Our Approach to Data Privacy

Whitepaper for informational purposes (2023)

At Varonis, we apply the highest security standards to the way we use your personal information in our day-to-day operations. We also believe in full transparency, and so in this whitepaper, we have outlined key aspects of our standards, practices, and safeguards for your information and compliance assessment purposes. For any further questions, please do not hesitate to contact your Varonis representative or use the contact details provided below.

What Varonis Does (through the privacy lens)

Our SaaS Platforms include the following capabilities (note: this is not a comprehensive list of our products' capabilities and advantages, but a highlight of the main items that are related to the processing of private data):

- **Data activity monitoring** monitors who and what is accessing data and what they do with that data (create/open/modify/delete, etc.) and monitors authentication and perimeter telemetry in the data access chain.
- **Data discovery and classification** automatically and continuously scans the contents of files, folders, and other objects to determine the sensitivity of the document.
- **Data access intelligence** combines data sensitivity, permissions, and activity to show customers who has access to critical data (i.e., their data blast radius), how they derive access, and whether access is necessary.
- **Posture management** interrogates configurations and settings to assess, report on, and optimize configurations.
- **User and entity behavior analytics** profiles users, applications, and devices and their associated behaviors with respect to the monitored systems and data and detects and alerts on meaningful deviations that indicate compromise.

Nature and Scope of Personal Information Processed by Varonis SaaS

Varonis technology crawls data sources for the purpose of threat detection and response, data protection, and compliance and remediation.

Varonis differentiates between data and metadata:

- Customer data includes file and email content.
- Customer metadata includes user IDs and names, group names, folder and file names, email subjects, domains, and IP addresses.

Varonis also sends technical logs and telemetries from the Collector to Varonis SaaS. However, those do not contain any personal data.

Customer data is retrieved and processed by the Collector server(s) that are installed inside the customer premises; Varonis personnel or subcontractors do not have access to it. Administrative functions that affect change in the customer environment (such as removing monitored servers/systems) are also run from servers inside the customer premises (e.g., the Collector) without access by Varonis or its subcontractors.

Varonis SaaS does not persistently store customer data in the cloud. Only metadata that is included in its monitored platforms logs and events are stored, which is the essence of Varonis SaaS.

Please note that there are two exceptions to the above:

- DatAdvantage Cloud Product (DAC)
  DatAdvantage Cloud works directly with cloud data sources, such as Salesforce, Google Suite, Box, etc. For these data sources, Varonis does not require installing a Collector on the customer's premises, and the full data is retrieved by DatAdvantage Cloud from the data sources for classification. The data is not stored in the cloud, and after data is classified (which is a matter of seconds per file), the data is discarded, and only metadata and classification results are stored in the cloud to enable their analysis by the customers (similar to the of Varonis SaaS).
- File Analysis
  The File Analysis functionality, which is part of Varonis SaaS (except for DAC), is disabled by default. If a customer decides to enable the File Analysis functionality, the customer can grant the optional "File Analysis" role, which authorizes the customer's chosen user to view files that contain hits from File Analysis. Such files are transiting for a short period of time via Varonis SaaS to present the file to the chosen user. After passing through, the file is immediately discarded from Varonis SaaS.

  Additionally, the customer may choose that the user who is granted the File Analysis role must enter their organizational credentials, which are used to access the file on the data source and therefore are subject to access permissions defined by the customer. This means that if a user does not have permission to access a certain file through the customer's file system, that user won't be able to access that file using their File Analysis role in Varonis SaaS.

Data Locality

Varonis SaaS can be set to operate from any of the below geographies at the customer's choice upon onboarding (Varonis SaaS on Azure servers; DatAdvantage Cloud on AWS servers):

1. USA
2. Europe
3. Canada*
4. Australia*

**Not yet supported for DAC*

Varonis consistently develops and adds server locations to accommodate various customers' needs. Servers adhere to the local standards and requirements set by their region (e.g., GDPR in Europe).

Varonis uses sub-processors, which are third-party SaaS platforms, to provide certain service functions for its customers. The full list of Varonis sub-processors and their locations of processing can be found in our DPA for SaaS Customers. Note that the location of the processing by sub-processors with access to customer metadata are defined by the initial customer's choice of geography. This means that we can store the metadata in one territory (such as USA or Europe).

Data transfer outside of Europe — despite the option to keep the metadata on Varonis SaaS within Europe, as detailed above, Varonis acknowledges that some customers may need to store their data regarding

European individuals on Varonis SaaS located outside of Europe. Therefore, we have implemented safeguards and measures to secure the metadata of European individuals when that metadata is exported outside of Europe. In this framework, Varonis incorporated the Standard Contractual Clauses (SCC) in its DPA with its customers, and also conducted a Transfer Risk Assessment (TIA) and executed SCCs with all Varonis sub-processors. For further information, please refer to the section Service Providers Compliance below.

Official Roles in Varonis related to Privacy and Data Security

Varonis highly values the privacy and security of the data it processes and, accordingly, incorporates the "Privacy by Default" principle in its processes and "Privacy by Design" in its products. Therefore, Varonis designated several senior positions and teams across the organization to ensure all aspects of data safekeeping are attended to properly:

Data Protection Officer (DPO) — Our DPO has a vital role in supervising and ensuring Varonis complies with all necessary security and privacy legislation, evaluating and reviewing processing activities, and drafting and overseeing compliance with our procedures and internal policies.

The DPO developed a comprehensive privacy compliance practice at Varonis based on in-depth knowledge and understanding of Varonis technology. The DPO collaborated with multiple stakeholders in all departments across the company, ensuring Varonis' various products and processes are compliant with the rapidly evolving legal privacy landscapes across the globe.

Our DPO has the required expertise in data protection laws and practices, an in-depth understanding of the GDPR, CCPA, and other applicable privacy laws, an understanding of our processing operations, and the integrity and independence to be an objective supervisor necessary for such a role.

Chief Information Security Officer (CISO) — Our teams follow strict security policies and procedures designed by our CISO and his highly qualified team of experts. The team's purpose is to protect personal information from disclosure, unauthorized access, and leakage by setting up the proper classifications, controls, and measurements.

To learn more about our CISO operation and Varonis Compliance Certifications, please visit our Trust Center.

Chief Architect and VP of Cybersecurity Engineering — Varonis designated two senior positions in the R&D organization, each to lead a team of experts and oversee the integrity of Varonis software.

> *Chief Architect* leads the technological architecture of our products and reviews designs of all architecture changes. He maintains a data catalog and ensures that data residence and data governance principles are taken into consideration during the design process.
>
> *VP of Cybersecurity Engineering* verifies, from the security perspective, that private data is guarded according to industry standards and best practices, including conducting active assessments to ensure adherence to security standards and policies.

Main Privacy Legal Frameworks

Because we operate globally, we invest significant effort to be aligned and compliant with various applicable privacy laws and requirements. The primary regulations that guide our alignment and compliance decisions are:

Europe — The **European GDPR** and legislation implementing the **GDPR within the U.K.** presents a comprehensive legal framework for protecting natural persons in matters concerning the processing of their personal information and its free movement. Over the years, Varonis has made extensive adjustments to its internal practices and legal documents, including signing DPAs with all its sub-processors (for further information, please refer to the Service Providers Compliance section below) to comply with this legal framework.

United States — While the U.S. has not enacted a general federal privacy legislation, specific states have enacted their own comprehensive privacy laws. **California's** privacy law (California Consumer Privacy Act and the California Privacy Rights and Enforcement Act of 2020, **CCPA** and **CPRA**) is notable for being the first legislation in the United States. Another example is **Virginia's** privacy law (Virginia Consumer Data Protection Act, **VCDPA**) which came into effect in 2023.

Privacy laws in additional states have also been enacted (Connecticut, Utah, and Colorado), with others expected to become effective in the coming years (such as Texas, Montana, Iowa, Tennessee, Indiana, etc). We actively monitor legal developments and analyze whether additional steps are required to comply with new legislation.

With respect to **healthcare information**, the Health Insurance Portability and Accountability Act of 1996 **(HIPAA)** is the U.S. federal law enacted to protect the privacy and security of individuals' medical records and other individually identifiable health information. Although the scope and nature of the personal health information (PHI) that may be processed by Varonis is limited in nature and scope (as detailed above), Varonis practices are HIPAA-compliant, and Varonis has executed Business Associate Agreements (BAAs) with its relevant sub-processors.

Additional Regions — We monitor legislation in all relevant jurisdictions (such as **Singapore's** Personal Data Protection Act 2012, **Australia's** Privacy Act 1988 and the Australian Privacy Principles, etc.) and make sure our processes and documents are aligned with applicable laws. Varonis adjusts its DPA for its SaaS customers to applicable legislation.

Respecting Personal Information

Varonis is committed to the privacy and protection of the personal information we process, and that commitment manifests itself in our day-to-day activities. The below describes the key aspects of our security and privacy controls and measures.

The personal information that is processed by Varonis is treated with care for the users' (data subject) rights. We have implemented the necessary mechanisms to enable users to exercise such rights. Our teams are kept up to date with new privacy legislation and our internal procedures are updated to satisfy new

requirements. Our internal accountability documents and policies are continuously reviewed and updated to ensure our teams follow and operate in accordance with a cohesive and detailed policy.

Purpose Limitation and Data Minimization

We process information only at the scope and duration that is necessary to provide our services. The information we process is strictly necessary to provide our services. As detailed above, some information is processed temporarily.

Furthermore, we have built into our systems various privacy features, such as the ability to limit some of the data processing (such as in the Management Console).

Retaining Personal Information

All information we retain is for the purposes of providing our services or to comply with legal obligations, resolve disputes, or as otherwise described in detail in our publicly available privacy policies. We delete personal information periodically (in accordance with the retention policy indicated in the Software Privacy Policy), unless we have a valid legal need to retain such data.

Data Protection Impact Assessment (DPIA)

Whenever a new technology, system, policy, or significant change is sought to be put in place, a privacy and security assessment is performed (aka Data Protection Impact Assessment). Such assessment allows us to identify and mitigate any potential privacy-related risks and implement applicable solutions.

Detailed Policies, Procedures and Documentation

Processing activity is documented in our internal records, detailing — among other things — all purposes, categories of personal information, retention schedules, and recipients, while constantly being kept up to date by the relevant stakeholders in the R&D and privacy teams.

Personnel vetting and training

Our personnel is trained in privacy and security matters during the onboarding process, as well as on an ongoing and annual basis. Our personnel is subject to disciplinary measures if our policies are violated.

Varonis personnel also must receive proper clearance for accessing personal information and undergo either background checks or appropriate reliability tests.

Keeping Personal Information Secure

Varonis implements a wide array of security measures to keep your information safe and secure. Security measures are also applied to applicable Varonis service providers.

Varonis Certifications and Accreditations

Varonis has achieved numerous certifications and successfully completed audits, including but not limited to **ISO 27001, ISO 27017, ISO 27018, ISO 27701**, **SOC2 Type 2**, **SOC3,** and **CSA's STAR Level 1** security assessment.

The above certifications are only part of the full scope of technical and organizational measures we use. For more information, please visit our Trust Center.

Additional information regarding security matters can also be found in our security standards and practices whitepaper.

Service Providers Compliance

Personal information is transferred only to our service providers (sub-processors) who need to access such information as part of their services. The transfer of personal information to new sub-processors is subject to a Security Risk Assessment (conducted by the CISO team), Transfer Impact Assessment (conducted by the DPO), and procedures that establish the requirements and standards for disclosing or transferring such information. These procedures are designed to ensure that any transfer complies with applicable privacy laws.

Security Risk Assessment

Prior to engaging with a third-party vendor, Varonis conducts a security risk assessment. Varonis thoroughly investigates vendors for security and posture. The risk assessment reviews the vendor's security, compliance, and privacy practices and ensures appropriate safeguards are put in place. Each engagement with the potential disclosure of PII requires an enhanced privacy assessment. High-risk vendors that hold customer data undergo periodic reviews.

Transfer Impact Assessments (TIA)

We do not transfer any personal information to countries outside the European Economic Area (EEA) or U.K. without making sure it is being transferred lawfully and that the transferred information will be in good hands. For that purpose, we perform Transfer Impact Assessments (TIAs), which allow us to ensure that any recipient of personal information has the proper legal, organizational, and security mechanisms in place to avoid any mishandling or abuse of personal information.

TIAs performed by Varonis include a wide variety of inquiries regarding the level of security the recipient can apply to the personal information transferred. This includes questions regarding the organizational, technical, and contractual mechanisms being implemented, the possibility of disclosure of personal information to a governmental authority (mainly, when stored in the U.S.), and the feasibility of transferring personal information exclusively to data centers allowing the maximum protection possible (e.g., data centers in the EU when the GDPR is applicable).

In addition, TIAs cover matters such as whether the laws in the recipient's jurisdiction ensure the integrity of personal data privacy and whether the recipient itself is performing any relevant onward transfers.

TIAs allow Varonis to make informed decisions and maintain control over where personal information is being kept and how it is processed on Varonis' behalf.

Data Processing Agreement (DPA)

Any transfer of personal information will be subject to a data protection agreement (DPA), detailing the parties' obligations under the applicable privacy laws and implementing all safeguards

necessary by law to ensure that personal information will always be treated in accordance with the requirements of privacy laws and industry best standards. These DPAs apply to any external transfer, as well as to internal data transfers between members of the Varonis group of companies.

When required by law, Varonis also incorporates the GDPR's Standard Contractual Clauses (SCCs), or their U.K. counterpart, providing further protection in terms of privacy and security matters whenever personal information is transferred to certain jurisdictions.

Varonis' DPAs also oblige the receiving party (sub-processors) to assist Varonis and maintain various security mechanisms to ensure the security of personal information transferred. For example, data recipients must:

- implement and maintain appropriate technical and organizational methods to protect personal information against accidental or unlawful destruction;
- comply with a detailed list of measures ensuring the security of the information, including having a written security management system, maintaining a security policy that is regularly reviewed, applying encryption, maintaining a firewall configuration, and limiting personal information storage to that which is necessary;
- conduct periodic reviews of network security and adequacy, measured against industry security standards; and
- notify Varonis without undue delay after becoming aware of a security incident and assist in investigations and resolution thereof.

Additional Information and Inquiries

If you would like to know more about our policies concerning privacy matters, please visit our Software Privacy Policy and our Website Privacy Policy.

For any privacy-related questions, you may contact our DPO and privacy team at privacy@varonis.com.