GENERAL DATA PROTECTION REGULATION (GDPR) & DATA PROTECTION POLICY

TABLE OF CONTENTS

PREAMBLE

Urathon Europe Ltd ("the Company"), as a controller and, where appropriate, a processor of personal data, is committed to ensuring that all personal data under its control is managed in accordance with the applicable laws of the United Kingdom. These include:

- The **UK General Data Protection Regulation (UK GDPR)**, as retained and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019;
- The **Data Protection Act 2018** ("DPA 2018"), which supplements the UK GDPR in domestic law;
- The **Privacy and Electronic Communications (EC Directive) Regulations 2003** ("PECR") where relevant to direct marketing and cookies.
- Relevant sector-specific standards issued by the **Information Commissioner's Office (ICO)**, **Medicines and Healthcare products Regulatory Agency (MHRA)**, and NHS Digital;
- Obligations under the **Freedom of Information Act 2000 (FOIA)** and **Health and Social Care Act 2012** where applicable to NHS tendering and information disclosure.

This policy defines the rules, standards, and operational responsibilities applied by Urathon Europe Ltd in managing personal data across all commercial, clinical, technical, and administrative functions, including its manufacture and distribution of **Mobility Aids** and **Continuous Glucose Monitoring (CGM)** systems.

SECTION 1: POLICY PURPOSE AND LEGAL AUTHORITY

1.1 The purpose of this policy is to articulate the Company's position on the acquisition, handling, storage, use, transmission, and disposal of personal data in accordance with UK legal requirements.

1.2 This document shall serve as the master data governance policy for the Company, superseding any conflicting internal guidance or practice.

1.3 Failure to comply with this policy may result in regulatory enforcement action under Articles 58, 83, and 84 of the UK GDPR, and/or civil or criminal liability under the DPA 2018.

SECTION 2: SCOPE AND APPLICABILITY

2.1 This policy applies to all personal data processed by or on behalf of Urathon Europe Ltd, regardless of whether such data is held electronically, on paper, or by third-party systems.

2.2 The scope includes:

- Data collected from customers, patients, clinicians, employees, suppliers, contractors, and partners;
- Data arising from **mobility devices** (e.g. usage logs, health indicators, accessibility flags);
- **Biometric and medical data** collected from **CGM devices**, apps, or related interfaces;
- Records of business activities involving third-party processors and international data transfers

2.3 This policy applies to:

- All permanent and temporary staff;
- Contracted and agency staff;
- Subcontractors, data processors, and service providers;
- Directors, board members, and strategic decision-makers

SECTION 3: DEFINITIONS

3.1 **Personal Data**: Any information relating to an identified or identifiable natural person. This includes but is not limited to names, addresses, identification numbers, location data, and physiological characteristics.

3.2 **Special Category Data**: Sensitive data including health information, genetic and biometric data, racial or ethnic origin, and religious beliefs. Processing of such data is prohibited unless a condition under Article 9 of the UK GDPR is met.

3.3 **Controller**: The entity that determines the purposes and means of the processing of personal data.

3.4 **Processor**: A natural or legal person that processes personal data on behalf of the controller.

3.5 **Data Subject**: A living individual who is the subject of personal data.

3.6 **Consent**: Freely given, specific, informed, and unambiguous indication of the data subject's wishes, signifying agreement to the processing of personal data.

3.7 **DPIA (Data Protection Impact Assessment)**: A documented process assessing the potential impact on data protection of a high-risk processing activity.

3.8 **DPO (Data Protection Officer)**: The individual appointed to oversee data protection strategies and ensure legal compliance.

3.9 **UK GDPR**: The General Data Protection Regulation as retained in UK law post-Brexit.

3.10 **MHRA**: The UK government agency responsible for ensuring that medical devices work and are acceptably safe.

SECTION 4: ROLES AND RESPONSIBILITIES

4.1 Board of Directors

The Board retains overall responsibility for ensuring that Urathon Europe Ltd complies with its legal obligations under data protection laws and delegates oversight to the Data Protection Officer.

4.2 Data Protection Officer (DPO)

The DPO is responsible for:

- Monitoring compliance with data protection law and internal policy;
- Providing advice and guidance on data protection impact assessments (DPIAs);
- Acting as the point of contact for the ICO and data subjects;
- Maintaining the Company's Record of Processing Activities (RoPA);
- Training and awareness programmes.

4.3 **Employees and Contractors**

All staff must:

- Handle personal data in accordance with this policy.
- Report data breaches immediately.
- Complete mandatory data protection training.
- Only access personal data on a need-to-know basis.

4.4 **Third-Party Processors**

External vendors or service providers must:

- Enter into Data Processing Agreements (DPAs) with Urathon Europe Ltd.
- Implement equivalent security and privacy safeguards.
- Cooperate with audits, inspections, and data breach notification obligations.

SECTION 5: LAWFUL BASIS FOR PROCESSING

5.1 Urathon Europe Ltd must identify and document a valid legal basis before any personal data is processed, in line with Article 6 of the UK GDPR. The six available bases are:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

5.2 **CGM Systems**

Processing of CGM data (including glucose levels, timestamps, alert data) is carried out on the basis of:

- **Article 6(1)(a)** – explicit consent.
- **Article 9(2)(h)** – provision of healthcare.
- **Article 6(1)(b)** – performance of a contract (for connected services).

5.3 **Mobility Aids**

Mobility aid data (including ergonomic measurements, accessibility settings, diagnostic usage) is processed under:

- **Article 6(1)(f)** – legitimate interest for product improvement and safety.
- **Article 6(1)(c)** – compliance with MHRA post-market surveillance obligations.

5.4 Records of each lawful basis must be included in the RoPA and reviewed annually.

SECTION 6: SPECIAL CATEGORY DATA PROCESSING

6.1 **Definition and Sensitivity**

Special category data includes information revealing health status, biometric identifiers, genetic characteristics, and any data that, if breached or mishandled, could result in discrimination, reputational harm, or clinical risk.

6.2 **Conditions for Lawful Processing**

Under Article 9(1) UK GDPR, special category data is prohibited from processing unless a lawful exception under Article 9(2) is met. Urathon processes special category data based on:

- **Article 9(2)(a)** – the data subject has given explicit consent.
- **Article 9(2)(h)** – the processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, or provision of health or social care.
- **Article 9(2)(i)** – for public interest in the area of public health, particularly for CGM data used in remote monitoring.

6.3 **Data Protection Impact Assessments (DPIAs)**

For any new system or use case involving special category data (e.g., new CGM firmware update, mobility aid telemetry app), a DPIA must be undertaken to evaluate risks to confidentiality, availability, and integrity.

6.4 **Data Storage and Access Controls**

Special category data is stored using AES-256 encryption and accessed only by employees with enhanced authorisation under the Company's Role-Based Access Control (RBAC) structure. Audit logs must be retained for seven years.

6.5 **Disclosure Restrictions**

Disclosure of special category data to third parties (e.g., insurers, public health bodies) shall only be permitted:

- With the explicit written consent of the data subject.
- Where required by law or a statutory authority.
- Under contractually governed data-sharing agreements approved by the DPO.

SECTION 7: CONSENT MANAGEMENT

7.1 **Standard for Consent**

Consent must be:

- Freely given
- Specific
- Informed
- Unambiguous
- Given via a clear affirmative action
- Capable of being withdrawn at any time

7.2 **Explicit Consent – CGM Devices**

When CGM device users interact with cloud-based monitoring, digital dashboards, or clinician-linked APIs, **explicit consent** must be collected using a double opt-in mechanism with affirmative checkboxes. Implied or pre-ticked boxes are not valid under UK GDPR.

7.3 **Consent Recordkeeping**

Consent records must include:

- Date and method of collection
- What the data subject was told
- Whether the data subject withdrew or amended consent
- System logs confirming capture

7.4 **Withdrawal of Consent**

Users must be able to withdraw consent with the same ease with which it was given. Web interfaces, mobile apps, and email communications must include opt-out options and contact details for data queries.

7.5 **Minors and Consent**

Where consent is required from a child under the age of 13, the Company must obtain verifiable consent from a parent or guardian, in line with Section 9 of the DPA 2018.

SECTION 8: DATA SUBJECT RIGHTS

Urathon recognises the full set of rights afforded to individuals under Chapter III of the UK GDPR:

Right	Implementation
Right to be Informed	Fulfilled via layered privacy notices available at point of data capture.
Right of Access (SARs)	Responded to within 30 calendar days. Verified ID required.
Right to Rectification	Processed upon request; correction made within 30 days.
Right to Erasure	"Right to be forgotten" evaluated based on legal, regulatory, and contractual duties.
Right to Restriction	Imposed upon request or during dispute resolution.
Right to Data Portability	Provided in structured, commonly used, machine-readable format.
Right to Object	Honoured unless legitimate interests or legal obligations override.
Rights related to Automated Decision-Making	Individuals may request human review of AI-generated outcomes.

All rights requests are logged and tracked by the DPO. Where applicable, requests impacting CGM or health data are triaged within 7 days.

SECTION 9: DATA MINIMISATION AND ACCURACY

9.1 **Principle of Necessity**

Urathon commits to collecting only the minimum amount of personal data necessary for each lawful and specified purpose.

9.2 **Form Design and Field Audits**

All data collection forms (digital and paper-based) are reviewed semi-annually to ensure unnecessary fields are removed and justification exists for all required data.

9.3 **Accuracy Reviews**

For CGM and mobility aid registries, the Company shall:

- Allow users to view and amend their data
- Flag stale records for review every 12 months
- Conduct automated and manual checks for conflicting or illogical inputs

9.4 **Duty to Update**

All employees have a continuing obligation to update personal and employment records as necessary. Outdated records must be archived or destroyed according to the Data Retention Schedule (see Section 10)

SECTION 10: DATA RETENTION AND DESTRUCTION

10.1 **Retention Schedules**

Urathon maintains a detailed Data Retention Schedule based on statutory obligations, clinical necessity, and commercial needs. Key examples:

Data Type	Retention Period	Legal Justification
Employee Personnel Records	6 years from termination	Limitation Act 1980
CGM Health Data (Clinical)	10 years after last use	MHRA and NHS retention rules
Customer Orders and Invoices	6 years	HMRC requirements (s7, Finance Act 2008)

Supplier Contracts	6 years after expiry	Contractual dispute limitation periods
CVs / Unsuccessful Applications	6 months	ICO guidance on proportionality

10.2 **Secure Disposal Methods**

Data shall be securely destroyed when no longer required:

- Digital data: overwritten, purged using DOD 5220.22-M standards
- Paper records: cross-cut shredded and incinerated by authorised waste handlers
- Backups: subject to automated deletion after final lifecycle period expires

10.3 **Archival Protocols**

Legacy data retained for research, analysis, or lawful public interest will be anonymised or pseudonymised before storage. Access is restricted and subject to annual justification reviews.

SECTION 11: DATA SECURITY AND ACCESS CONTROL

11.1 **Information Security Governance**

Urathon Europe Ltd implements and maintains appropriate **technical and organisational measures (TOMs)** to safeguard personal data, as mandated under **Article 32 of UK GDPR**. These include but are not limited to:

- ISO 27001-aligned Information Security Management System (ISMS)
- Role-based access control (RBAC)
- Regular security risk assessments
- Encryption-at-rest and in-transit using TLS 1.3 and AES-256
- Secure VPN for remote access

11.2 **Device and Application Security**

All CGM systems and associated mobile or web applications must:

- Undergo penetration testing prior to release
- Comply with NHS Digital's **DTAC (Digital Technology Assessment Criteria)**
- Encrypt stored and transmitted biometric data

- Restrict backend database access to authorised support staff under audit

11.3 **Physical Security Controls**

The Company's data centres, head office, and warehouses must apply:

- Multi-factor authentication for access
- CCTV surveillance and entry logs
- Fire suppression systems and redundant power supplies

11.4 **Removable Media and BYOD**

Use of USB drives and personal mobile devices for storing or accessing personal data is prohibited unless:

- Pre-authorised by IT Security
- Encrypted and policy-enforced via Mobile Device Management (MDM)

11.5 **Monitoring and Audit Logging**

All access to personal data is logged and monitored. Logs are retained for 12 months and reviewed during security audits and incident investigations.

SECTION 12: PROCESSORS AND THIRD-PARTY SHARING

12.1 **Legal Obligations for Processors**

Urathon may engage third-party data processors (e.g., cloud providers, logistics, clinical app developers). All such engagements require:

- A **Data Processing Agreement (DPA)** compliant with Article 28 UK GDPR
- Written instructions on permitted processing
- Security standards and audit clauses
- Incident notification clauses (within 24 hours)

12.2 **Due Diligence and Vetting**

All processors must:

- Demonstrate GDPR compliance via policies, accreditations (e.g., ISO 27001), or audit reports
- Complete a Data Privacy Risk Assessment (DPRA) prior to onboarding

- Accept random or scheduled inspections

12.3 **Joint Controllers**

Where the Company determines processing jointly with another entity (e.g., a hospital trust, platform partner), a **Joint Controller Agreement (JCA)** shall be executed per **Article 26**, setting out responsibilities and public-facing contact points.

12.4 **International Processors**

Transfers to non-UK/EU entities are subject to Section 7 of this policy and must include:

- ICO-approved **Standard Contractual Clauses (SCCs)** or
- UK **International Data Transfer Agreement (IDTA)**
- A formal **Transfer Risk Assessment (TRA)**

SECTION 13: RECORDS OF PROCESSING ACTIVITIES (RoPA)

13.1 **Obligation to Maintain RoPA**

As a non-micro organisation engaged in health data processing, Urathon Europe Ltd is required by **Article 30** to maintain a detailed **Record of Processing Activities (RoPA)**.

13.2 **Required Content**

The RoPA must include:

- The name and contact details of the controller and DPO
- Purposes of processing
- Categories of data subjects and personal data
- Categories of recipients
- Data transfers to third countries
- Envisaged retention periods
- Security measures applied to each processing activity

13.3 **Maintenance and Review**

The RoPA is owned by the DPO and maintained in a digital compliance register. It is reviewed every six months, or sooner where a new processing activity is introduced (e.g., launch of a CGM monitoring feature).

13.4 **Audit and Disclosure**

The RoPA must be made available to the ICO on request without undue delay. Process owners must cooperate with audits to validate the RoPA entries.

SECTION 14: DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

14.1 **Triggering Conditions**

A **Data Protection Impact Assessment (DPIA)** must be undertaken before any processing operation likely to result in high risk to individuals. This includes:

- Processing of biometric data (CGM analytics, wearable integration)
- Large-scale monitoring of device usage or patient data
- Systematic profiling for marketing or clinical outcomes
- New digital platform or mobile app deployments

14.2 **Content of DPIA**

Each DPIA must include:

- A description of the planned processing
- An assessment of necessity and proportionality
- Identification of potential risks to individuals
- Measures to mitigate those risks

14.3 **Approval and Recordkeeping**

All DPIAs must be reviewed and approved by the DPO. Where high residual risk remains, the ICO must be consulted prior to proceeding with processing.

14.4 **Templates and Registry**

The Company maintains a DPIA template and a DPIA Registry, both monitored by the DPO and subject to annual audit by the Risk Committee.

SECTION 15: DATA BREACH NOTIFICATION AND RESPONSE

15.1 **Definition of a Personal Data Breach**

A data breach is a breach of security leading to the accidental or unlawful destruction, loss,

alteration, unauthorised disclosure of, or access to personal data. This includes digital, physical, or verbal breaches.

15.2 **Obligations Under UK GDPR**

Urathon must:

- Notify the ICO within **72 hours** of becoming aware of a breach (Article 33)
- Inform affected individuals **without undue delay** where there is a high risk to rights and freedoms (Article 34)
- Maintain a breach register recording all incidents and actions taken

15.3 **Breach Response Procedure**

Steps in the response process include:

1. Identification by staff or automated alerts
2. Initial triage by IT Security
3. Notification of the DPO
4. Internal containment and mitigation
5. Root cause analysis
6. ICO notification (if required)
7. Communication to affected data subjects (if applicable)
8. Post-incident review

15.4 **Staff Duties**

All employees must report any suspected breach within **2 hours** to the DPO or Information Security Officer using the internal incident report form.

15.5 **Disciplinary Action**

Deliberate or negligent breaches of data security will be treated as misconduct and may result in disciplinary measures up to and including termination of employment.

SECTION 16: TRAINING AND AWARENESS

16.1 **Mandatory Staff Training**

All staff, contractors, and agency workers employed by Urathon Europe Ltd must complete mandatory GDPR and Data Protection training:

- Within **14 days** of starting employment
- **Annually** thereafter
- Immediately following a serious breach or legislative update

16.2 **Training Content**

Training shall include:

- Principles of UK GDPR and DPA 2018
- Data subject rights and handling of SARs
- Lawful basis, special category data, consent
- Clinical and product data protection (CGM/mobility aid specific)
- Breach detection and reporting
- Cybersecurity best practices

16.3 **Specialist and Role-Specific Training**

Additional training is provided to:

- Engineers and developers (secure coding, DCB0129)
- Customer service staff (SAR recognition, verbal disclosures)
- Procurement officers (vendor due diligence and DPAs)
- Marketing staff (PECR and consent-based campaigns)

16.4 **Training Records and Compliance**

Attendance is logged in the **HR compliance system** and monitored by the **Information Governance Team**. Staff who fail to complete training within deadlines may be suspended from access to systems containing personal data.

SECTION 17: PRIVACY BY DESIGN AND DEFAULT

17.1 **Design Philosophy**

In compliance with **Article 25 UK GDPR**, Urathon Europe Ltd shall adopt **privacy by design and by default** principles in the architecture and deployment of all products, services, and processes.

17.2 **Applications to Product Development**

All digital platforms (e.g., CGM dashboards, mobility aid apps) must:

- Limit personal data visibility to what is strictly necessary
- Present data subjects with privacy controls at the point of use
- Embed anonymisation and pseudonymisation where feasible
- Prevent unauthorised access through logical access controls
- Record every processing purpose at design stage

17.3 **Cross-Departmental Collaboration**

The DPO must be engaged from the beginning of every project lifecycle involving personal data. This includes collaboration with:

- R&D/engineering teams for sensor or software design
- Legal for licensing and compliance frameworks
- Marketing for audience profiling
- IT for storage, hosting, and access decisions

17.4 **Technical Controls**

Design specifications must mandate:

- Data minimisation in APIs and databases
- Default encryption-at-rest
- Non-persistent storage of session data unless justified
- No user tracking without explicit and informed opt-in

SECTION 18: DIRECT MARKETING, COOKIES, AND PECR COMPLIANCE

18.1 **Direct Marketing Principles**

All direct electronic marketing activities by Urathon Europe Ltd must comply with:

- **UK GDPR** (lawful basis and transparency)
- **PECR** (electronic communications rules)
- ICO's Code of Practice on Direct Marketing

18.2 **Lawful Basis for Email or SMS Marketing**

Email or SMS campaigns must be conducted under either:

- Prior **opt-in consent**, OR

- **Soft opt-in** (where the data was obtained during a sale and relates to similar products/services, and an unsubscribe was offered at point of capture)

18.3 **Opt-Out Mechanisms**

All messages must contain a clear unsubscribe link or free-of-charge method for opting out. The system must automatically suppress future mailings upon request.

18.4 **Cookies and Tracking Technologies**

Any website or application operated by Urathon that uses cookies must:

- Provide a clear and visible cookie banner on first visit
- Group cookies by function (essential, analytics, marketing)
- Prevent deployment of non-essential cookies unless and until consent is given
- Provide a full cookie policy explaining duration, controller, and purpose

18.5 **Children and Vulnerable Users**

Marketing systems must implement safeguards to prevent profiling or advertising to users under the age of 13 or users who have not consented to profiling.

SECTION 19: NHS, PUBLIC SECTOR, AND TRANSPARENCY OBLIGATIONS

19.1 **Public Sector Interface**

Urathon Europe Ltd engages with NHS entities, Integrated Care Boards (ICBs), and other UK health authorities. In these contexts, additional obligations apply:

- Compliance with **NHS Data Security and Protection Toolkit (DSPT)**
- Conformance with **NHS Digital's DCB0129 and DCB0160 standards**
- Adherence to **FOIA 2000** for relevant information requests
- Observance of NHS data sharing principles, including duty of confidentiality

19.2 **Clinical Safety Cases**

CGM-related solutions must be accompanied by a **Clinical Safety Case** and designated **Clinical Safety Officer (CSO)**under NHS framework agreements.

19.3 **Open Contracting and Tender Transparency**

Where personal data is processed in relation to public sector contracts, Urathon must maintain:

- An internal **Public Sector Data Access Register**
- FOIA response protocols
- Transparency logs of contractually mandated data flows

19.4 **Medical Device Tracking (MDR/UDI)**

Mobility aid devices and CGM systems must be registered under Unique Device Identification (UDI) schemes and be available for inspection by MHRA and NHS procurement bodies.

SECTION 20: POLICY GOVERNANCE, ENFORCEMENT, AND VERSION CONTROL

20.1 **Ownership and Approval**

This policy is owned by the **Head of Legal and Data Protection** and is approved by the **Board of Directors**. The **DPO**is responsible for ensuring its operational implementation and review.

20.2 **Enforcement**

Failure to adhere to this policy may result in:

- Internal disciplinary action (for employees)
- Termination of service contracts (for vendors)
- Regulatory penalties (ICO fines up to £17.5 million or 4% of annual turnover)
- Liability in civil claims brought under **Article 82** or the **DPA 2018**

20.3 **Policy Updates**

This policy is reviewed:

- **Annually**, or
- Immediately following material legal, operational, or technological changes

20.4 **Distribution and Publication**

The policy is published internally via the staff intranet and externally upon request.

Contractors and vendors must sign a confirmation of policy adherence during onboarding.

20.5 **Change History**

Version	Date	Change Summary	Author
1.0	May 2025	Initial release	DPO, Legal & Compliance