

Viewplus Ireland and Ordis UK website Privacy Statement

Contents

1. INTRODUCTION..... 2

2. CONTACT DETAILS 2

3. SENSITIVE DATA 3

4. HOW WE COLLECT YOUR PERSONAL DATA..... 3

5. MARKETING COMMUNICATIONS 4

6. DISCLOSURES OF YOUR PERSONAL DATA 5

7. TRANSFER OF PERSONAL DATA 5

8. DATA SECURITY 5

9. DATA RETENTION 7

10. YOUR LEGAL RIGHTS..... 8

11. THIRD-PARTY LINKS 8

1. INTRODUCTION

This privacy notice provides you with details of how we collect and process your personal data through your use of our site: <https://ordishealthcare.com/>

By providing us with your data, you guarantee us that you are over 18 years of age.

2. CONTACT DETAILS

Our full details are Full name of legal entity: **(Ireland)** Viewplus Ireland Limited and **(UK)** Ordis UK Ltd

Name of person responsible for data protection: The manager

Email address: info@ordishealthcare.com

Postal address:

Ireland - The View, Marina Village, Malahide, Dublin, K36 CX99, Ireland

UK- Unit D Pendyris St, Cardiff CF11 6BH with the Company Number 17083318

It is very important that the information we gather about you is accurate and up to date. Please let us know if at any time your personal information changes by emailing us info@ordishealthcare.com

2. WHAT DATA DO WE COLLECT ABOUT YOU, FOR WHAT PURPOSE AND ON WHAT GROUND WE PROCESS IT

Personal data means any information capable of identifying an individual. It does not include anonymised data.

We may process the following categories of personal data about you:

- **Communication Data** that includes any communication that you send to us whether that be through the contact form on our website, through email, text, social media messaging, social media posting or any other communication that you send us. We process this data for the purposes of communicating with you, for record keeping and for the establishment, pursuance or defense of legal claims. Our lawful ground for this processing is our legitimate interests which in this case are to reply to communications sent to us, to keep records and to establish, pursue or defend legal claims.
- **Customer Data**- that includes data relating to any purchases of goods and/or services such as your name, title, billing address, delivery address email address, phone number, contact details, purchase details and your card details. We process this data to supply the goods and/or services you have purchased and to keep records of such transactions. Our lawful ground for this processing is the performance of a contract between you and us and/or taking steps at your request to enter into such a contract.
- **User Data**- that includes data about how you use our website and any online services together with any data that you post for publication on our website or through other online services. We process this data to operate our website and ensure relevant content is provided to you, to ensure the security of our website, to maintain back- ups of our website and/or databases and to enable publication and administration of our website, other online services and business. Our lawful ground for this processing is our legitimate interests which in this case are to enable us to properly administer our website and our business.

- **Technical Data** that includes data about your use of our website and online services such as your IP address, your login data, details about your browser, length of visit to pages on our website, page views and navigation paths, details about the number of times you use our website, time zone settings and other technology on the devices you use to access our website. The source of this data is from our analytics tracking system. We process this data to analyse your use of our website and other online services, to administer and protect our business and website, to deliver relevant website content and advertisements to you and to understand the effectiveness of our advertising. Our lawful ground for this processing is our legitimate interests which in this case are to enable us to properly administer our website and our business and to grow our business and to decide our marketing strategy. Please also review the new changes to User Data under the GA4 category listed below.
- **Marketing Data** that includes data about your preferences in receiving marketing from us and our third parties and your communication preferences. We process this data to enable you to partake in our promotions such as competitions, prize draws and free giveaways, to deliver relevant website content and advertisements to you and measure or understand the effectiveness of this advertising. Our lawful ground for this processing is our legitimate interests which in this case are to study how customers use our products/services, to develop them, to grow our business and to decide our marketing strategy. Please also review the new changes to User Data under the GA4 category listed below.
- We may use Customer Data, User Data, Technical Data and Marketing Data to deliver relevant website content and advertisements to you (including Facebook adverts or other display advertisements) and to measure or understand the effectiveness of the advertising we serve you. Our lawful ground for this processing is legitimate interests which is to grow our business. We may also use such data to send other marketing communications to you. Our lawful ground for this processing is either consent or legitimate interests (namely to grow our business).

3. SENSITIVE DATA

Viewplus Ireland Ltd/ Ordis UK will capture sensitive data during the course of your relationship with us. This information will be disclosed at sign-up and will be treated with the utmost discretion. We will only store this information if it is relevant to the performance of our contract and will be anonymised when the contract ends.

We will not collect sensitive information about you without first obtaining your consent, and we will only use or disclose your sensitive information as permitted via the contract, required, or authorized by law.

4. HOW WE COLLECT YOUR PERSONAL DATA

Google Analytics

We may collect data about you by you providing the data directly to us (for example by filling in forms on our site or by sending us emails). We may automatically collect certain data from you as you use our website by using cookies and similar technologies.

We may receive data from third parties such as analytics providers such as Google based outside the EU, advertising networks such as Facebook based outside the EU, such as search information providers such as Google based outside the EU, providers of technical, payment and delivery services, such as data brokers or aggregators.

As a visitor to this website, we may be using Google fonts and as such your IP address will be made available to Google. Please note that Google can have access to your IP address and/or personal when their platform is used in the performance of the website. Many websites and apps use Google services to improve their

content and keep it free. When they integrate our services, these sites and apps share information with Google. In order to learn more about the kind of information that is used please click on <https://policies.google.com/technologies/partner-sites?hl=en-US>.

As per Google, GA4 will collect the below features:

- How they collect both website and app data to understand the customer journey better.
- Uses events instead of session-based data.
- Includes privacy controls such as cookieless measurement and behavioral and conversion modeling.
- Predictive capabilities offer guidance without complex models.
- Direct integrations to media platforms help drive actions.
- IP anonymization is always enabled for GA4 properties & no manual action is required.
- Google Analytics 4 uses IP only to determine where to record other personal data of users, and then it is deleted.

GA4 will no longer monitor sessions and pageviews but instead monitor events and parameters.

Events are divided by:

Automatically collected events:

The following parameters are collected by default with every event, including custom events:

- language;
- page location
- page referrer
- page title
- screen resolution

Enhanced Measurement events – These events allow measuring interactions with the website's content by enabling options (events) in the Google Analytics interface. These events include scrolls, outbound clicks, site search, and video engagement.

Recommended Events – These are events recommended by Google to help measure additional features and behavior and generate more detailed reports.

Custom Events – Events and parameters that can be created and implemented based on website requirements.

How Long does GA4 retain data:

While for Universal Analytics user-level and event-level data properties could have an indefinite duration, user-level data can be retained for a maximum of 14 months for Google Analytics 4 properties.

For more information on how Google and GA4 collects your data please review the following link: <https://policies.google.com/terms?hl=en-US>.

5. MARKETING COMMUNICATIONS

Our lawful ground for processing your personal data to send you marketing communications is either your consent or our legitimate interests (namely to grow our business).

You can ask us or third parties to stop sending you marketing messages at any time [by logging into the website and checking or unchecking relevant boxes to adjust your marketing preferences] OR [by following the opt-out links on any marketing message sent to you or] OR by emailing us at info@ordishealthcare.com

If you opt out of receiving marketing communications this opt-out does not apply to personal data provided as a result of other transactions, such as purchases, warranty registrations etc.

6. DISCLOSURES OF YOUR PERSONAL DATA

We may have to share your personal data with the parties listed below:

- Service providers who provide IT and system administration services.
- Professional advisers including lawyers, bankers, auditors, and insurers.
- Third parties to whom we sell, transfer, or merge parts of our business or our assets.
- Google – our email and meeting platform
- Amazon Web Services (AWS): hosting, storage and networking
- Calendly – for demo appointments
- Wordpress - for website hosting and form submission
- Asana - for project management tracking

7. TRANSFER OF PERSONAL DATA

Viewplus Ireland Ltd and Ordis UK Ltd use WordPress as our website platform. WordPress has servers that are based within Europe. We also use NameCheap for the hosting of our website, and they have servers located in Europe.

Also, if you synchronize your data, it may be transferred to and processed in countries outside your own, including the UK which is covered with an adequacy decision.

We ensure that such transfers comply with applicable laws and are protected by safeguards, including EU & UK Data Processing Agreements.

8. DATA SECURITY

Ordis - Data Protection & Processing Architecture Brief Overview.

Processing Architecture Model

Ordis uses a **self-hosted processing architecture within isolated EU/UK cloud environments.**

- All core processing occurs within AWS regions:
 - Ireland (eu-west-1)
 - United Kingdom (eu-west-2)
- Infrastructure is deployed within a **Virtual Private Cloud (VPC)** with:
 - Private subnets for sensitive processing components
 - No direct public access to databases or AI models
- Application access is controlled via:
 - Web Application Firewall (WAF)
 - Application Load Balancer (ALB)
 - TLS 1.2+ encrypted connections

This architecture ensures that **all primary processing remains within controlled, region-specific environments.**

Data Flow and Processing Controls

The Ordis data pipeline enforces strict minimisation and isolation:

1. Audio is captured via PWA or mobile application
2. Data is transmitted securely over TLS 1.2+
3. Audio is processed within the private subnet using a self-hosted speech-to-text model
4. A **PII reduction layer** removes or masks identifiable data (e.g. names, DOB, PPS/NHS numbers)
5. A self-hosted language model structures the transcript into clinical documentation formats
6. Output is stored in encrypted databases and presented for clinical review

Key controls:

- No raw audio leaves the controlled environment
- Identifiable data is minimised before any downstream processing
- All outputs require **human validation prior to finalisation**

Data Residency and Sovereignty

Ordis enforces strict data residency controls:

- Irish deployments: data processed and stored in AWS Dublin region
- UK deployments: data processed and stored in AWS London region
- No cross-region replication outside these jurisdictions
- All storage systems (MongoDB, S3, Glacier) are region-bound

Data residency applies to all **primary processing, storage, and retention layers**.

Sub-processors

Ordis utilises a limited set of infrastructure sub-processors:

- Amazon Web Services (AWS) – hosting, compute, storage, and networking

Sub-processors:

- Operate exclusively within EU/UK regions
- Are bound by Data Processing Agreements
- Act solely on instructions from Ordis
- Do not access or use data for independent purposes

No third-party AI processors are used in the primary processing flow.

Data Categories Processed

Ordis processes the following categories of personal data:

- Health and care-related data (clinical notes, observations, incident reports)
- Audio recordings (short-term, for transcription purposes only)
- Transcribed text derived from speech
- Structured care documentation
- Limited identifiers (e.g. resident name, date of birth) where required for care documentation

All processing is limited to what is necessary to support care documentation workflows.

Legal Basis for Processing

Processing is carried out under the instruction of the data controller.

Typical legal bases applied by the controller include:

- Performance of a contract (care provision)
- Provision of health or social care (GDPR Article 9(2)(h))

Ordis does not independently determine the legal basis for processing.

Data Retention Policy

Ordis implements a tiered retention model aligned with healthcare regulations:

- Audio data: retained for up to 10 days, then permanently deleted
- Structured care records: retained for up to 7 years
- Long-term archival: stored in encrypted, immutable (WORM) storage

Retention policies are:

- Configurable where required by the controller
- Fully auditable
- Enforced through automated lifecycle management

Security Measures

Ordis implements technical and organisational measures aligned with GDPR Article 32:

- Encryption at rest (AES-256 with KMS key management)
- Encryption in transit (TLS 1.2+)
- Network isolation (VPC, private subnets, NAT-controlled outbound traffic)
- Web Application Firewall (WAF) protection
- Role-based access control (RBAC)
- Monitoring and alerting via SNS
- Regular system and infrastructure updates

AI Processing and Risk Controls

Ordis functions as a **documentation support system**, not a clinical decision-making system.

Risk controls include:

- PII reduction prior to AI processing
- Self-hosted AI models within controlled infrastructure
- Full audit logging of system activity
- Mandatory human review of all outputs
- No autonomous clinical decisions or recommendations

Audit and Accountability

Ordis supports compliance and audit requirements through:

- Structured data logging
- Controlled access to processing records
- Defined retention and deletion policies
- Infrastructure-level monitoring and alerting

Audit information can be made available to the controller upon request.

Summary Position

- All primary processing is conducted within EU/UK-controlled infrastructure
- Data exposure is minimised through architectural design
- No external AI services are used in standard operation
- The system is designed to support GDPR, DSPT, and HIQA/CQC compliance requirements

Ordis maintains a **compliance-first architecture**, ensuring that data protection is embedded into both system design and operational processes.

9. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

When deciding what the correct time is to keep the data for, we look at its amount, nature and sensitivity, potential risk of harm from unauthorized use or disclosure, the processing purposes, if these can be achieved by other means and legal requirements.

During the performance of our contract some personal data may be transferred through our operating systems. We treat this information with the utmost importance and given the sensitivity and possible legal consequences which could be attached to the retention of this material we operate a specific retention period for this area. We will store this information for seven calendar years after it has been captured and the services we offer have been completed and upon which time it will then be deleted.

For tax purposes the law requires us to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for seven years after they stop being customers.

In some circumstances we may anonymise your personal data for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

Please note you can always delete your information on your device at any time.

10. YOUR LEGAL RIGHTS

Under data protection laws you have rights in relation to your personal data that include the right to request access, correction, erasure, restriction, transfer, to object to processing, to portability of data and (where the lawful ground of processing is consent) to withdraw consent.

For Ireland you can see more about these rights at: <https://www.dataprotection.ie/> and for the UK at <https://ico.org.uk/>

If you wish to exercise any of the rights set out above, please email us at info@ordishealthcare.com

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive or refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you.

If you are not happy with any aspect of how we collect and use your data, you have the right to complain to the Data Protection Commission's Office <https://www.dataprotection.ie/> or for the UK this is the Information Commissioner's Office [Information Commissioner's Office](https://ico.org.uk/). We should be grateful if you would contact us first if you do have a complaint so that we can try to resolve it for you.

11. THIRD-PARTY LINKS

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit. Examples of our third-party links are; Calendly - this is not an extensive link and some of these platforms may not be in operation at the current time. There will also be other third-party links attached to the WordPress platform which are used to enhance the performance of the website. Please note this is not an exhaustive list and can be added to or deleted to as this website evolves.