

DECISION WHEEL



FORERUNNER
DIGITAL

DECISION WHEEL PRIVACY POLICY

Document version: V1
Effective date: 10/11/2026
Last updated: 10/11/2026
Service provider: Forerunner Ltd
Contact email: sales@decisionwheel.io

1. Introduction

Forerunner Digital Ltd ("Forerunner", "we", "us" or "our") is committed to protecting personal data and respecting the privacy of individuals who interact with Decision Wheel.

Decision Wheel is an enterprise-level data collection, decision-support and visualisation platform that enables organisations to create configurable forms, collect information, apply scoring and weighting methodologies, and present results through a range of visual formats.

This Privacy Policy explains how personal data is collected, used, stored, shared and protected in connection with:

- The Decision Wheel website.
- The Decision Wheel software platform.
- Customer accounts and subscriptions.
- Authentication and user access.
- Customer enquiries, communications and technical support.
- Our related business and administrative activities.

We process personal data in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, as amended, and the EU General Data Protection Regulation (EU GDPR), where applicable.

This Privacy Policy should be read alongside our Terms of Service and, where applicable, our Data Processing Agreement (DPA).

2. Who We Are and Our Data Protection Responsibilities

Decision Wheel is developed and provided by:

Forerunner Ltd
Registered company number: 16596671
United Kingdom
Email: sales@decisionwheel.io

Forerunner may act as either a data controller or a data processor, depending on the nature and purpose of the personal data being processed.

2.1 Where Forerunner Acts as Data Controller

Forerunner acts as a data controller where it determines the purposes and means of processing personal data for its own business activities.

This includes personal data used for:

- Responding to enquiries and prospective customers.
- Establishing and managing customer relationships.
- Administering subscriptions, contracts and payments.
- Managing access to Decision Wheel.
- Providing customer service and technical support.
- Maintaining the security and operational integrity of the platform.
- Complying with applicable legal and regulatory obligations.
- Conducting permitted business communications and marketing.

In these circumstances, Forerunner is responsible for determining the appropriate lawful basis for processing and fulfilling its applicable data protection obligations.

2.2 Where Forerunner Acts as Data Processor

Where an organisation uses Decision Wheel to collect, store, analyse or visualise personal data for its own purposes, that organisation will generally act as the data controller.

Forerunner will generally act as a data processor when hosting or otherwise processing that personal data on behalf of the Customer.

In these circumstances:

- The Customer determines the purposes and lawful basis for processing.

- The Customer determines what information is collected through its forms and assessments.
- The Customer is responsible for providing appropriate privacy information to affected individuals.
- The Customer determines appropriate retention periods and responds to applicable data subject rights requests.
- Forerunner processes the personal data in accordance with the Customer's documented instructions, the applicable DPA and relevant law.

The respective roles of the parties depend on the actual processing activity and are not determined solely by their contractual descriptions.

3. Personal Data We Collect

The personal data collected depends on an individual's relationship with Forerunner and their use of Decision Wheel.

3.1 Account and Identity Information

When an individual accesses Decision Wheel, we may process:

- Name and email address.
- Organisation name and organisational affiliation.
- Microsoft Entra ID identifiers associated with authentication.
- User account identifiers and tenancy associations.
- User roles, permissions and administrative status.
- Authentication timestamps and security-related access information.
- Account status and relevant access-management records.

Decision Wheel uses Microsoft Entra ID to authenticate users.

Authentication may involve the exchange of identity information between Microsoft identity services and Decision Wheel to establish an authenticated session and determine the user's permitted access.

Forerunner does not require users to provide their Microsoft account passwords directly to Decision Wheel.

3.2 Customer and Subscription Information

Where an individual represents a Customer or prospective Customer, we may collect:

- Name and business contact details.

- Organisation name, address and billing information.
- Job title or organisational role.
- Subscription and contractual information.
- Payment status, invoice records and transaction references.
- Correspondence relating to the customer relationship.

3.3 Technical and Operational Information

When individuals access Decision Wheel, we may process technical information reasonably necessary for operation, security and support, including:

- IP addresses.
- Browser and device information.
- Authentication and access timestamps.
- Application error records and diagnostic information.
- Security logs and records of potentially unauthorised activity.
- Information necessary to investigate technical issues.

Such information is used for legitimate operational purposes, including maintaining service availability, investigating faults, protecting accounts and detecting security threats.

3.4 Communications and Support Information

Where an individual contacts Forerunner, we may process:

- Contact details.
- Information included in emails and enquiries.
- Support requests and descriptions of technical issues.
- Relevant diagnostic information supplied during troubleshooting.
- Correspondence concerning incidents, complaints or contractual matters.

Individuals should avoid including unnecessary personal or sensitive information in support requests.

3.5 Customer-Provided Content

Decision Wheel enables Customers to create forms, collect responses, generate assessments and maintain associated records.

Depending on how a Customer configures and uses the Service, Customer Data may include personal data such as:

- Names and contact details.
- Employment or organisational information.
- Opinions, assessments and responses to questions.
- Information about individuals participating in organisational projects.
- Information contained in supporting documents.
- Other personal data selected and submitted by the Customer or its authorised users.

In some circumstances, Customers may use Decision Wheel to process special category personal data or other sensitive information.

The Customer is responsible for assessing whether such processing is lawful and appropriate and for meeting any additional requirements applicable to that information.

Forerunner does not independently determine which categories of personal data Customers choose to collect through their configured forms and assessments.

4. How We Obtain Personal Data

We may obtain personal data:

- Directly from individuals who contact us.
- From Customers who establish subscriptions or nominate administrators.
- From authorised users who access Decision Wheel.
- From Microsoft Entra ID during authentication.
- Automatically through necessary platform operations and security logging.
- From organisations that invite external collaborators to participate in Decision Wheel activities.
- From professional contacts or business communications.

Where personal data is supplied by a Customer for processing through Decision Wheel, the Customer is generally responsible for establishing a lawful basis for collecting and providing that information.

5. Purposes and Lawful Bases for Processing

Where Forerunner acts as data controller, we process personal data only where we have an appropriate lawful basis under applicable Data Protection Legislation.

Our principal processing activities are outlined below.

PURPOSE	APPLICABLE LAWFUL BASIS
ESTABLISHING AND MANAGING CUSTOMER ACCOUNTS AND SUBSCRIPTIONS	Performance of a contract where the individual is a party to it; otherwise legitimate interests in administering customer relationships
MANAGING USER IDENTITY, AUTHENTICATION AND PERMISSIONS	Legitimate interests in providing a secure service and fulfilling customer agreements
PROVIDING TECHNICAL SUPPORT AND RESPONDING TO ENQUIRIES	Legitimate interests in supporting customers and prospective customers; contract where applicable
MAINTAINING SECURITY, DETECTING MISUSE AND INVESTIGATING INCIDENTS	Legitimate interests in protecting the Service, users and infrastructure; legal obligations where applicable
PROCESSING INVOICES AND FINANCIAL RECORDS	Performance of a contract where applicable, legitimate interests in administering payments, and compliance with legal obligations
MAINTAINING BUSINESS RELATIONSHIPS AND CONDUCTING PERMITTED MARKETING	Legitimate interests or consent, as appropriate and subject to applicable electronic marketing rules
RESPONDING TO LEGAL REQUESTS AND FULFILLING REGULATORY REQUIREMENTS	Compliance with legal obligations where applicable

Where we rely on legitimate interests, we consider the necessity of the processing and balance those interests against the rights and freedoms of affected individuals.

Where we rely on consent, individuals may withdraw that consent at any time. Withdrawal shall not affect the lawfulness of processing undertaken before consent was withdrawn.

5.1 Processing on Behalf of Customers

Where Forerunner acts as data processor, we do not independently select the Customer's lawful basis for processing Customer Data.

The Customer determines the purposes and lawful basis of processing, while Forerunner processes the information in accordance with the DPA, documented instructions and applicable law.

6. How We Use Customer Data

Customer Data is processed for the purpose of delivering the functionality requested by the Customer.

This may include:

- Storing and retrieving forms, questions and answers.
- Collecting and displaying responses.
- Applying Customer-defined scoring and weighting configurations.
- Generating visualisations, reports and PDF exports.
- Managing authorised user access.
- Maintaining relevant version histories and audit records.
- Supporting security, backup and recovery arrangements.
- Providing technical support and investigating faults.
- Carrying out authorised data retrieval, export and deletion operations.

Customer Data is not used by Forerunner for unrelated commercial activities or independent. **We do not sell Customer Data to third parties.**

6.1 Decision-Support Functionality

Decision Wheel enables Customers to establish scoring methodologies and produce visual assessments from the information they collect.

Forerunner does not independently determine decisions made by Customers about individuals.

A Customer may use the platform as part of a wider decision-making process. The Customer is responsible for determining whether its use involves profiling or solely automated decision-making and for providing appropriate information, safeguards and rights where required by law.

Individuals with concerns about decisions made by an organisation using Decision Wheel should contact that organisation in the first instance.

7. Personal Data Protection and Disclosure

Forerunner is committed to minimising the personal information collected, stored and processed by Decision Wheel.

7.1 User Authentication and Identification

Decision Wheel uses Microsoft Entra ID to authenticate users.

During the initial authentication process, Decision Wheel receives the identity information necessary to verify the user and establish their access to the Service.

Identifying user information is then hashed and associated with a unique Globally Unique Identifier (GUID). Decision Wheel uses this GUID to reference the user throughout its internal systems, rather than routinely processing their directly identifying personal information.

This approach is designed to minimise the use of personal information within the platform and reduce the risk of individuals being identified through internal application records.

7.2 Personal Data Disclosure

Forerunner does not sell, distribute or voluntarily disclose users' personal information to independent third parties.

We do not share users' personal information for advertising, marketing, profiling, commercial analysis or any other purpose unrelated to providing Decision Wheel.

Microsoft Entra ID is used for authentication, and Microsoft Azure provides the underlying hosting infrastructure. These services process information as necessary to perform their respective functions, subject to applicable contractual, security and data protection requirements.

Forerunner does not independently provide identifiable user information to these providers for unrelated purposes.

Personal data may be disclosed where expressly authorised by the relevant Customer or where Forerunner is legally required to do so by applicable law or a binding requirement issued by a competent authority.

Where disclosure is legally required, Forerunner shall comply with the safeguards and notification requirements described in Section 18 of its Terms of Service, where applicable.

7.3 Customer Data

Information entered into Decision Wheel by Customers and their authorised users remains under the control of the relevant Customer.

Forerunner does not disclose Customer Data to independent third parties for their own purposes.

Customer Data is processed only as necessary to provide, maintain, secure and support Decision Wheel, in accordance with the Customer's instructions, the applicable Data Processing Agreement and legal obligations.

8. Data Hosting and International Transfers

Decision Wheel is hosted using Microsoft Azure infrastructure.

8.1 Customer-Selected Hosting Regions

Customers may select their preferred hosting region from the Microsoft Azure regions supported and made available by Forerunner when their tenancy is provisioned.

The selected region determines the intended primary location of the Customer's tenancy and associated data.

However, certain supporting services, authentication processes, infrastructure operations, technical support activities, backups or disaster recovery arrangements may involve processing or access outside the selected region.

Selection of a hosting region does not, by itself, guarantee that all associated personal data remains exclusively within that geographical location.

8.2 International Transfers

Where personal data is transferred outside the United Kingdom or European Economic Area, as applicable, Forerunner takes appropriate steps to ensure that the transfer complies with relevant Data Protection Legislation.

Depending on the circumstances, safeguards may include:

- Applicable UK adequacy regulations.
- European Commission adequacy decisions.
- Approved Standard Contractual Clauses.
- The UK International Data Transfer Agreement.
- The UK Addendum to the EU Standard Contractual Clauses.
- Supplementary technical, contractual or organisational safeguards where required.

Customers may request further information about relevant hosting and international transfer arrangements using the contact details in this Privacy Policy.

9. Data Security

Forerunner is committed to protecting the confidentiality, integrity and availability of information processed through Decision Wheel.

The platform has been designed with data protection and security as fundamental considerations, incorporating principles of privacy by design, data minimisation, pseudonymisation and restricted access.

We implement appropriate technical and organisational measures designed to protect personal data and Customer Data against unauthorised access, disclosure, alteration, loss, misuse and destruction.

9.1 Authentication and Personal Data Minimisation

Decision Wheel uses Microsoft Entra ID to authenticate users and verify their identity when accessing the Service.

During authentication, the platform receives the identity information necessary to establish and validate the user's access.

Identifying user details are hashed and associated with a unique Globally Unique Identifier (GUID), which is subsequently used to reference the user within Decision Wheel's internal systems.

This approach minimises the need to use directly identifying personal information within the application's operational records.

The use of hashed identifiers and GUIDs is a form of pseudonymisation rather than complete anonymisation, as individuals may remain identifiable through additional information or authentication systems.

9.2 Access Controls and Tenant Isolation

Decision Wheel implements access controls designed to ensure that users and application components can access only the information and functionality they are authorised to use.

These measures include:

- Authentication through Microsoft Entra ID.
- Role-based access controls and permissions.
- Separation of customer tenancies and associated information.
- Restricted administrative access based on the principle of least privilege.
- Controlled authentication and authorisation between application services.

- Appropriate safeguards to prevent unauthorised access between customer environments.

Customers are responsible for managing their authorised users and ensuring that permissions are assigned appropriately.

9.3 Encryption and Information Protection

Decision Wheel uses encryption and cryptographic security measures to protect information processed and stored within the platform.

These measures include appropriate encryption of stored information, secure communications between application components and controls governing access to encryption keys.

Customer information and historical records are protected using security measures appropriate to their sensitivity and the technical architecture of the Service.

Where supported by the relevant platform functionality, cryptographic controls also enable the removal or redaction of information while preserving the integrity of associated audit structures.

9.4 Infrastructure and Operational Security

Decision Wheel is hosted using Microsoft Azure infrastructure and incorporates security controls designed to protect the Service and its supporting systems.

These measures include:

- Restricted access to application services and infrastructure.
- Security monitoring and vulnerability management.
- Controlled software deployment and change-management procedures.
- Appropriate backup and disaster recovery arrangements.
- Security incident detection, investigation and response procedures.
- Periodic review of security configurations and access permissions.

Forerunner takes reasonable steps to identify and address security vulnerabilities and to maintain appropriate safeguards as the platform and its underlying technologies evolve.

9.5 Protection of Customer Data

Customer Data remains under the control of the relevant Customer and is processed by Forerunner only as necessary to provide, maintain, secure and support Decision Wheel, in accordance with the Customer's instructions, the applicable Data Processing Agreement and legal obligations.

Forerunner does not voluntarily disclose Customer Data to independent third parties for unrelated purposes.

Access to Customer Data by Forerunner personnel or authorised service providers is restricted to circumstances where such access is necessary for legitimate service operations and is subject to appropriate confidentiality and security obligations.

Customer Data will only be disclosed to external parties for their independent purposes where expressly authorised by the Customer or legally required, subject to the safeguards described in the Terms of Service.

9.6 Security Monitoring and Incident Response

Forerunner maintains procedures designed to identify, investigate, contain and respond to potential security incidents affecting Decision Wheel.

Where a personal data breach affects information processed on behalf of a Customer, Forerunner shall notify the Customer without undue delay and provide reasonable information and assistance in accordance with the applicable Data Processing Agreement and Data Protection Legislation.

We periodically review our security arrangements and take reasonable steps to address identified vulnerabilities and emerging risks.

While no internet-connected service can guarantee absolute security, Forerunner is committed to maintaining appropriate and proportionate safeguards to protect information entrusted to Decision Wheel.

10. Data Retention and Deletion

We retain personal data only for as long as reasonably necessary for the purposes for which it is processed, subject to applicable legal requirements and the Customer's instructions where Forerunner acts as data processor.

10.1 Customer Data

Where a Customer uses the standard Decision Wheel hosting arrangement, Customer Data may be retained for up to six (6) months following termination or expiry of the subscription for the purpose of allowing data retrieval.

This six-month grace period applies only where consistent with the Customer's documented instructions and the applicable DPA.

Customers may instruct Forerunner to return or delete personal data in accordance with the DPA, including requesting earlier deletion.

Following an applicable deletion instruction or the expiry of the authorised retention period, Customer Data shall be deleted from active Forerunner-managed systems, subject to any legal retention requirements and applicable backup procedures.

10.2 Customer-Controlled Databases

Where a Customer elects to use its own database infrastructure, the Customer is responsible for the retention, backup and deletion of information held within that database.

Forerunner remains responsible for personal data processed within systems under its own control, in accordance with the DPA and applicable law.

10.3 Backup Data

Residual copies of information may remain temporarily within protected backup and disaster recovery systems until they are deleted or expire in accordance with the applicable backup retention schedule.

Such information remains subject to appropriate security restrictions and the deletion obligations set out in the applicable DPA.

10.4 Business and Administrative Records

Personal data relating to customer relationships, subscription administration, communications, security and financial records is retained according to the purpose for which it was collected and applicable legal obligations.

Relevant retention criteria include:

- The duration of the customer relationship.
- The period reasonably necessary to resolve enquiries or disputes.
- Applicable accounting and taxation requirements.
- Security investigation and operational requirements.
- Relevant legal limitation periods.

Further information about specific retention periods may be requested from Forerunner.

11. Cookies, Authentication Storage and Similar Technologies

Decision Wheel uses authentication and related technologies necessary to provide secure access to the platform.

These may include cookies, session storage or other browser-based mechanisms used to:

- Maintain authenticated sessions.

- Support Microsoft Entra ID authentication.
- Protect against unauthorised access and security threats.
- Maintain essential application functionality.
- Preserve necessary security-related session information.

Decision Wheel does not currently use advertising or behavioural tracking analytics as part of the Service.

Where cookies or similar technologies are strictly necessary to provide a service requested by the user, consent may not be required under applicable law.

Where we introduce technologies requiring consent, we shall provide appropriate information and obtain consent where required before using them.

Users may manage certain browser storage settings, although blocking essential authentication or session technologies may prevent Decision Wheel from operating correctly.

Any additional cookies or similar technologies used on the public Decision Wheel website shall be identified and addressed in the applicable cookie information.

12. Individual Rights

Depending on the circumstances and applicable Data Protection Legislation, individuals may have rights to:

- Request access to their personal data.
- Request correction of inaccurate information.
- Request deletion of personal data.
- Request restriction of processing.
- Object to certain processing activities.
- Request portability of personal data, where applicable.
- Withdraw consent where consent is the applicable lawful basis.
- Exercise applicable rights relating to solely automated decisions.
- Lodge a complaint with a competent data protection supervisory authority.

These rights may be subject to statutory conditions and exceptions.

12.1 Where Forerunner Is the Data Controller

Individuals may contact Forerunner using the details in Section 15 to exercise their applicable data protection rights.

We may request information reasonably necessary to verify an individual's identity before responding to a request.

We shall respond within the periods required by applicable Data Protection Legislation.

12.2 Where Forerunner Is the Data Processor

Where personal data has been collected by an organisation using Decision Wheel, the organisation will generally be responsible for responding to requests relating to that information.

Individuals should contact the relevant organisation directly.

Where Forerunner receives such a request, we may refer it to the relevant Customer and provide appropriate assistance in accordance with the DPA and applicable law.

13. Data Protection Complaints

Individuals who have concerns about Forerunner's handling of their personal data may submit a complaint to us using the contact details in Section 15.

We shall maintain a process for receiving and investigating data protection complaints.

In accordance with applicable UK requirements, we shall:

- Acknowledge receipt of a data protection complaint within thirty (30) days.
- Take appropriate steps to investigate the complaint without undue delay.
- Keep the complainant reasonably informed of relevant progress.
- Communicate the outcome without undue delay following the investigation.

Individuals may also complain to the UK Information Commissioner's Office (ICO):

Information Commissioner's Office
Website: https://ico.org.uk

Where the EU GDPR applies, individuals may have the right to complain to the competent data protection supervisory authority in the relevant EU Member State.

We encourage individuals to contact us first where appropriate so that we have an opportunity to address their concerns.

14. Changes to This Privacy Policy

Forerunner may update this Privacy Policy to reflect changes in:

- Applicable data protection legislation.
- Decision Wheel functionality.

- Our processing activities.
- Security and hosting arrangements.
- Our business operations.
- Regulatory guidance or legal obligations.

The most recent version shall be made available through the Decision Wheel website or platform.

Where changes materially affect how personal data is processed, we shall provide additional information or notification where required by applicable law.

Updates shall not retrospectively authorise processing that requires a separate lawful basis, notice or consent.

15. Contact Details

For questions, requests or complaints concerning this Privacy Policy or the processing of personal data, please contact:

Forerunner Digital Ltd
Email: sales@decisionwheel.io
Technical support: support@decisionwheel.io
Tel: +44 (0)1872 248 542

Where applicable, the contact details of any appointed Data Protection Officer or EU representative shall also be published here.

Individuals should include sufficient information to help us identify and respond to their enquiry, but should avoid sending unnecessary sensitive personal data by ordinary email.