloud Logging, and application-level monitoring
Triage & containment	On-call engineer responds within defined SLAs; affected systems are isolated to prevent spread
Data breach notification	In the event of a personal data breach, WMC will notify the relevant supervisory authority (Datatilsynet, Norway) within 72 hours as required by GDPR Art. 33. Affected data subjects are notified without undue delay where required
Post-incident review	All significant incidents are followed by a root-cause analysis and documented corrective actions
Contact for reporting	security@worldmedicalcard.io

Business continuity & disaster recovery

WMC has a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to ensure continued service availability in the event of a major disruption:

- ✓ Automated daily backups with point-in-time recovery capability
- ✓ Geographically redundant storage across multiple GCP regions
- ✓ Documented recovery time objectives (RTO) and recovery point objectives (RPO)
- ✓ Regular testing of backup restoration procedures
- ✓ Critical systems are monitored 24/7 with automated alerting and failover

8 Summary & Contact Information

World Medical Card is committed to the responsible stewardship of its members' most sensitive data. Our security and data protection programme is built on a foundation of strong technical controls, clear policies, GDPR compliance, and a culture of security awareness across the organisation.

We recognise that enterprise clients and partners have rigorous procurement and due diligence requirements. We welcome the opportunity to discuss our practices in more detail and to provide any additional documentation or attestations required.

Contact

General enquiries	support@worldmedicalcard.io
Data protection / GDPR	compliance@worldmedicalcard.io
Security incidents	security@worldmedicalcard.io
Enterprise & partnerships	enterprise@worldmedicalcard.io