DATA PROTECTION POLICY

Version Number:	3.1
Version Date:	10/09/2025
Owned by:	Security GRC
Approved by:	Nate Fitch, Sr. V.P., Chief of Staff
Confidentiality level:	Internal

Table of Contents

1. Purpose

This policy establishes Docker's framework for protecting the privacy rights of individuals whose personal data is collected, processed, or stored by the organization. It ensures all processing of personal data complies with applicable privacy laws including GDPR, CCPA, and other global data protection regulations, while upholding principles of fairness, transparency, and accountability.

The policy mandates:

- Identification and documentation of lawful bases for all personal data processing activities
- Implementation of data protection principles including purpose limitation, data minimization, accuracy, and storage limitation
- Technical and organizational measures to ensure confidentiality, integrity, and security of personal data
- Processes for honoring data subject rights including access, rectification, erasure, portability, and objection
- Privacy by Design integration into systems, processes, and services from inception
- Vendor governance ensuring third-party processors meet equivalent privacy standards through Data Processing Agreements
- Incident response procedures with timely breach notification to authorities and affected individuals
- Regular privacy impact assessments for high-risk processing activities

This framework ensures Docker processes personal data lawfully and ethically, maintains trust with customers and employees, supports transparent data practices, and privacy regulations. It protects individuals' fundamental privacy rights while enabling Docker to conduct legitimate business operations.

2. Scope

This policy applies broadly to all individuals and entities involved in the handling of personal data within Docker’s operational ecosystem. It governs the actions of Docker personnel, including employees, contractors, vendors, and third-party service providers, who are granted access to personal data in the course of their work.

The scope of this policy includes all personal data that is collected, stored, transmitted, or otherwise processed on behalf of Docker, regardless of whether it resides in digital systems, physical records, or cloud-based environments. It applies uniformly across all environments where personal data may be handled, including production systems, testing platforms, and development environments.

This policy specifically addresses the management of personal data associated with a wide range of stakeholders, customers, employees, business partners, vendors, and any other individuals whose information is entrusted to Docker. Its requirements are intended to ensure consistent, secure, and lawful handling of personal data throughout its lifecycle, from collection through disposal.

3. Roles and Responsibilities

Role	Responsibilities
Head of Legal	Owns the privacy program, ensures compliance with global privacy laws, maintains this policy, and advises on legal risks related to personal data. Legal also verifies adherence to regulatory requirements, maintains processing records, and supports regulatory and customer audits.
Security Team	Implements and monitors technical safeguards (e.g., encryption, access controls), supports breach response, and performs regular control audits.
Engineering / Product Teams	Integrate Privacy by Design and Default into new systems and services, support DPIAs, and ensure that new features do not introduce unnecessary privacy risk.
IT Operations	Ensures proper system configuration for data storage, retention, and destruction based on privacy requirements.
All Employees and Contractors	Handle personal data in accordance with this policy and complete mandatory privacy training; promptly report suspected violations or data breaches.

4. Definitions

Personal Data - Any information relating to an identified or identifiable natural person, including names, identification numbers, location data, online identifiers, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity.

Data Subject - The individual to whom personal data relates and who can be identified directly or indirectly from that data.

Lawful Basis - The legal justification required under privacy regulations for processing personal data, including consent, contractual necessity, legal obligation, legitimate interest, vital interests, or public task.

Data Processing Agreement (DPA) - A legally binding contract between Docker and third-party processors that defines the scope, nature, purpose, duration, and type of personal data processing, including security obligations and sub-processor restrictions.

5. Data Protection

This Data Protection Policy describes how Docker must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

Personal Data Must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Everyone who works for or with Docker has some responsibility for ensuring data is collected, stored and handled appropriately.

However, these people have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that Docker meets its legal obligations.
- Executive management is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating third-party services, the company is considering using it to store or process data. For instance, cloud computing services.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Docker holds about them (also called 'subject access requests').
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

6. General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Docker will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used, and they should never be shared. Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager, the data protection officer, or Docker Legal if they are unsure about any aspect of data protection.

7. Data Use

Personal data is of no value to Docker unless the business can make proper use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data must not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted / password protected before being transferred electronically. The External Sharing Policy explains how to send data to authorized external contacts.
- Personal data should never be transferred outside of the European Economic Area without prior approval and legal mechanism in place.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

8. Data Accuracy

Docker is required to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible as follows:

- Data will be held in as few places as necessary. Staff must not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Docker will make it easy for data subjects to update the information Docker holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

9. Subject Access Requests

In support of global data privacy regulations including but not limited to the GDPR, UK Extension, Swiss-U.S, and all other privacy regulations, all individuals who are the subject of personal data held by Docker may be entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it. Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by visiting our privacy policy and clicking on the appropriate link to our standard web form.

We will always verify the identity of anyone making a subject access request before handing over any information.

10. Providing Information

Docker aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights including deletion of their personal data i.e. exercising the "Right to be Forgotten".

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is available on request. A version of this statement is also available on the company's website.

11. Enforcement and Exceptions

All Docker personnel are expected to comply with this policy in full. Failure to adhere may result in disciplinary action, up to and including termination of employment or contract. In cases involving willful misconduct, malicious activity, or violations of law, Docker may initiate legal proceedings. The organization reserves the right to monitor, audit, and inspect user activity on its systems to ensure compliance.

Any exceptions to this policy must be formally requested, documented, and approved by Docker's GRC or Legal team. Exception requests must clearly outline the business justification and associated risks, and should be submitted to Docker's Risk Submission Portal.

12. Reference Documents

- Information Security Policy
- Data Classification Policy
- Data Handling Policy
- Incident Management Policy
- Appendix A: Customer PII Definition Document

13. Change History

Date	Version	Created by	Description of change
10/09/2025	3.1	Nate Fitch, Sr. V.P., Chief of Staff	Revised policy approved
10/8/2025	3.0	Stephen Oriowo, Sr GRC Analyst Chad Fryer, Sr GRC Engineer	Annual policy update
06/12/2024	2.1	Joel Benavides, Head of Legal	Revisions approved
05/21/2024	2.0	Rachel Taylor, Director, Security, Risk & Trust Karen Hajioannou, Senior Security & Compliance Engineer	Policy annual review and update
02/6/2023	1.2	Joel Benavides, Head of Legal	Draft document approved
01/12/2023	1.1	Rachel Taylor, Senior Manager, Security, Risk & Trust	Draft Submitted for review
12/19/2022	1.0	Rachel Taylor, Senior Manager, Security, Risk & Trust	Basic document outline

Appendix A: Customer PII Definition Document

Customer Personal Identifiable Information (PII)

Definition Document

Overview

Personal Identifiable Information (PII) and “personal data” (under the GDPR), refers to any information relating to an identified or identifiable natural person. This includes information that can be used alone or in combination with other data to distinguish or trace an individual's identity.

Scope

Note that while this document outlines PII in general, this document focuses on customer (end-user) data. As opposed to other PII sets (employee, vendor, etc).

What Constitutes Customer PII

Direct Identifiers

These elements can identify an individual on their own:

Personal Identifiers

- Full name
- Biometric data (fingerprints, iris scans, facial recognition data, DNA)
- email addresses that identify an individual including an email address with their employer’s email domain i.e. company email address.
- Personal phone numbers
- Home addresses
- Photographs that show identifying features

Government-Issued Identifiers

- Social Security Numbers (SSN) (or national ID)
- Driver's license numbers
- Passport numbers
- State-issued ID numbers
- Tax identification numbers
- Military ID numbers

Financial Information

- Bank account numbers
- Credit/debit card numbers
- Financial account numbers
- Investment account information

Health Information (also called "PHI" were handled by HIPAA covered entities and business associates).

- **Docker should not be handling customer PHI. If you encounter customer PHI at Docker, please immediately escalate to the GRC team. Do not agree with any party to Docker being deemed a business associate of any covered entity as defined by HIPAA and/or a foreign health information privacy regime equivalent).**
- Medical record numbers
- Health insurance ID numbers
- Medical diagnoses when linked to identity
- Prescription information

Digital Identifiers

- IP addresses
- Device identifiers (MAC addresses, IMEI numbers)
- Social media handles/usernames (when linkable to real identity)
- Personal URLs
- Digital certificates

Indirect/Quasi-Identifiers

These become PII when combined with other information: There need to be a correlation of two or more of these to constitute PII.

- Zip codes (especially when combined with birthdate)
- Gender
- Race/ethnicity
- Age or birth year
- Job title and employer
- Educational institution and graduation year
- Vehicle registration numbers
- Geolocation data
- Browser cookies (when linked to identity)

Sensitive Categories (handle with heightened care and controls)

- GDPR special categories: race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for identification; health; sex life or sexual orientation.
- US/California 'Sensitive Personal Information' (examples): SSN and government IDs; account credentials; precise geolocation; racial/ethnic origin; religious beliefs; union membership; genetic and biometric data; health data; contents of communications; sexual orientation.

What Is NOT Considered Customer PII/Personal Data

Anonymized or Aggregated Data

- Statistical data that cannot be reverse-engineered to identify individuals
- Data sets where identifying information has been properly removed
- Aggregated demographic information (e.g., "35% of users are aged 25-34"), aggregated from sufficiently sized datasets

Public Business Information

- Business phone numbers (general lines)
- Business addresses
- General business email addresses (info@, support@) as compared to john.doe@acme.com
- Company names
- Business registration numbers
- Public job postings

Generic Information

- Country of residence (without additional identifiers)
- Language preferences
- Time zone
- General product preferences (not linked to identity)
- Anonymous survey responses
- Device type (e.g., "iPhone" without specific identifiers)

Properly De-identified Data

- Randomly generated user IDs that cannot be linked back
- Hashed data that cannot be reversed
- Tokenized information where tokens cannot be traced back
- Test data using fictional information

Quick Test: Is it PII?

Ask yourself:

1. Can this identify a specific person by itself? → **Yes = PII**
2. Could this identify someone if combined with other data? → **Yes = Probably PII**
3. Is this about a business rather than a person? → **Yes = Probably NOT PII**
4. Has this been properly anonymized? → **Yes = NOT PII**