

# Supplier Privacy Notice

Effective 9 June 2025

Oxehealth Limited and/or its subsidiaries ("Oxehealth", "we", "us", or the "Company") are responsible for the processing of your Personal Data as described in this Privacy Notice, unless specified otherwise. As the controller of your Personal Data, we determine how and why your data is processed and ensure that all processing activities comply with applicable legal requirements.

At Oxehealth, we respect your privacy and we want to be as transparent as possible about how we collect, use, and protect your data, including Personal Data. For the purposes of this Privacy Notice, "Personal Data" means any information that relates to an identified or identifiable individual and includes what may be referred to as "Personal Information" under applicable US privacy laws.

As a Data Controller we are committed to complying with the relevant data protection laws in the jurisdictions where we operate. This includes but is not limited to the EU and UK General Data Protection Regulations and the California Consumer Privacy Act (as amended by the California Privacy Rights Act).

This Privacy Notice applies specifically to current and past Oxehealth suppliers and to potential new suppliers and sets out the way in which we process, protect, and manage your Personal Data. This includes data provided directly by you or collected from others.

In this notice we will explain who we are, who our Data Protection Officer is, how we collect your information, what information we collect about you and what we use it for, our lawful basis for processing your personal data, how we store and keep your information secure, how long we keep your information for, who your information is shared with, and transfers to third countries. This notice also explains your data rights, including your rights to access, correct, or restrict our use of your personal data, how to contact us about these rights, and how to contact us and the supervisory authorities in the event you have a complaint.

## 1. Who we are

Oxehealth, We, Us, Our refers to the following group of companies:

### **Holding company and main office (UK)**

Oxehealth Limited

Registered in England and Wales, Company Registration Number 08163325

Address: Bee House, Eastern Avenue, Milton Park, Abingdon, England, OX14 4SB

### **Fully owned subsidiaries:**

Oxehealth Inc

Registered in the United States of America, No. 3389479

Address: 9419 North Market Street, Suite 950 Wilmington, 19801 Delaware

Oxehealth AB

Registered in Sweden, Registration Number 559275-7487

Address: Nordenskiöldsgatan 11, 21119 Malmö

## 2. What Personal Data we may collect about you, what we use it for, where we collect it from and our legal basis for processing

### Invoicing and reporting

To process purchase orders and invoices, make payments to suppliers and for financial reporting we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> <li>• Supplier staff Name</li> <li>• Vat No</li> <li>• Bank Details (may be personal bank details if supplier is a sole trader)</li> </ul>	<ul style="list-style-type: none"> <li>• Directly from the individual or from information provided by the individuals employer (e.g. contract or invoice).</li> </ul>

Oxehealth has a contractual obligation to make payments against supplier invoices and a legitimate interest to manage Oxehealth's financial operations including generating financial reports.

### Communicating

To enable contact with a specific individual at a supplier in order to make decisions on procurement, to procure goods and services, and to discuss customer service issues we may collect and use the following information:

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> <li>• Supplier Staff Name</li> <li>• Work Address</li> <li>• Work Phone</li> <li>• Work Email</li> <li>• Supplier Name</li> </ul>	<ul style="list-style-type: none"> <li>• Directly from the individual or from information provided by the individual's employer.</li> </ul>

Oxehealth has a legitimate interest to correspond with potential suppliers to carry out due diligence and assess the products which they are offering and to correspond with existing suppliers and store relevant information such as contracts to maintain the supplier relationship

### Compliance and audits

To **carry out risk assessment as part of** supply chain management, quality management, and traceability of materials and components used in medical devices.

What Personal Data we collect and use	Where we collect your Personal Data from
---------------------------------------	--

<ul style="list-style-type: none"> <li>• Name</li> <li>• Work Address</li> <li>• Work Phone</li> <li>• Work Email</li> <li>• Supplier Name</li> <li>• Employment and Education History (where required for certain business services)</li> </ul>	<ul style="list-style-type: none"> <li>• Directly from the individual or from information provided by the individual's employer.</li> </ul>
--	---

Oxehealth processes supplier information to comply with its legal obligations under medical device regulations, including quality management, traceability, and regulatory audit requirements, as required by the UK Medical Device Regulations 2002, EU MDR 2017/745, and FDA Quality System Regulation (21 CFR Part 820), and Oxehealth processes supplier information under its legal obligation to ensure compliance with GDPR (Article 28) by maintaining data processing agreements with sub-processors. Additionally Oxehealth has a legitimate interest to conduct supplier due diligence and monitor supplier performance and compliance with agreements.

#### Use of CCTV on Oxehealth Premises:

Oxehealth uses CCTV in selected areas of its premises for the purposes of physical security and access control. Cameras are positioned at entry points and within internal areas where there is a need to monitor access to sensitive infrastructure such as server equipment and stock.

CCTV may also operate in shared office areas, delivery zones, and access routes. Cameras are not installed in private areas such as bathrooms or meeting rooms. The system does not record sound or use facial recognition or biometric technologies. CCTV footage is video-only.

If you attend our premises to make a delivery or perform contracted services, you may be recorded on CCTV while accessing or passing through monitored areas.

What Personal Data we collect and use	Where we collect your Personal Data from
<ul style="list-style-type: none"> <li>• Video recordings of individuals walking through or entering areas adjacent to secure infrastructure (e.g., entrance to the demo and experiment suite).</li> </ul>	<ul style="list-style-type: none"> <li>• CCTV cameras located on company premises.</li> </ul>

Oxehealth has a legitimate interest in maintaining physical security, preventing unauthorised access to critical infrastructure, and protecting its property and systems.

## 3. How we keep your Personal Data Secure

The security of all data held and processed by Oxehealth is important to us. Oxehealth has implemented an ISO 27001 and ISO 27701 certified information security and privacy management system which is audited to ensure that we have the appropriate technical and organisational controls in place to protect your Personal Data.

Oxehealth maintains physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of Personal Data. Our security and privacy procedures mean that we may request proof of identity before we disclose Personal Data to you.

We have put in place procedures to deal with any suspected Personal Data breach and will

notify you and any applicable regulator of a breach where we are legally required to do so.

## 4. How long we keep your Personal Data for

Most supplier data is kept for the duration of the contract or agreement with the supplier. Some data is required to be kept for longer to comply with legitimate business purposes according to Oxehealth's retention policy or for legal obligations which Oxehealth is required to comply with. For example invoicing information is retained for a period of 7 years after the end of the customer contract to comply with HMRC requirements and information collected for compliance purposes may be retained for the lifetime of the medical device plus an additional 15 years to comply with medical device requirements.

## 5. Who your Personal Data is shared with

In addition to sharing your data with HMRC and other public authorities as required by law, your personal data will be routinely shared with the following third party contractors:

Third Party Service / Contractor	Purpose	Location
<a href="#">Atraxa Consulting Limited</a>	Provide accounting services on behalf of Oxehealth Limited (including the preparation and processing of VAT returns)	Brookes Mill, Armitage Bridge, Huddersfield, West Yorkshire, HD4 7NR
<a href="#">Bookwise AB</a>	Provide financial and administrative support to Oxehealth Limited in respect of our Swedish operations	PO Box 384, 101 27 Stockholm Sweden
<a href="#">SVB</a>	Banking portal through which supplier payments are paid	Alphabeta, 14-18 Finsbury Square, London EC2A 1BR
<a href="#">NatWest</a>	Banking portal through which supplier payments are paid	36 St Andrew Square, Edinburgh, United Kingdom, EH2 2YB

In addition Oxehealth uses the following cloud service providers for the processing activities outlined above or for general day to day running of the business, and your data may be stored on the servers owned by these providers. Where available links to their privacy notices are attached. Third party service providers may change and while Oxehealth endeavours to keep this list up to date as these changes happen, we request you do not rely on this but contact us using the details in section 8 (Contacting Us) for the most up to date list.

Software Service (click link for privacy notice)	Purpose	Storage Location	Third Country Data Transfer Mechanism
<a href="#">Google Workspace</a>	Storing supplier information as part of supplier assessment	Europe	Adequacy Decision (EU to UK)

			EU-US Data Privacy Framework with UK extension.
<a href="#">Sage Online50</a>	Storing supplier details to support processing invoices	United Kingdom	Sage's intra-group Personal Data Processing agreements, UK IDTA or Sage's SCCs with UK Addendum.
<a href="#">Microsoft Office 365</a>	Maintaining relationship and corresponding with suppliers	United Kingdom	Adequacy Decision (EU to UK)  EU-US Data Privacy Framework with UK extension.
<a href="#">Archon Systems Inc (Inflow)</a>	Managing inventory of equipment for installation at customer sites	Canada	EU-US Data Privacy Framework with UK extension.
<a href="#">Hik-Vision</a>	Provides a mobile application (Hik-Connect) for remote access to CCTV footage stored locally on Oxehealth servers for physical security and access monitoring.	Video footage is stored on Oxehealth-controlled servers in the UK. Streaming may be transiently routed via Hikvision-managed cloud infrastructure in Ireland (AWS). Hikvision is headquartered in China.	EU SCCs only. No UK Addendum or IDTA is in place. A Transfer Risk Assessment (TRA) has been completed, and the risk is being monitored and reviewed.

## 6. Location of Personal Data

We may sometimes transfer, store, or host Personal Data with third-party service providers located outside the UK and/or the European Economic Area (EEA), including in countries where data protection laws may offer a lower level of protection than in the UK.

Where such transfers occur, we ensure that they are carried out in accordance with this Privacy Notice and applicable data protection laws. We take steps to ensure that recipients provide adequate levels of protection and security for Personal Data.

The international transfer mechanisms we rely on include:

- The UK–EU adequacy decision (for transfers to EEA countries);
- The EU–US Data Privacy Framework with UK extension (for transfers to certified US organisations);
- Standard Contractual Clauses (SCCs) with the UK Addendum;
- Or, where available, Binding Corporate Rules (BCRs).

Where none of the above mechanisms apply, we will carry out a Transfer Risk Assessment (TRA) to identify appropriate supplementary measures and ensure an equivalent level of protection.

Where third parties process Personal Data on our behalf, we require them to implement appropriate safeguards to protect that information.

## 7. Your Personal Data Rights

You may have certain legal rights relating to your Personal Data, subject to local data protection laws. Depending on the applicable laws these rights may include the right to:

- Access the personal data we hold about you.
- Learn more about how we process your personal data..
- Correct any inaccurate or incomplete personal data we hold about you.
- Request the deletion or erasure of your personal data where applicable.
- Restrict or object to the processing of your personal data including for direct marketing purposes.
- Obtain a copy of your personal data in a portable format or request that we transfer it to another provider.
- Opt out of certain types of processing, including the sale of personal data (note: we do not sell personal data) or sharing of your personal data for targeted advertising, where applicable under local laws.
- Not be subject to decisions based solely on automated processing, including profiling, which produce a legal or similarly significant effect on you.

To exercise any of these rights, please contact us using the contact details below. We will respond to your request as required by applicable law, typically within one month. In some cases, we may need additional time due to the complexity or volume of requests, in which case we will notify you.

Where permitted by law, we may require proof of your identity before fulfilling your request. In some cases, we may decline a request if it is manifestly unfounded, excessive, or otherwise not required by applicable law, but we will provide an explanation in such instances.

### **Direct Marketing**

You have the right to object to the use of your personal information for direct marketing at any time. You do not need to provide a specific reason for such objection, and we will honour your request promptly.

### **Non Discrimination**

Oxehealth respects and upholds applicable data protection rights and ensures that no unfair treatment or discrimination occurs as a result of exercising those rights.

### **Automated Decision Making**

We do not currently engage in decision-making based solely on automated processing, including profiling, that produces legal or similarly significant effects.

## 8. Contacting Us

Oxehealth is registered with the Information Commissioner's Office (ICO) in the UK and has appointed a Data Protection Officer (DPO) to oversee compliance with all data protection laws in the jurisdictions in which we operate. You can find details of our registration and the data protection officer on the ICO's [register of fee payers](#).

To exercise your rights regarding your Personal Data, or if you have questions regarding this Privacy Statement or our privacy practices please email us at [privacy@oxehealth.com](mailto:privacy@oxehealth.com), call us at +44-1865-900599, or write to us at:

Oxehealth Data Protection Officer  
Bee House  
140 Eastern Avenue  
Milton Park  
Oxfordshire, OX14 4SB  
United Kingdom

When you contact us please indicate what country and state you reside in so we can address your inquiry appropriately.

## 9. In The Event You have a Complaint

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. If you are unhappy with the way in which your Personal Data has been processed please contact Oxehealth's Data Protection Officer using the contact details above.

If you remain dissatisfied then you have the right to apply directly to the relevant supervisory authority for a decision. You may contact them as follows:

### **United Kingdom**

Information Commissioner's Office  
Tel: 0303 123 1113  
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF  
Live chat: <https://ico.org.uk/global/contact-us/contact-us-public/public-advice/>  
Website: [www.ico.org.uk](http://www.ico.org.uk)

### **Sweden**

IMY - Swedish Authority for Privacy Protection  
Integritetsskydd Myndigheten, Box 8114, 104 20 Stockholm, Sweden  
Tel: +46 (0)8 657 61 00 (Monday to Friday 9am to 12pm)  
Email: [imy@imy.se](mailto:imy@imy.se)  
Website: [www.imy.se](http://www.imy.se)

## United States

If you are based in the United States, you may contact the following organisations:

Federal Trade Commission (FTC): File a complaint via <https://reportfraud.ftc.gov>

Your State's Attorney General: A directory of state Attorneys General is available at <https://www.naag.org>

California residents: For complaints under the California Consumer Privacy Act (CCPA), you may contact the California Privacy Protection Agency (CPPA) via their website at [www.ccpa.ca.gov](http://www.ccpa.ca.gov)

## 10. Review and Update of Privacy Notices

Oxehealth will review and update our Privacy Notices from time to time to reflect changes in our practices, technologies, legal requirements and other factors. If we do, we will update the 'effective date' at the top of this page. We encourage you to periodically review this Privacy Notice to stay informed about our collection, processing and sharing of your Personal Data.