

Harpocrates overview

> **Read time**: 10 minutes

> **Prerequisite**: You have registered in <https://app.privacyone.co> and agreed Privacy1 service terms of use.

> **Mission**: Understand the legal and technical scope Harpocrates paradigm so your business can start a trial.

Introduction

When a business is required to comply with data privacy regulations such as the General Data Protection Regulation (GDPR)

or California Consumer Privacy Act (CCPA) the business must apply the legal requirements into different areas. In general fulfilling the following areas will help your business establish a very solid defensible position.

- * Lawfulness and data transparency
- * Data security
- * Accountability and governance
- * Privacy rights management

Harpocrates system achieves these goals by giving your business and its end users more explicit controls over what data is

collected, why the data is processed, how the data is processed, when the data is accessed and finally to what extend the

data can be processed etc. Privacy1 has packaged everything into an infrastructure so your business can effortlessly comply

with data regulations. The overview architecture looks like the following diagram:

alt="harpocrates" width="800" height="450"/>

In principle Harpocrates does not store any personal data from your business systems. If a client needs our help to implement some very complicated workflows, we have to store such data. But you can be assured, those cases are rare and Harpocrates uses the same technology internally to guard any client's data.

Lawfulness and data transparency

Not all regulations require consent as the lawful basis. Showing respect to user consent nevertheless try gain more trust from your users and add a big plus for your services. With the technology implemented in Harpocrates, you can bring data transparency both ex Ante (before data disclosure) and ex post (after data disclosure) to all data stakeholders.

- ✓ User Consent
- ✓ Data privacy policy
- ✓ Data processing purpose
- ✓ Workflow for handling data subject access requests
- ✓ Data processing activities recording | Data mapping

Data security protection

Privacy1 implemented a patented encryption and key management system to realize data pseudonymization. In addition to that, your business can manage data risk analysis and conduct impact assessment using a model established by ISO 29134. Data permission is clearly defined and easily managed like never before.

- ✓ Data Pseudonymization in services with database
- ✓ Data Pseudonymization in data pipelines
- ✓ Data permission governing
- ✓ Data access control workflow (Tech | Legal | Actual data usage)
- ✓ Data usage separation in micro-services
- ✓ Data risk analysis
- ✓ Data protection impact assessment

Data accountability

Every operation is role-based. Each role is assigned certain permissions in data processing activities. In essence Harpocrates guarantees only end users can mutate their own data. Data reading permissions should only be granted to an authenticated service account in business for processing purposes. Tech team members should get permissions from legal in order to read personal data.

- ✓ Data compliance auditing
- ✓ Service account and user account for data management
- ✓ Role-based privacy management system, Privacy Console (DPO | Admin | Engineering)

Data subject privacy rights management

We love automation. There is no excuse not to automate Data subject privacy rights management. Because your business never

wants to spend engineering hours on tracking down personal data and having it restricted or deleted. This can divert your business

from its main course if you get those requests in high frequency or in high volume.

- ✓ Privacy Manager UI for data subjects privacy rights management
- ✓ Automate data subjects' data restriction requests
- ✓ Automate data subjects' data erasure requests
- ✓ Automate data subjects' data objection requests
- ✓ Automate data subjects' data access requests

Integration

The software integration is done in both front-end and back-end of your system.

A business usually develops a Privacy Manager for its end users to manage their privacy settings on its website or in its mobile apps. The Privacy Manager can either embed Privacy1's code or directly call Privacy1's APIs to access Privacy1's infrastructure.

A business can deliver its privacy compliance work in phases with Privacy1's solution. The golden path option, which takes few engineering resources, is provided for a business to quickly start handling the requests from its end users. It focuses

on laying the foundation for your compliance work. The second phase Privacy by Design concentrates on data automation, data workflows, and security enforcement and therefore will require more engineering hours to complete.

To view the Golden Path documentations, please start a trial of Harpocrates service by downloading the trial license on the [License](<https://app.privacyone.co/license/purchase>) page.

To view the Privacy by Design documentations, please purchase a commercial license on the [License](<https://app.privacyone.co/license/purchase>) page.