Title: Replenit SECURITY, PRIVACY, AND ARCHITECTURE DATASHEET
Owner: Security Team / DPO
Version: 1.2
Update Date: 24.12.2025

Replenit SECURITY, PRIVACY, AND ARCHITECTURE DATASHEET

(effective as of December 2024; subject to change without notice)

Introduction

The goal of this document is to provide high-level information to our customers regarding Replenit's commitment to security and data protection.

Replenit's Corporate Trust Commitment

Replenit is committed to achieving and maintaining the trust of our customers. Our goal is to be as transparent as possible with our customers in offering state-of-the-art security and protections to meet and exceed expectations in today's modern computing world.

1. Policy Ownership

Replenit has a documented information security policy that all employees must read and acknowledge. This policy is reviewed and updated annually. Security policy development, maintenance, and issuance is the responsibility of the Replenit Security Team.

2. Replenit Infrastructure

Replenit uses Microsoft Azure and Google Cloud for European hosting.

For Europe-hosted customers, Replenit hosts the Replenit Services with Microsoft Azure (Microsoft Deutschland GmbH", registered with the District Court of Munich under the commercial register number HRB 70438, with the European Unique Identifier (EUID) DED2601V.HRB70438, is a company incorporated and having its registered office at Walter-Gropius-Str. 5, 80807 München, Germany) or Google Cloud (**Google Cloud Poland Sp. z o.o. registered in** Rondo Daszyńskiego 2C 00-843 Warsaw, Poland)

3. Third-Party Architecture

Replenit may use one or more third-party content delivery networks to provide the Replenit Services and to optimize content delivery via the Replenit Services. Content items to be served to subscribers or end-users, such as images or attachments uploaded to the Replenit Services, may be cached with such content delivery networks to expedite transmission. Information transmitted across a content delivery network may be accessed by that content delivery network solely to enable these functions.

4. Audits, Certifications, and Regulatory Compliance

Replenit, an EU-based entity established in Warsaw, Poland, primarily processes personal data within the European Economic Area. Where personal data is transferred outside the EEA, Replenit ensures an appropriate legal transfer mechanism is in place, including the European Commission's Standard Contractual Clauses and, where applicable, reliance on adequacy decisions such as the EU–U.S. Data Privacy Framework, the Swiss–U.S. Data Privacy Framework, and the UK Extension thereto.

Security Controls

5. Organization Security

Replenit's CPO is responsible for the overall security of the Replenit Services, including oversight and accountability. Replenit's contracts with third-party hosting providers such as Microsoft Azure, Google Cloud include industry-standard information protection requirements.

6. Asset Classification and Logical Access Control

Replenit maintains an inventory of essential information assets such as servers, databases, and information. All Customer Data is classified as Confidential by Replenit.

Replenit adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff. Replenit maintains separate development, staging (or sandbox), user acceptance testing, and production environments access to each environment and within each environment is strictly controlled.