platform.sh

Record of processing activities

Status	Active
Version	v1.8
Owner	Iva Kotur // Erika Bustamante
Reviewed by	Joey Stanford
Date of creation	2019-03-15
Date of last review	2022-02-15
Date of last update	2022-08-10
Classification	**Public**

Table of contents

Company information

Platform.sh	
Management	Fred Plais, CEO
Address	131 Boulevard de Sébastopol, 75002 Paris, France
Phone number	+33 (0) 1 40 09 30 00
DPO	Joey Stanford
Email	dpo@platform.sh

The purpose of the processing

The data we collect is for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

We use the information we collect from customers to provide, maintain, protect, and improve our sites and Services, and to develop new ones. With respect to the EU GDPR, Platform.sh is both a Controller and Processor. We are a Controller for the overall service and in particular when we are in charge of data subjects who are explicitly the users of our services (Infrastructure Control Plane). In relation to the Platform.sh Accounts Portal, Platform.sh is a data controller. We collect the data which we store in the Platform.sh Accounts Portal and it is used by Platform.sh to enable our users to create projects, host websites, or provide services.

We are a Processor for our customers (Controllers) that are in charge of data subjects that they have collected (Customer Data Plane).

Additionally, we may use the information for one or more of the following purposes:

+ To provide information to customers that customers request from us relating to our products or services
+ To provide information to customers related to products or services provided by us
+ To inform customers of any changes, offers, updates, or other announcements about our Services
+ To allow customers to participate in interactive features of our Services when customers choose to do so
+ To provide customer support
+ To gather analysis or valuable information so that we can improve our Services
+ To monitor the usage of our Services

+ To detect, prevent, and address technical issues
+ To provide customers with new Services offers and relevant Services information and events, unless customers have opted not to receive such information

We collect and use collaborators' personal data for the following purposes:

+ To detect, prevent, and address technical issues
+ For recruitment benefits
+ Personnel files
+ Absence records (sickness, maternity, paternity, parental leaves, etc.)
+ Monitoring
+ Personnel reports and severance
+ Perks and benefits
+ Applicant Tracking System

Legal basis for processing

If data subjects are from the European Economic Area (EEA), Platform.sh's legal basis for collecting and using the personal information described in this document depends on the data we collect and the specific context in which we collect it. For each processing purpose listed in this document, Platform.sh has a legal basis for such processing, in accordance with Article 6 of the GDPR. We use the following legal bases:

+ We need to perform a contract with you
+ We have been given permission to do so
+ The processing is in our legitimate interest and it's not overridden by a data subject's rights
+ For payment processing purposes
+ To comply with applicable law

Categories of data subjects

A data subject is identified, or an identifiable natural person 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

At Platform.sh, we collect data from the following data subjects:

1. Collaborators (employees, interns, contractors, work-study individuals)
2. Customers
3. Prospects, including conference attendees

Categories of personal data

Customers and prospects

We collect information that customers and prospects give us or that we get from customers' use of our sites and Services, including without limitation, the following:

+ Personal data (name, surname, address, photo, date of birth, phone number)
+ Financial/bank info
+ Online identifiers (IP address, log files)
+ Internet (cookies)

Collaborators

We also collect data from collaborators to comply with obligations under employment law, as well as to protect collaborators. The data collected include the following:

+ Financial/bank info
+ Personal data (name, surname, address, photo, date of birth, phone number)
+ Professional life (ex: CV, diplomas, education, etc.)
+ Government ID/Social Security
+ Financial/bank info
+ Healthcare Data (US FMLA status only)
+ Criminal background check, emergency contact, family information as part of healthcare coverage (ex: number of children, name, date of birth, and place of birth of children and spouse, salary information, role)
+ Online identifiers (IP address, log files)

We do not process any of the special categories of personal data, except when hosting a conference or event, and attendees need special health accommodations. Attendees will be required to provide explicit consent for these accommodations

Special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Retention

Customers and prospects

Platform.sh will retain customer personal information only for as long as is necessary for the purposes set above. We will retain and use customer personal information to the extent reasonably necessary to comply with our legal obligations (for example, if we are required to retain customer data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. Platform.sh retains usage data for a reasonable time period to pursue a legitimate business interest, or for internal analysis purposes. Usage data is generally retained for up to 14 months, except when this data is used to strengthen security, improve the functionality of our Services, or we are legally obligated to retain this data for longer time periods.

Collaborators

Platform.sh will retain collaborators' personal information only for as long as necessary for the purposes set above, such as to comply with labor, tax, social security legislation, or any other regulations that require the retention of collaborators' personal data for reporting purposes.

We have also created and implemented a Data Retention Policy.

Data Mapping

In order to have an inventory of the data processing and an overview of what we are doing with the concerned personal data, we have created a Data Inventory list.

We have also created a Personal data flow diagram - Client data and Employee HR and Finance Data Flow Diagram to track how we gather the data and how the data flows through various internal and external systems.

Recipients to whom the personal data will be disclosed

Customers and prospects

We will not disclose customers' personal information to any other party other than those in our Sub-processor List, which can be sent upon request. Further, we will only disclose customers' personal information in accordance with our Privacy Policy and under the circumstances detailed below:

+ Consent: We may disclose personal information if we have a customer's specific consent to do so.
+ Co-sponsored activities: When customers sign up for a webinar or other activity that is co-sponsored by another company, we may share customer registration information with that company.
+ Third-Party Services: We use trusted third-party service providers, consultants, and other agents to help us provide, maintain, protect, and improve our Services. We may provide customers' personal information to such third-party service providers to perform certain tasks based on our instructions and in compliance with this Privacy Policy. Examples of third-party services include data storage, maintenance services, database management, web analytics, and payment processing.
+ Legal: We will share personal information if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- under certain circumstances, comply with legal obligations, meet applicable laws, regulations, or legal processes, or enforceable governmental requests (however, we will use reasonable efforts to provide notice to Platform.sh's customers when we receive a request for customer personal data unless Platform.sh is explicitly prohibited from doing so by applicable laws)
- enforce applicable Terms of Service or any of our other agreements with you, including investigation of potential breaches
- detect, prevent, or otherwise address fraud, security, or technical issues in connection with the Services
- protect against harm to the rights, property, liability, or safety of Platform.sh, our users and customers, or the general public, as required or permitted by law
- prevent an emergency when a person is at risk of potential imminent death or serious physical injury, and Platform.sh may have personal data necessary to prevent such emergency
- protect against apparent instances of child exploitation or missing children detected on Platform.sh's services

+ Succession: If we are involved in a merger, acquisition, or asset sale, customers agree that customers' personal information may be transferred to such third-party.

Collaborators

We do not disclose collaborators' personal data to third parties unless we are legally obliged to do so, or for the provision of benefits.

In order to comply with a legal obligation we will disclose collaborators' personal data to the following parties:

+ Social security and healthcare organizations (ex: public and private health insurance, dental insurance, etc.)
+ Accountants (ex: salaries, tax legislation, etc.)
+ Organizations that perform background and security checks
+ Organizations that deal with training and work-study contracts (ex: Fafiec)
+ Other organizations in order to exercise relevant HR requirements (ex: BambooHR, food vouchers, recruitment, etc.)

Transfers of personal data to a third country or an international organization

We may transfer personal data outside of the European Economic Area (EEA) to countries with and without an EU adequacy decision to enable customers to rapidly deploy projects in any geographical region. Some of our computer systems are based outside of the EU, and therefore, customers' personal information may be transferred to and processed by us in those locations.

Customer name, email, and ssh keys may be transferred from the Platform.sh Accounts portal located in Ireland to clusters in France, Ireland, USA, Australia, Canada, Germany, and the United Kingdom using securely encrypted transfer channels (TLS) and encrypted at rest. Platform.sh transfers its data, only as necessary to fulfill a needed function, to companies that are GDPR compliant or to those which meet an adequate level of data protection. Platform.sh signs Data Processing Agreements or Standard Contractual Clauses (SCCs) with all processors, and has replaced vendors who fail compliance assessments. We also conduct Supplementary Measures Assessments on vendors who store personal data in non-adequate countries.

Security measures

We take all reasonable measures to:

+ Protect customers' and collaborators' personal data and information, as well as our Services from, unauthorized access to, or unauthorized alteration, disclosure, or destruction of, the information we maintain.
+ Ensure that we are in compliance with the EU General Data Protection Regulation (GDPR), Germany's BDSG, Canada's PIPEDA, the California Consumer Privacy Act, the Australian Privacy Act, HIPAA, and other privacy regulations as described in our Privacy Policy.

Platform.sh is audited by third parties and maintains SOC 2 Type 2 and PCI-DSS Level 1 certifications.

Customers

+ Auto-redundant architecture
+ Project & data isolation
+ Security updates & stack management
+ Permissions & access management
+ Data protection compliance
+ Subprovider certifications

In order to satisfy compliance obligations and security requirements, we perform an annual review of our InfoSec policies, as well as an annual supplier GDPR and security review. We use Compliance and Security questionnaires in order to learn about vendors' security programs and practices, as well as to gather information about their compliance with relevant data protection laws. In addition, these questionnaires help us to determine any risk connected to a specific vendor.

Customers can visit our Security page to get more information about the security measures mentioned above.

Collaborators

+ All collaborators must complete annual GDPR, Data Protection, and Security awareness training, as well as training on secure coding, PCI-DSS, and SOC 2.
+ SentinelOne antivirus installation is mandatory for all collaborators
+ We have implemented a PCI-compliant Password Policy
+ Incident Management procedures are in place

Privacy Impact Assessments

We have completed Privacy Impact Assessments on all our Processing Activities in order to assess and identify privacy and data protection impacts. This enables us to take appropriate actions to prevent or, at the very least, minimize the risk of those impacts.

Risk Assessments

We have identified all the essential assets in our Asset Registry and have identified potential threat vectors, threat actions, and vulnerabilities that may negatively impact the company's assets and created a Risk Registry.

Furthermore, we perform risk assessments on all of our vendors.

We analyze potential threats and ensure we have appropriate prevention and mitigation strategies in place.

Business Impact Assessments

In our Business Impact Assessments, we have determined the consequences of disruption of our business functions and processes and have designated a maximum tolerable downtime (MTD). We have also identified potential loss scenarios. This effort has enabled us to gain a more comprehensive understanding of the potential business and financial impacts on our organization.