Global Applicant and Employee Privacy Notice

Last Updated – November 1, 2023

California residents can find specific disclosures, including “Notice at Collection” details about how we collect, use, disclose, sell or share, and retain your personal data here.

A. Overview

At Sysdig, we uphold the principle that all individuals are entitled to transparent and trustworthy treatment of their personal data. With this objective in mind, we have created this Global Applicant and Employee Privacy Notice (Privacy Notice) to offer job applicants and members of our workforce comprehensive, explicit, and user-friendly details regarding Sysdig and its affiliated companies' privacy policies.

This Privacy Notice outlines our procedures for collecting, processing and personal data. It is not intended to create any rights beyond those that exist by virtue of applicable privacy and data protection law.

If you are looking for information about how we collect personal data from visitors of our website or users of our products and services, please review the Privacy Policy.

The defined terms we have used in this Privacy Notice have the following meanings:

- “Applicant” means an individual who has submitted information to Sysdig (such as a resume or job application) in order to apply to be a Team Member, or who has otherwise given consent to be considered as a candidate for a position.
- “computing resources” includes all electronic systems, networks, applications, equipment, devices, software, and means of communication operated and managed by Sysdig. As examples, these include but are not limited to, critical business systems, networks, personal computers, laptop computers, personal digital assistants, peripheral equipment such as disk drives, USB drives, printers, electronic mail, Instant Messaging, telephones, computer enabled ID cards and voicemail or other electronic communications or other information systems provided by or on behalf of Sysdig or operated on Sysdig computer or telecommunications hardware or use for conducting Sysdig business.
- “monitor” (and “monitoring”) includes, but is not limited to, intercepting, accessing, reviewing, collecting, recording, processing, organizing, storing, retrieving, transferring, tracking, dissemination, blocking, combining, aligning,

modifying, deleting (e.g. wiping) and removing electronic data related to or contained on computing resources.

- “personal data” (and “data”) means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “processing” (and “process”) means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- “Team Member” means a full or part time Sysdig employee, director or Board member or advisor, as well as members of our extended workforce, including non-executive directors, independent contractors, contingent, or agency workers and interns.
- “Sysdig”[1] means Sysdig Inc. and its affiliated group companies (as listed at https://sysdig.com/legal/subprocessors/).

The majority of this Privacy Notice applies equally to Applicants and Team Members. To the extent there are differences for Applicants, we highlight those throughout this Privacy Notice.

B. What Personal Data Do We Process and Why Do We Process it?

We collect personal data about you from different sources and in various ways during your candidacy or employment, including information you provide directly, information collected automatically, information from third-parties (including service providers, insurance and benefits providers, travel partners, online sources like social networks and recruiting sites or public data sources), and data we infer or generate from other data.

The personal data we process about you may vary according to whether you are an Applicant or Team Member, the type of processing we conduct, the jurisdiction you are located in, and local legal requirements. In general, however, we use your personal data as necessary to administer and carry out the employment relationship or our contract with you, including for human resources purposes, and our operational, business, safety, and security purposes and as further described in the table below.

In addition to personal data, we may use de-identified information in accordance with applicable law.

1. Data categories & examples

Identification data

Name, date of birth, government identifiers, and employee identification number, and badges.

Contact data

Home address, telephone, email addresses, and emergency contact details.

Hiring and work permit data

Information related to applicant qualifications, past employment, interview notes, references, immigration status and documentation, residency permits and visas, national ID/passport, and other official documentation in support of authentication or eligibility for employment (e.g. Form I-9 in the US).

Education and employment data

Information related to your qualifications, your role at Sysdig such as position information, role changes, resignation/termination, resume/CV, office location, employment contracts, performance and disciplinary records, academic/professional qualifications, criminal records data, immigration status and documentation, residency permits and visas, national ID/passport, occupational health assessments and work-related accidents, training and employee resource group participation.

Benefits data

Information related to employment benefits we provide to you such as spouse and dependent information, health information, information about types of benefits used, retirement account information, insurance, vacation, leaves of absence, and accommodations information.

Performance and management data

Information related to performance evaluations or reviews, disciplinary actions and grievances, and training and development plans.

Financial, compensation and tax data

Banking details, tax information, payroll information, withholdings, salary, expenses, insurance and benefit payments, company allowances, and commission and stock and equity grants.

Internet or other electronic network activity; systems and asset use data

Including as related to Applicant communications and use of our devices, systems, wi-fi, internet service, internal and external websites, equipment, applications, databases, network resources, and infrastructure (“Systems”); and personal devices used to connect to our Systems.

Information required to use and provide access to Sysdig's computing resources such as usernames, passwords, aliases, IP addresses, log files, login information, software/hardware inventories, internal communications and video and audio recordings, and information collected by internal Sysdig applications provided to employees such as employee communications tools and platforms.

Usage data such as time spent on our systems, features used, and actions taken in our systems, including page views, links clicked, and documents downloaded; contents, header, metadata, delivery and access information for voice calls, voicemail, emails, chats, messaging, documents, and other communications, data, and files stored or transmitted through our computing resources (at all times in accordance with our monitoring policy as outlined below).

Information collected through cookies and web beacons to operate our websites, applications, and online services accessible to you in the context of our recruiting and hiring relationship.

Asset allocation data and data used for security and business continuity purposes and information required to use Sysdig sites including from CCTV, access, and security controls.

Demographic data

Date of birth, gender, marital status, spouse and dependent information, military service, union membership, race/ethnicity, veteran status, disability and gender expression. Team Members can view their demographic data in the HRIS systems.

Audio, electronic, visual, thermal, olfactory, or similar information

Facial images and voice information, such as photos, videos, CCTV or voice recordings.

Sensitive personal data

To support our legal and business activities, and as permitted by law, we may collect sensitive personal data as part of our applicant or employment relationship with you.

Sensitive personal data that we collect includes: government issued identifiers, account log-in, financial account, password, or credentials that allow access to an account; precise geolocation; sensitive demographic information such as racial or ethnic origin, religious or philosophical beliefs, or union membership; genetic data; health information; information relating to sex life or sexual orientation in certain locations (such as California), the content of your mail, email, and text messages where we are not the intended recipient of the communication.

Other information you share with us

Information you choose to provide including hobbies, social preferences, answers to feedback surveys.

Content of your business communications, such as through our employee and IT support programs (for example, we record employee support and technical support calls) as well as communications via our email service provider, internal website, forms, audio and video recordings, business applications, chat features, and other channels.

Inferences

Inferences drawn from personal data reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

We only process your personal data where we have a legitimate business reason or legal requirement to do so. The table below outlines the main reasons for processing and the types of data involved.

2. Why we process your personal data & data categories

Recruitment and Hiring. During the recruitment and hiring process, we process Applicant personal data to determine suitability and eligibility for a role. This includes identifying prospective candidates and verifying qualifications. It may also include administering lawful background checks and establishing your right to work in a specific jurisdiction. For this processing activity we rely on your consent (for Applicants). We also process data for this purpose as necessary to carry out the employment contract and relationship with you and to comply with our legal requirements.

Identification data, contact data, hiring and work permit data, inferences, sensitive personal data, internet or other electronic network activity

---

Compensation and Benefits. We use this information to manage payroll, taxes, and benefits as well as to process work-related claims (e.g., worker compensation, insurance claims, expense and travel management) and leaves of absence. We also process data for this purpose as necessary to carry out the employment contract and relationship with you.

Identification data, contact data, education and employment data, benefits data, financial, compensation and tax data, sensitive personal data

---

Training and career development. We use this information to help us with creating and updating Team Member training and other development opportunities and enforcing mandatory training completions. For this processing activity we rely on our legitimate interest in ensuring our workforce receives appropriate training and development opportunities. We also process data for this purpose as necessary to comply with our legal requirements.

Employment data

Performance reviews. We use this information to review how you are performing at work and to help determine your work performance requirements and career development needs. For this processing activity we rely on our legitimate interests

in reviewing and improving the performance of our workforce and improving and providing employee services.

Identification data, contact data, education and employment data, performance and management data, financial, compensation and tax data

Legal requirements. We use this information to comply with laws and regulations (e.g. labor and employment laws, health and safety, tax, anti-discrimination laws) or to exercise or defend our legal rights. We process data for this purpose as necessary to comply with our legal requirements or to exercise or defend our legal rights.

Identification data, contact data, education and employment data, hiring and work permit data, benefits data, performance and management data, financial, compensation and tax data, sensitive personal data, systems and asset use data, demographic data

---

Contacts. We use this information internally to compile employee directories or send documents or items to home addresses. For this processing activity we rely on our legitimate interests in conducting our business operations and improving and providing employee services. We also process data for this purpose as necessary to carry out the employment contract and relationship with you.

Identification data, contact data, education and employment data, audio, electronic, visual, thermal, olfactory, or similar information

---

Security & IT. We use this information to maintain the security of Sysdig's computing resources, assets and premises and, provide you with access to them, to manage our general operations and assets through an MDM software, to provide services to you as necessary for your role, and to protect your personal safety. For this processing activity we rely on our legitimate interests in managing our network and information systems security.

Identification data, contact data, education and employment data, hiring and work permit data, inferences, internet or other electronic network activity, systems and asset data, audio, electronic, visual, thermal, olfactory, or similar information

---

Emergencies. We use this information to help us establish emergency contacts for you and respond to and manage emergencies, crises, and business continuity. For this processing activity we rely on your consent.

Identification data, contact data, benefits data

Investigations and Disciplinary actions. We use this information when necessary to investigate and support decisions on disciplinary actions or terminations, conduct grievance management, or when necessary to detect fraud or other types of wrongdoing. For this processing activity we rely on our legitimate interests of securing our business, fighting against fraud and investigating violations of law, our internal policies or the employment contract. We also process data for this purpose as necessary to comply with our legal requirements or to exercise or defend our legal rights.

Identification data, contact data, education and employment data, benefits data, inferences, Financial,compensation and tax data, Internet or other electronic network activity, systems and asset data

---

DEI goals. We use this information as necessary to help us understand the diversity of our workforce and to support core business diversity, equity, and inclusion initiatives. For this processing activity we rely on your consent. We also process data for this purpose as necessary to comply with our legal requirements.

Demographic data, inferences, sensitive personal data

Day-to-day business operations. We may use this information for other legitimate purposes that are reasonably required for day-to-day operations at Sysdig, such as managing our relationship with our employees, accounting, financial reporting, business analytics, employee surveys, operational and strategic business planning, mergers and acquisitions, real estate management, business travel, and expense management. For this processing activity we rely on our legitimate interests in running our business and providing and improving employee services.

Identification data, contact data, education and employment data, hiring and work permit data, benefits data, inferences, financial, compensation and tax data, internet or other electronic network activity, systems and asset data, other information you share with us, audio, electronic, visual, thermal, olfactory, or similar information

---

We will only use this data for the reasons we originally collected it and if we need to use the data for another legitimate business reason, we will notify you and get your permission where required.

3. Jurisdictions With Special Requirements

Legal Basis to Process — If you are from a jurisdiction that requires a legal basis for processing personal data (such as the EEA, UK, or Brazil), Sysdig's legal basis will depend on the personal data concerned and the context in which we collect it. We will normally collect personal data from you only where we need the data to carry out our employment contract with you, to comply with our legal obligations or exercise rights in the field of employment, or where the processing is in our legitimate interests, provided this is not overridden by your data protection interests or fundamental rights and freedoms. We also rely on your consent in certain situations, where permitted by applicable law. You can see examples of the various legal bases we use to process data in the table above.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal data, please contact us at privacy@sysdig.com.

Data Controllers — If you are located in the EEA or the UK, the data controller of your personal data will be the corporate entity that manages the hiring process or employs you.

Global workforce diversity, equity, and inclusion is a priority for us. We collect certain demographic data such as race, ethnicity, disability, and military status to help us understand the diversity of our workforce and to support core business diversity, equity, and inclusion initiatives. In some circumstances, we may also need to use this data to comply with local laws. We generally collect this information on a voluntary consensual basis, and you are not required to provide it unless it is necessary for us to comply with a legal obligation. We will not share your demographic data without your permission unless we are legally required to do so.

C. Who Do We Share Your Personal Data With and Why?

We do not sell your personal data or share your personal data for the purpose of behavioral advertising and we do not allow any personal data to be used by third parties for their own marketing purposes. You can see the type of recipients we might need to share your personal data (including your sensitive personal data) with, and our reasons for doing so, in the table below. We will obtain your consent to any disclosure of your personal data where required by law.

1. Recipients and Why We Share It

Team Members, contractors, and Sysdig group companies

To establish, manage, or terminate your employment with Sysdig.

Consultants and Advisors

To seek legal advice from external lawyers and advice from other professionals such as accountants, management consultants.

Service Providers

To enable third parties to provide services to you on behalf of Sysdig such as recruitment providers, financial investment service providers, insurance providers, healthcare providers and other benefits providers, payroll support services. All service providers we engage to process your personal data on our behalf go through a robust privacy and security vetting process and are required to contract with us on terms that ensure the appropriate use and protection of your personal data.

Partners in Corporate Transactions and their professional advisors

In connection with the sale, assignment or other transfer of all or part of our business.

Government Authorities or Law Enforcement

- If we in good faith believe we are compelled by any applicable law, regulation, legal process or government authority; or
- Where necessary to exercise, establish or defend legal rights, including to enforce our agreements and policies.

Other Recipients

- To facilitate benefits administration;
- To protect Sysdig's rights or property;
- To protect Sysdig, our other customers, or the public from harm or illegal activities;
- To respond to an emergency which we believe in good faith requires us to disclose personal data to prevent harm; or
- With your consent or at your direction, such as for social events hosted by employee resource groups

Please note that some of our internally provided applications and services that we make available to you also include integrations, references, or links to services provided by providers whose privacy practices differ from ours. If you provide personal data via these integrations, references, or links, or allow us to disclose personal data to them, that information is governed by their privacy statements.

Finally, we may disclose de-identified information in accordance with applicable law.

D. How Do We Handle International Transfers of Personal Data?

As a global organization, we may need to transfer your personal data outside your home jurisdiction to Sysdig group companies, including our headquarters in the US, and other countries. These countries may have data protection laws that are different from the laws of your region. We will only transfer personal data to another country in accordance with applicable data protection laws, and provided there is adequate protection in place for the data and will ensure data privacy compliance such as the standard contractual clauses or other mechanism with at the minimum the same protection of privacy that may be established in the future.

If you have a question or a complaint related to our processing of your personal data, you may contact us as indicated below.

E. What is Sysdig's Policy on Monitoring?

1. Overview

We respect your expectation of privacy and only monitor your individual activity if we have a reasonable, proportionate, and legal reason for doing so. Our normal monitoring use cases are outlined in the table below and you can find additional information about the circumstances under which we monitor Team Members on our Policies Page (please note that such policies are not applicable to Applicants).

2. Type of Monitoring & Reasoning

We monitor the physical activity and presence in our offices of Applicants and Team Members with badge readers, sign-in sheets, and video cameras. The data we capture may include identification data, employment data, audio, electronic, visual, thermal, olfactory, or similar information, and Internet or other electronic network activity, systems and asset use data. Though Sysdig is not seeking to collect such information, sensitive personal data and demographic data may also, incidentally, be collected by virtue of our in-office cameras. Where we have in-office cameras, we post signs to let you know.

To prevent unauthorized access to our offices and to protect Team Members, authorized visitors, and our property.

For some Team Member roles, subject to additional notice and your consent, we may record your calls when you speak to customers or potential customers.

For training, verification, or quality assurance purposes.

We may monitor the electronic activity of Team Members on our IT and communications systems and network. This electronic activity includes log files and content sent over our network and specifically may include Internet or other electronic network activity and Systems and asset use data, no matter where generated.

- Validating business transactions and archiving;
- For network and device management and support;
- Protection of confidential information, intellectual property and other business interests;
- To protect our internal systems from security risks, including potential exposure to viruses and malware; and
- For compliance with a legal obligation.

We may conduct individual level monitoring of Team Members' use of physical or IT assets, in each case subject to applicable local laws.

To investigate breaches of Sysdig policies and procedures, or other unlawful or improper acts.

We will conduct our monitoring in a way that is proportionate, justified and lawful and as minimally invasive as possible, and with all necessary consents, supplemental notices and internal approvals.

F. How do we keep your data up-to-date?

We endeavor to use personal data that is up-to-date and accurate. If we are made aware that the personal data that we maintain is inaccurate, we take reasonable measures to rectify the data.

We also need your help to keep our records accurate and current. This means that we need you to be vigilant with keeping information like your address, phone number, and personal email up to date. In some cases, failing to provide us with accurate data will impact our ability to function as a business and to comply with legal obligations.

G. How Long Do We Retain Your Personal Data?

Team Members — We will keep your data for as long as we need it to carry out the purposes we've described above, or as otherwise required by applicable law including applicable labor and employment laws.

Generally, this means we will keep your data until the end of your employment or contract with us, plus the period of time required by the law of the country you are employed in or a reasonable period of time to respond to any inquiries, deal with legal, tax, accounting, or administrative matters, to provide you with ongoing pensions or other benefits or to meet any other post-employment obligations we may have to you.

We seek to minimize our retention of data wherever possible.

Where we have no continuing legitimate business need or legal requirement to process your data, we will either delete or anonymize it or, if this is not possible (for example, because your data has been stored in backup archives), then we will securely store your data and isolate it from any further processing until deletion is possible.

If you have a specific question about how long we store your data, please reach out to us at privacy@sysdig.com.

Applicants — If you apply for a job with us, we retain your data to determine your eligibility for a current or future role with us. The retention periods vary depending on your location and local legal requirements. If you have specific questions about how long we retain your data for the respective jurisdictions please contact us at privacy@sysdig.com

H. How Can You Exercise Your Rights in Relation to Your Personal Data?

1. Overview

Regardless of whether you are an Applicant or Team Member you have the right to make choices about your personal data. Where applicable and in certain circumstances, these legal rights include:

- The right to receive notice of our personal data practices at or before the collection of the personal data;
- The right to update or request the correction of your data if it's out of date, incomplete, or inaccurate;
- The right to request confirmation that we are processing your data and be provided with access to the data we process about you. You also have a right to request additional information about our collection, use, disclosure, sale, or sharing of such data;
- The right to have your data deleted;
- The right to restrict or opt-out of certain types of processing of your data. In particular, you may have the right to request that we limit the use and disclosure of your sensitive personal information;
- The right to transmit your data to another organization (in certain circumstances);
- The right to object to the processing of your personal data;
- The right to withdraw consent for data you've provided to us on a consensual basis;
- The right to obtain information about the entities Sysdig has shared your data with; and
- For residents of France, you can send us specific instructions regarding the use of your data after your death.

You may also have the right not to be discriminated against for exercising any of the rights outlined above.

Team Members — We provide you with a number of tools to help you update, access, or delete some of your data, as detailed below. To exercise other rights, please contact the Privacy Team via our service portal or contact us using the information in the "How do I contact Sysdig?" section below.

Applicants — Please contact the recruiter you worked with or contact us using the information in the “How do I contact Sysdig?” section below to exercise your rights.

To obtain more information, including information about how to designate an authorized agent to make a request for you, please contact us using the contact method described at the bottom of this privacy notice.

In order to process your request, we may need to ask you to provide specific information to help us verify your identity and applicable rights. You may also designate, in writing or through a power of attorney, an authorized agent to make requests on your behalf to exercise your rights under certain laws. Before accepting such a request from an agent, Sysdig may require the agent to provide proof you have authorized it to act on your behalf and may need you to verify your identity directly with us.

Alternatively, we may refuse to comply with the request in certain circumstances. If you receive a response from us informing you that we have declined your request, in whole or in part, you may appeal that decision by submitting your appeal to us.

2. I would Like to:

---

a) Update my data

HRIS System & Email. If your personal data changes during the course of your time at Sysdig, please login to your HRIS account (currently ADP) to update that data.

---

b) Access my data or receive a copy of my data

HRIS & Email. HRIS allows you to see the data that we hold about you and download a copy.

---

c) Delete my data or withdraw consent

HRIS & Email. You can ask that we delete personal data that you believe is inaccurate or no longer relevant by emailing your HR team at hrteam@sysdig.com. In addition, you can go into your HRIS account and the data you’ve chosen to share with us, such as demographic data. We might need to refuse deletion of personal data in certain cases, such as when providing deletion might impact our legal obligations.

I. How Do We Secure Your Personal Data?

1. Overview

We use appropriate technical and organizational security measures to protect the security of your personal data both online and offline including the implementation of access controls, firewalls, use of anti-virus software and other. These measures vary based on the sensitivity of the personal data we collect, process, and store, and the current state of technology. We also take measures to ensure that third parties that process personal data on our behalf also have appropriate security controls in place.

In addition, in accordance with our Code of Ethics and related training, each Team Member has a responsibility to protect data they have access to.

2. What Are Your Responsibilities?

Data Accuracy

We need your help to keep our records accurate and current. This means that we need you to be vigilant with keeping information like your address, phone number, and personal email up to date. In some cases, failing to provide us with accurate data will impact our ability to function as a business and to comply with legal obligations.

Data Usage

Team Members with access to personal data, in addition to complying with the internal policies and completing the relevant training, must endeavor to make wise choices about how they use data. This means ensuring that you are thoroughly assessing (1) why you need the data, (2) whether that use fits the uses outlined above, and (3) whether there is another way to get to your goals without using personal data. After assessing, it's equally important to ensure that you maintain good data security practices for the data in your possession, report data misuse, whether accidental or malicious, and keep up with required training.

Data Confidentiality

We rely on our Team Members to keep data confidential. In addition to complying with the internal policies and completing the relevant training, you may use this data only as necessary for the performance of your role and must protect the confidentiality of personal data at all times.

J. How Does Sysdig Handle Disputes Relating to Personal Data?

We hope we can resolve any disputes relating to our data protection practices between us. However, if you have a dispute with us relating to our data protection practices, you can raise your concern or dispute by contacting our Privacy Team either via email at privacy@sysdig.com.

Right to Complain to a Supervisory Authority — While we hope we can resolve any dispute between us, you have the right to lodge a complaint with the supervisory authority or data regulator in the country where you work or where you consider any data protection rules to have been breached.

Rights under Standard Contractual Clauses for a Controller — You may have additional rights under our Standard Contractual Clauses in the EU and other countries that recognise such clauses. For example, where you believe your personal data has been transferred by an EU-based company to our US headquarters and processed by the US company in breach of the Standard Contractual Clauses (where applicable), you may have a right to:

- File a complaint with the Sysdig entity that transferred your data outside Europe;
- File a complaint with the supervisory authority in the same country as the Sysdig entity that transferred your data outside Europe; and
- Bring a court action against the Sysdig entity that transferred your data outside Europe.

Changes to this Privacy Notice
You can see when this Privacy Notice was last updated by checking the "last updated" date displayed at the top. If we make material changes to this Notice, or in how we use your personal data, we will provide advance notice to you by sending an email via the address we have on file for you. We will comply with applicable law with respect to any changes we make to this Privacy Notice and seek your consent to any material changes if this is required by applicable law.

K. How can I contact Sysdig?

Contact Us

If you have any questions or comments about this Privacy Notice, the ways in which we collect, use, and disclose your personal data, or your choices and rights regarding such use, please contact us as follows:

- privacy@sysdig.com
- 1-888-430-3130