Data Protection & Trust at Oura

ŌURA

ouraring.com

August 2026

Table of Contents


9:41
ŌURA
88
Readiness
84
Sleep
91
Activity
6
Cycle day
88
READINESS
Go get 'em
A great night's sleep can boost your readiness. If there are any challenging tasks on your to-do list, today could be the day to tackle them!
Learn more
Sleep
GOOD

Overview

Overview

Oura is committed to winning the trust of our Members and business partners. Security and privacy are non-negotiable and at the core of our mission to improve the way we live our lives.

This document, created for our partners, shares the key elements of Oura's business, security, and privacy functions so our business customers' and research partners' security and privacy teams feel confident that we take data protection seriously.

Our Information Security Management System (ISMS) is informed by industry standards and guidelines to design our organization. We aim to proactively mitigate harm and be resilient in light of globally emerging threats to data in our care. We understand the importance of data protection for our partners, business customers, and Members.

Products & Services

Why is Oura Valued by Our Members?

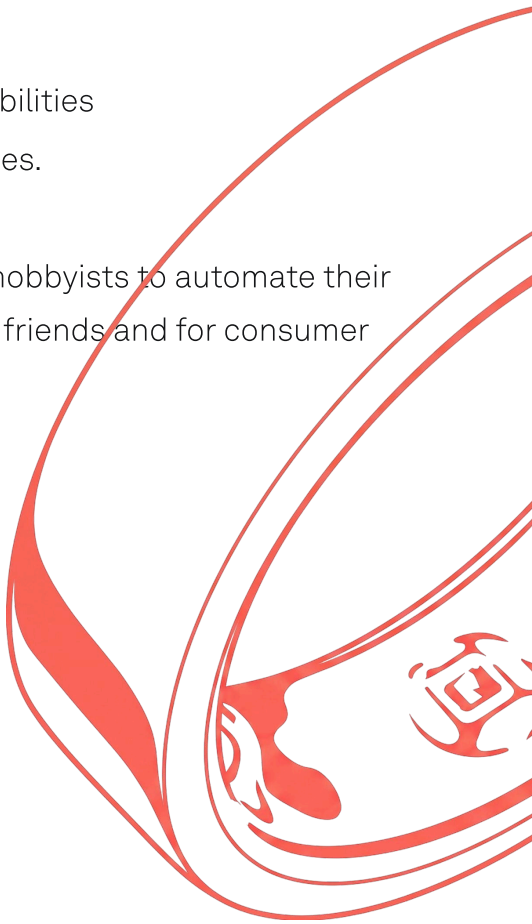
Oura Ring is a revolutionary smart ring that delivers personalized health data, insights, and daily guidance. With its advanced, research-grade sensors, Oura Ring packs state-of-the-art heart rate (HR), heart rate variability (HRV), average blood oxygen, average skin temperature, activity, and sleep monitoring technology into a convenient, non-invasive ring — prioritizing both accuracy and comfort without compromise.

Trusted by top-tier research institutions worldwide, Oura has developed and verified the functionality across a range of features including heart rate and heart rate variability, sleep staging, and skin temperature.

Member Products & Services

When Members get Oura Ring, either personally or from one of our partners, they can enter the Oura ecosystem, which includes the following connective points with which they can directly interact:

- **Oura Ring:** The smart ring that delivers personalized health data, insights, and daily guidance.
- **Oura Paid Membership:** A subscription service which provides detailed insights behind their Sleep, Readiness, and Activity scores. More information available here.
- **Oura App:** Receives the data from the ring and makes users' Sleep, Readiness, and Activity scores, as well as Members' insights, available to them in a beautifully designed interface.
  - Android: https://play.google.com/store/apps/details?id=com.ouraring.oura
  - iOS: https://apps.apple.com/us/app/oura/id1043837948
- **Integrations:** Members can optionally access additional capabilities through integration to a growing set of partner enabled services. Read more about our partnerships here.
- **Public Oura API:** This API is available for both small scale for hobbyists to automate their own data and build apps for themselves and their consenting friends and for consumer app integrations.
  - Oura API: https://cloud.ouraring.com/docs/



Business Partners: Products & Services

Business Partners can interact with Oura and Member data in a few ways:

- Provision Oura Ring, subscriptions, and complementary services to your associated populations for a variety of purposes, including:
  - Gifting programs
  - Occupational health management and guidance
  - Connected health care delivery programs
  - Research studies
- Sale and provision of complementary devices and services to Oura Members at large

To support these Business Partner use cases, Oura provides a set of Products & Services that include:

- Oura Enterprise Platform: Oura Enterprise Platform (OEP) is a web-based platform that allows administrators to integrate, analyze, view, and access health data to drive informed decisions:
  - Data Access & Management: Collect and manage data from Members to deliver insights with organizational context.
  - Visualization & Reporting: Monitor adoption and manage population health in one easy-to-use dashboard.
  - Data analytics: Extract population insights and track trends of associated members.
  - Consent and data sharing management: Control the level of data sharing with members and manage consent workflows.
- Oura Enterprise API: Access data from consented members via a powerful API that can be used to create valuable experiences in your own application.

Oura is committed to member privacy, prioritizing data protection and that member data sharing to organizations is on an opt-in basis and consent to share may be revoked by a member at any time.

Business Partners: Products & Services (continued)

Commercial Ordering Pathways

Business Partners can order or enable fulfillment of Oura Rings via several pathways each suited for specific use cases:

- Bulk Order Portal: Customers can work with an internal Oura sales representative to manage bulk orders of rings to be shipped to a single address, or multiple addresses. The use of Bulk Order Portal is appropriate when a single large order is to be placed and, at a minimum, names, email addresses, and shipping countries of Oura Ring Recipients are known. Orders can be fully specified, including full address, phone number, size and finish, or may be partially specified. For partially specified orders that include address, a sizing kit will be mailed to the provided shipping address, and the recipient will complete sizing through the Recipient Redemption Site accessed through a link sent to the provided email address.
- Bulk Order Portal Self Service: Customers can gain access to their own instance of the Bulk Order Portal to manage bulk orders of rings to be shipped to a single address, or multiple addresses. The use of Bulk Order Portal Self Service is appropriate when a Customer will be placing many orders over a period of time, does not want to complete an API integration and, at a minimum, names, email addresses, and shipping countries of Oura Ring Recipients are known. Orders can be fully specified, including full address, phone number, size and finish, or may be partially specified. For partially specified orders that include address, a sizing kit will be mailed to the provided shipping address, and the recipient will complete sizing through the Recipient Redemption Site accessed through a link sent to the provided email address.

Business Partners: Products & Services (continued)

- Commercial API: Customers can integrate with Oura's Commercial API to programmatically submit individual orders to Oura for fulfillment. Use of the Commercial API is appropriate when a customer has their own enrollment or checkout flow and where there is an expectation that orders will come in individually over a period of time. The Commercial API requires at a minimum name, email address, and shipping country to be supplied. When the Oura Commercial API is invoked with a shipping address, a sizing kit is shipped to the recipient who will complete ring sizing through the Recipient Redemption Site Oura accessed through a link sent to the provided email address or a QR code on the sizing kit. When the Oura Commercial API is invoked with only a shipping country, the recipient will complete their shipping information, can decide if they need a sizing kit to be shipped to them and then proceed to sizing through the Recipient Redemption Site via the link sent to the provided email address or the QR code on the back of the sizing kit.
- Recipient Redemption Site: The Recipient Redemption Site (RRS) allows ring recipients to provide needed information to Oura to complete their sizing kit and ring orders. When an order is placed on a ring recipient's behalf, either a sizing kit is immediately dispatched to the address provided or an email is sent to the user to prompt them to supply their shipping address. In both cases, users supply their requested size and finish to complete their transaction.
- Eligibility API: The Eligibility API allows for HIPAA covered entities and upstream business associates to securely send and update member eligibility in real time, so that eligible members can enroll in an Oura program and claim their benefit via the Enrollment Flow on the Recipient Redemption Site.
- Enrollment Flow via Recipient Redemption Site: In tandem with the Eligibility API, The Recipient Redemption Site (RRS) allows eligible users to opt into an Oura program, whether they are receiving a ring, ring plus membership, or otherwise. When a user is input into the eligibility API, the customer directs the user to the redemption site, to prompt them to opt into the benefit and supply their shipping address. The user will also supply their requested size and finish to complete their transaction.

Data Flow

Oura Ring, App, Consumer & Enterprise Clouds, & SaaS Access

Member-side Data Flow

During initial onboarding, Members connect their Oura Ring and account via the Oura App to the cloud. Members use their email to create an account and input some basic information like sex assigned at birth, height, and weight, which our Products use to generate personalized health and wellness insights. This data is transmitted from the Oura App to the Oura Cloud encrypted in transit (using TLS 1.2+).

> Oura encrypts data in transit from Oura App to Oura Cloud using TLS 1.2 or greater.

Additionally, Oura Ring connects to the Oura App via Bluetooth using Secure BLE.

Oura runs its primary infrastructure on a leading cloud service provider and our databases utilize AES 256 encryption at rest by default.

In addition to the Oura App, Oura Members can access dashboards, exports, and more directly on Oura on the Web (via cloud.ouraring.com) where their access requires authentication and is encrypted in transit from site to user using TLS 1.2 or greater.

> All four of our primary web properties encrypt traffic in transit utilizing TLS 1.2 or greater:
>
> - ouraring.com **E-commerce, company information, & blog**
> - cloud.ouraring.com **Oura on the Web**
> - platform.ouraring.com **Oura Enterprise Platform**
> - orders.ouraring.com **Bulk Order Portal**

Business-side Data Flow

Business users can submit or access member data on our two web properties:

- orders.ouraring.com **Oura Bulk Order Portal**
- platform.ouraring.com **Oura Enterprise Platform**

Within Bulk Order Portal, business admins can create orders on behalf of members and have rings shipped directly to them. In some cases, business admins must provide all necessary information (name, email, shipping address, size & finish). In others, business admins may provide only name, email and shipping country. In the case that there is missing information, the user fills in the missing information via Recipient Redemption Site and it is written back into Bulk Order Portal. At this point, the business admin is able to see any information that the user has added.

With Member consent, businesses can view data on the Oura Enterprise Platform.

- Oura does not need access to our enterprise partners' internal systems.
- Enterprise partners do not need to download any applications, grant VPN, API, or any other internal system access.
- Enterprise partners may receive access to Oura's two SaaS portals via any web [illegible] workstations.

Consumer & Enterprise Data Flow

Oura Members benefit from an integrated ecosystem that includes Oura-provided capabilities as well as Partner and Business Customer provided capabilities. To efficiently support security, privacy, and other compliance needs, clear boundaries and controls are implemented to govern data flow among participating systems. Key points of separation and control include:

- Any Business Customer & Partner access to member data is managed through the Oura Enterprise Platform
  - Each Business Customer & Partner is provisioned an individual account. Deployment options can support geo-specific residency and secure enclave deployment needs that may vary among customers & partners.
  - Administrative users and API access are governed through RBAC and all interactions are logged.
  - Sharing of Member data requires explicit consent by Members, and consent is managed by the platform.
- Members opt into any relationships with Partner provided services and associations with Business Customer & Partner accounts

To support our Enterprise Customers & Partners, including health plans, research institutions, and government agencies, Oura maintains a segmented architecture that separates Enterprise Partner Data from Member Data. This structure ensures we meet distinct compliance and data residency requirements without compromising our consumer experience.

Enterprise Partner Data refers to information provided by or collected on behalf of a Company (e.g., eligibility files, partner-specific survey responses, pooled Member data), while Member Data includes information created or shared by individuals through use of the Oura Ring and App. We retain a strict distinction between these domains to uphold member data ownership and minimize scope creep under compliance frameworks like HIPAA.

Consumer & Enterprise Data Flow continued

The Oura Enterprise Platform enforces logical tenant isolation, role-based access controls, and consent-gated data sharing. Enterprise Customers & Partners can only access data explicitly shared by members, and members may revoke that consent at any time. Oura does not require access to our partners' internal systems, and all partner interactions occur within designated, access-controlled SaaS environments.

Key services in the Enterprise Partner Data Environment include:

- Eligibility APIs: Secure ingestion of partner-provided data
- Oura Enterprise Platform: Visualization and management for partner programs
- Enterprise Partner API: Programmatic access to consented Member Data

This targeted segmentation of systems and responsibilities allows Oura to support complex enterprise needs while preserving our unified commitment to privacy, member ownership, and operational excellence.

Enterprise Deployments

For Enterprise clients, including healthcare and research partners, Oura can deploy tailored infrastructure with enhanced compliance controls:

- Tenant Isolation: Available multi-tenant controls enforce strict boundaries between client data domains.
- Data Residency Options: U.S. based Enterprise Partner Data Environment is available for HIPAA-aligned use cases. Other countries available, by request

Our Team & Security Directive

Our Data Protection Team

Oura's Security team is led by our Chief Information Security Officer. Oura has appointed a Data Protection Officer, who can be reached at dataprotection@ouraring.com.

Oura has functions supported by internal team members including Governance, Risk, and Compliance, Security Engineering, Privacy, and Legal.

Our Security Engineering team provides EU and US escalations and incident response backed by our outsourced SOC which monitors and responds to events from our SIEM.

Our Mission

Our Security Team's goal is simple:

> Enable Oura to operate and grow by building the best security program in health tech.

The following elements support this objective:

Security and Internal Stakeholder Alignment

Security's role and responsibility in an organization is to be a business partner to the internal teams. Oura's Security Team prioritizes collaborative and proactive risk management. The Security Team works with internal teams to judiciously mitigate risk while building relationships within the organization. This results in security being brought in at key moments and proactively consulted, leading to a more secure environment.

Systemic Solutions

Aiming for systemic solutions to individual problems allows for greater efficacy and speed. For example, instead of overburdening engineering with countless tickets for individual vulnerability tickets, Oura tackles root causes of issues, creating solutions that wipe out a breadth of vulnerability tickets in one fell swoop.

Relentless Iterations and Optimizations

Oura is constantly adding new security programs and procedures as well as going back and adding to existing ones, even recently created ones. Audits, partnerships, and internal collaboration frequently leads to opportunities where improvement is an option and optimizations can be made to improve the efficacy of a program.

Security Methodology

Introduction to our Methods

Oura builds enterprise-grade security into every aspect of our business, so Partners and Members can sleep well at night. We organize security controls across the various domains listed below, in an effort to mitigate against cyber attacks:

Education, Training, and Awareness

Data protection starts with people. Verizon's 2026 Data Breach Investigations Report (DBIR) found that the non-intentional human element was involved in 62% of breaches, while Social Engineering remained the third most common breach pattern, representing 16% of breaches [1].

We regularly engage with teams in various forms to support data protection education, training, and awareness initiatives. From presenting at all-hands meetings to sending relevant security notifications via our lovable slackbot, Ourry (pictured right), we constantly seek to humanize and elevate the concepts of data protection awareness in the hearts and minds of our colleagues. With much of our personnel working remotely, it's imperative for us to emphasize the key elements of our acceptable use policy and to support and enable them with information on how to work safely out of the office.

As a part of our security program, we conduct initial security awareness training for new hires and continuous training for existing personnel annually. These annual trainings are not your typical check-the-box training. We design our training material to be engaging, specific, and relevant to our personnel. In addition to this, we conduct regular application security awareness training for our engineers including OWASP Top 10 topic coverage. We proactively assess and address areas of impact and progressively mature our overall architecture to improve security and stability.

Education, Training, and Awareness (continued)

Oura maintains a public Vulnerability Disclosure Program to facilitate responsible reporting of security vulnerabilities by the global security research community. Oura also maintains a private bug bounty program for more in-depth security assessment by well vetted security researchers.

Lastly, we have a continuous, interactive phishing training that regularly tests Oura employees with clever phishing attempts that dynamically imitate co-workers and produce enticing calls to to action. This helps keep personnel on their toes and trains them how to spot the subtleties of clever spear-phishing attempts.

Device Management and Protection

The security of managed workstations (laptops and desktops) and managed mobile devices are guided by our Acceptable Use Policy and executed by Oura's EU- & US-based in-house IT team. Increasing the homogeneity of systems helps to simplify hardening, device management, patching, and vulnerability management. Beyond this, below are some of the security methods we utilize in this area:

Managed Workstations

- **Physical access controls:** Enforced inactivity screen lock with re-authentication required and enabling biometric authentication on managed devices for passwordless login.
- **Required authentication:** Biometric authentication or strong passwords subject to our password policy are required to unlock devices, including MFA, where applicable.
- **Encryption at rest:** Enforced on our managed workstations.
- **Admin account restriction:** Standard user accounts are enforced; requests for temporary administrative privileges must be submitted to IT with a defined business justification.
- **ZTNA for sensitive use:** Authenticated IPSec available for personnel handling more sensitive data.
- **Endpoint protection & Response:** EDR to prevent, detect, and respond to threats.
- **Lifecycle Management:** Secure erasure tooling and locked devices in IT storage.

Managed Mobile Devices

- **Screen lockout:** Enforced inactivity screen lock with re-authentication required to login.
- **Password Policy Enforcement:** Phones require pin or biometric authentication with minimum requirements.
- **Mobile Device Management:** This provides additional capabilities such as the ability to logically separate work and personal data, remotely wipe work data, improved inventory management, and enforced minimum device protection standards.

User and Access Lifecycle Management

- Provisioning and deprovisioning personnel is a cross-functional process managed by IT and supported by a custom system for logging tickets, monitoring, and approving access.
- Personnel are granted single sign-on (SSO) accounts during onboarding. Account provisioning includes identity verification prior to credential issuance, and initial credentials are single-use and must be replaced by the employee at first authentication.
- Oura uses phishing-resistant multi-factor authentication (MFA) as the standard for workforce authentication on SSO accounts. Primary authentication controls include hardware-backed authenticators, such as FIDO2/WebAuthn security keys where applicable, and managed-device verification through a managed identity provider and device trust policies. Personnel are given enterprise-managed password manager accounts for password management usage outside of SSO.
- Our password management policy requires strong, unique passwords, in combination with MFA. Additionally, passkeys are widely enabled for passwordless authentication into Oura SSO accounts to further reduce the risk of password-based attacks. Security training on how to create strong passwords helps support this effort. This is an improvement over constantly expiring and changing passwords, in alignment with NIST's guidance in SP800-63B Rev.3 [2].

Cloud Security

Oura's primary infrastructure lives on a leading cloud service provider which holds high standards across virtually every compliance framework on the market. We layer our own defense-in-depth program on top of our cloud service provider foundation, combining proactive engineering practices, continuous detection and response, and disciplined vendor selection to identify, assess, and mitigate risk throughout the full development lifecycle.

Cloud Security (continued)

Shifting Left: Proactive Measures

Before code or infrastructure ever reaches production, we work to surface and eliminate risk as early as possible:

- Security reviews and threat modeling for new services, architectures, and significant changes, so design decisions account for risk before they become commitments.
- Infrastructure as Code (IaC) scanning to catch misconfigurations at the source and block insecure infrastructure from being deployed.
- Vulnerability scanning in our build process, including container and dependency scanning, so vulnerable artifacts are caught and remediated before they ship.
- Private Artifact management repositories to securely host internal software packages and enforce security policies to protect against software supply chain attacks.
- Cloud Infrastructure Entitlements Management (CIEM) to enforce least privilege as environments and access patterns evolve.

Continuous Detection, Response, and Assurance

Once workloads are running, we maintain layered tooling and processes to continually identify, assess, and mitigate risk:

- Cloud Security Platform (CSP) providing centralized visibility, context, and risk prioritization across our cloud environments, including:
  - Cloud Security Posture Management (CSPM): real-time detection and alerting on misconfigurations.
  - Container & Orchestration security: identifying and reducing risk across our containerized workloads.
  - Cloud Workload Protection Platform (CWPP): runtime protection, detection, and response for workloads.
  - Cloud Detection & Response (CDR): investigating and responding to threats with full cloud context.

- AI Security Posture Management (AI-SPM): AI-enabled prioritization of risks surfaced across our CSP data.
- Attack Surface Mapping: Dynamic testing and assessment of publicly exposed assets to catalog and identify vulnerabilities, bugs, and risks.
- Threat detection and alerting tuned and integrated with our incident response process.
- Automated vulnerability scanning across infrastructure, workloads, and code through multiple complementary tools, ensuring no single layer is the only line of defense.

Vulnerability and Patch Management

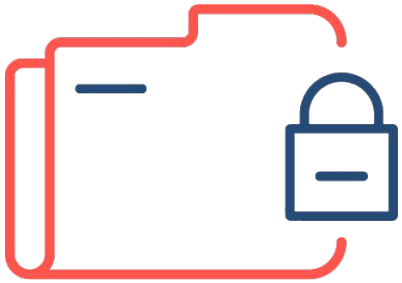
Oura operates a multi-faceted, tailored, and continuously iterated on vulnerability and patch management program which includes an annual review and recalibration of our program as needed.

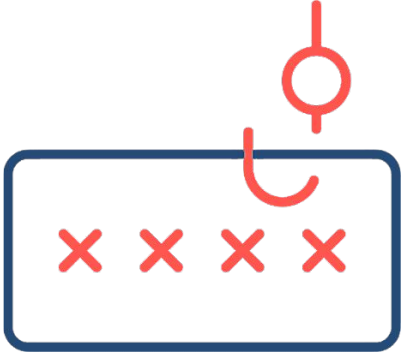
For years now, Oura has conducted penetration tests regularly to look for holes in the security posture of our app, cloud, web portals, and rings. We continue to employ third parties to test our systems regularly to help identify and mitigate risks.

Aligned with our mission of simplicity, our vulnerability prioritization levels are translated into language our teams can easily understand. This system of prioritization helps get security vulnerabilities attended to when they need attending.

Cloud Infrastructure

We conduct and attend to quarterly vulnerability scanning as part of our PCI compliance process. In addition, we conduct various vulnerability scans, which give us a better look at emerging threats and risks.





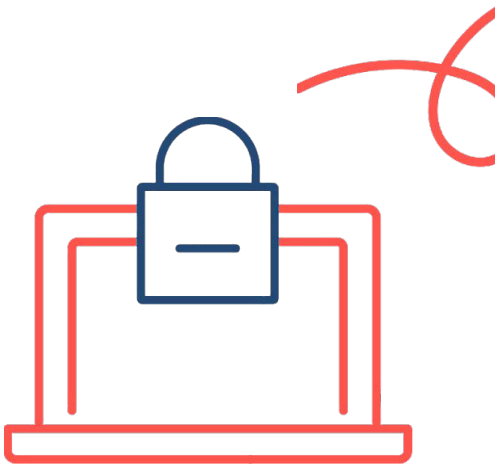
Product Security and Privacy

A myriad of product security initiatives support our Secure Software Development Lifecycle (SSDLC). This includes source control with dependency scanning, code scanning, and PR approval requirements. We leverage TLS 1.2+ for encryption in transit when communicating on the internet and AES 256 for encryption at rest on our production databases.

Cooperation is a cornerstone of our company with data protection, product, and engineering teams working together to shift left on integrating data protection into the design process. Oura conducts working sessions—leveraging STRIDE, Privacy-by-Design, or a custom format—to guide our design process towards mitigating against security and privacy risks throughout the entire product life cycle.

Logging, Monitoring, and Alerting

We take a proactive, evolving approach to ensure this area of security remains resilient. Our aim is to produce less noise and more meaningful alerts; the key to ensuring Oura maintains a safe and secure environment. We leverage a tiered response with our managed outsourced SOC monitoring our security information and event management (SIEM) and our EU & US located security engineering team as the escalation point to support investigation of suspicious activity. Additionally, as part of our data loss prevention strategy, systems handling sensitive data are subject to enhanced monitoring, with anomalous activity routed to our detection and response process. Logging, monitoring, and alerting is a continuous improvement process with the aim of producing less noise and more meaningful alerting. We regularly review our program to find opportunities to improve it.

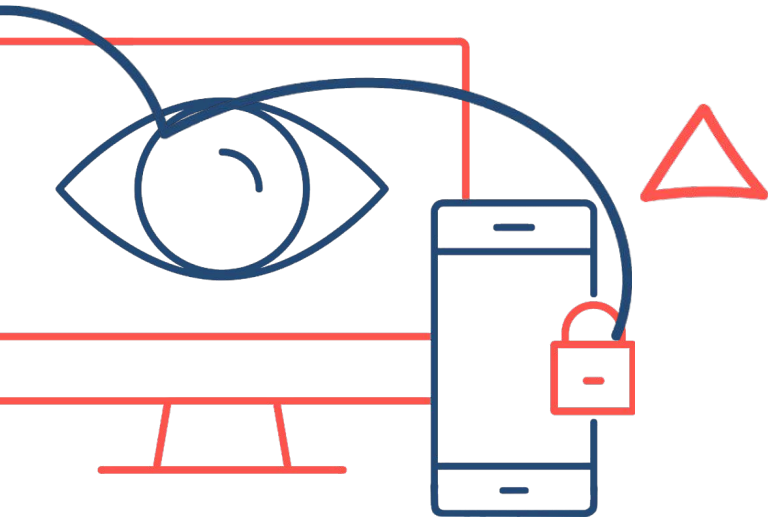


Incident Management & Business Continuity

Process is the foundation of a good incident management or business continuity program. We respond to data protection incidents with playbooks and procedures built for common events and templates for ensuring the right people are involved in every step of the way.

Legal & Privacy's involvement is required for any event involving the potential for personal data to be impacted. A breach notification plan is in place and we have escalation procedures for data protection events that require more resources.

Key personnel involved in the incident response and business continuity process have access to Oura's asset registry with the relevant business and technical owners for systems to involve when necessary. Criticality, type of information on systems, and other noteworthy data points for systems are noted and used when making decisions as a unit on how to respond to data protection events.



Data Protection Regulations

Data Protection Regulations

Overview

Oura is an international company with servers around the world. As a result, we are subject to stringent data protection regulations world-wide. Although data protection laws vary among countries, regardless of where personal information is processed, we apply the protections described in our privacy policies. We also strive to treat data subjects with the utmost respect for their privacy, without regard for the individual's geo-location.

Oura maintains updated privacy policies on our website: https://ouraring.com/privacy-policy.

We ensure appropriate data protection agreements are in place with our vendors, business, and research partners.

To contact our Data Protection Officer or submit a privacy inquiry, email dataprotection@ouraring.com.

Individuals can exercise their privacy rights as described in our privacy policies. Where feasible, we strive to enable self-service data subject requests such as, enabling Members to trigger account deletion from the Oura App.

GDPR & Legal Frameworks for International Transfers

Oura processes personal data of data subjects in the European Economic Area (EEA) and adheres to the EU and UK General Data Protection Regulation.

Because Oura is a global company with servers around the world, personal information may at times be processed on servers located outside of the country in which the data subject is located.

GDPR & Legal Frameworks for International Transfers (continued)

Oura participates in the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework (collectively, the "Data Privacy Frameworks") as set forth by the US Department of Commerce regarding the processing of personal information from the European Economic Area, the United Kingdom and Gibraltar, and Switzerland. Oura has further certified that we adhere to the principles of the Data Privacy Frameworks. Visit https://www.dataprivacyframework.gov/ to learn more about the GDPR Data Privacy Frameworks. If there is any conflict between the terms in our privacy policies and the Data Privacy Frameworks principles, the principles govern.

If Oura transfers personal information received under the Data Privacy Frameworks to a third party, the third party's processing of the personal information must also be in compliance with our Data Privacy Frameworks obligations, and we will remain liable under the Data Privacy Frameworks for any failure to do so by the third party, unless we prove we are not responsible for the event giving rise to the damage.

US State and Federal Privacy Laws

Oura processes personal information of US data subjects, and adheres to applicable US state and federal privacy laws, such as the California Consumer Privacy Act (CCPA) as modified by the California Privacy Rights Act, the Health Insurance Portability and Accountability Act (HIPAA), and the ever-growing list of US state privacy laws.

HIPAA

Given the sensitive nature of Protected Health Information (PHI), we have implemented a comprehensive compliance program for the Health Insurance Portability and Accountability Act (HIPAA). We have an enclave available for processing HIPAA Eligibility data from our partners signing a Business Associate Agreement (BAA) with us. Our HIPAA audits are conducted by a third-party auditor.

Research Partners

A special note for research partners:

Research partners may receive data that has been processed to protect data subject privacy ("Research Data"). Oura requires research partners to adhere to contracted processing purposes when they process Research Data. For more information, please discuss with your Oura point of contact.

Overview of Compliance at Oura

Our compliance program consists of a variety of security and privacy programs aimed at self-auditing and improving our data protection posture over time.

Third-Party Assurances

We undergo an annual SOC 2 examination and maintain HITRUST certification, assessed on its certification cycle.

Risk Management

We adopt a proactive and structured approach to risk management:

Product Risk Assessments (PRA)

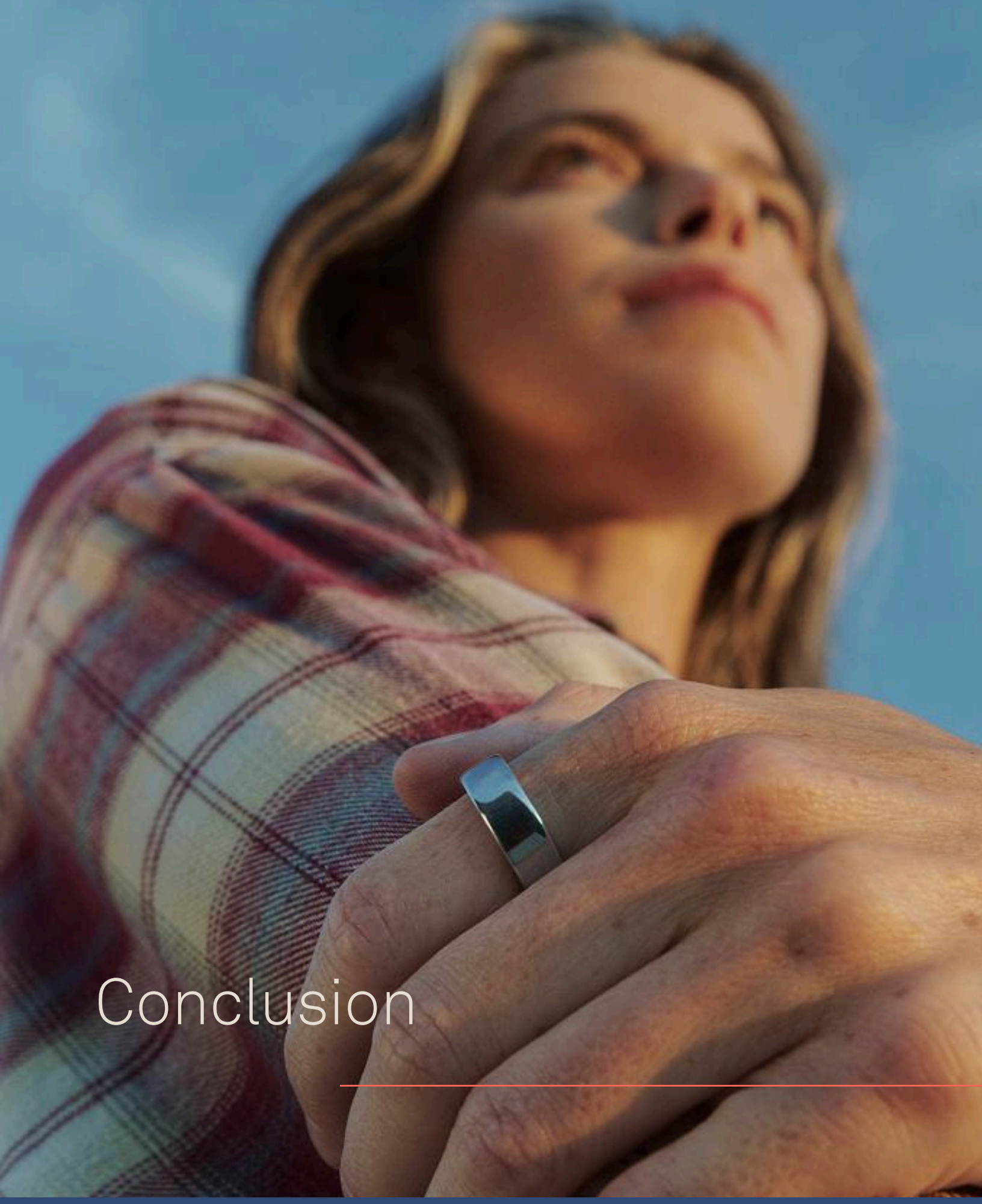
New features or material updates to products are candidates for product risk assessments and/or threat modeling exercises.

Third-party Risk Management (TPRM)

We ensure that our third-party vendors undergo a rigorous risk review before onboarding. This program includes a policy, procedure, and a structured template used for addressing the scope, threat, likelihood, risk, complementary user entity-controls (CUECs), and presenting an evaluation of the overall data protection posture as it relates to our scope of relationship with the third-party. We use a tool for managing this which requires approval from security and legal before allowing business owners to engage with and sign a contract to do business with third-parties.

Conclusion

The security and privacy of our users are paramount. Our comprehensive approach to security, privacy, compliance, and risk management demonstrates our commitment to protect our Members' data effectively. We continually strive to enhance our data protection posture and stay ahead of emerging threats, providing a secure and trustworthy environment for our partners and our Members. For any questions that we didn't answer, please email us at security@ouraring.com.



Conclusion

Citations & Definitions

Definitions

Business Customers or Partners ("Customers"): These are our business clients that are giving rings to their customers.

Members: Anyone with an active Oura account, regardless of their subscription status.

Citations

[1] Verizon. (2026). 2026 Data Breach Investigations Report. Verizon Business. Retrieved from https://www.verizon.com/business/resources/reports/dbir/. Accessed August 1, 2026.

[2] National Institute of Standards and Technology. (2017). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B). https://doi.org/10.6028/NIST.SP.800-63b. Accessed August 1, 2026.

Thank you

ŌURA

ouraring.com

August 2026