Technical and Architectural Overview

Solution Overview

Papirfly is a comprehensive platform designed to streamline the management and utilisation of digital assets and marketing resources. Our platform leverages AWS infrastructure to ensure robust, scalable, and secure operations.

The Papirfly Platform consists of the following tools:

- Point
- Place
- Produce
- Plan
- Prove
- Plus

Data Upload

Users can upload various types of digital assets (e.g., images, videos, documents, …) to the Papirfly Platform using the secure HTTPS protocol. This can be done manually via the web interface or through automated processes such as API integrations.

Data Processing and Storage

Once data is uploaded to the Papirfly Platform, it undergoes processing to ensure it is optimized and securely stored. This processing includes validation, categorization and indexing, making the data easily retrievable. The Papirfly Solution is designed in such a way as to minimise the amount of personal data it requires in order for a customer to access the platform. In most instances, just basic contact details (login name, email address) are required.

Our hosting provider (AWS) is located in Sweden (EU) and is thus bound by the GDPR.

Data Utilisation

The data stored within Papirfly's infrastructure can be accessed and utilized through various methods, enhancing the flexibility and efficiency of the platform:

1. Web Interface
   Users can interact with the Papirfly Platform via an intuitive and user-friendly web interface. This allows users to search, retrieve and manage their digital assets effortlessly. Advanced search capabilities and organised asset libraries facilitate quick access and efficient asset management.

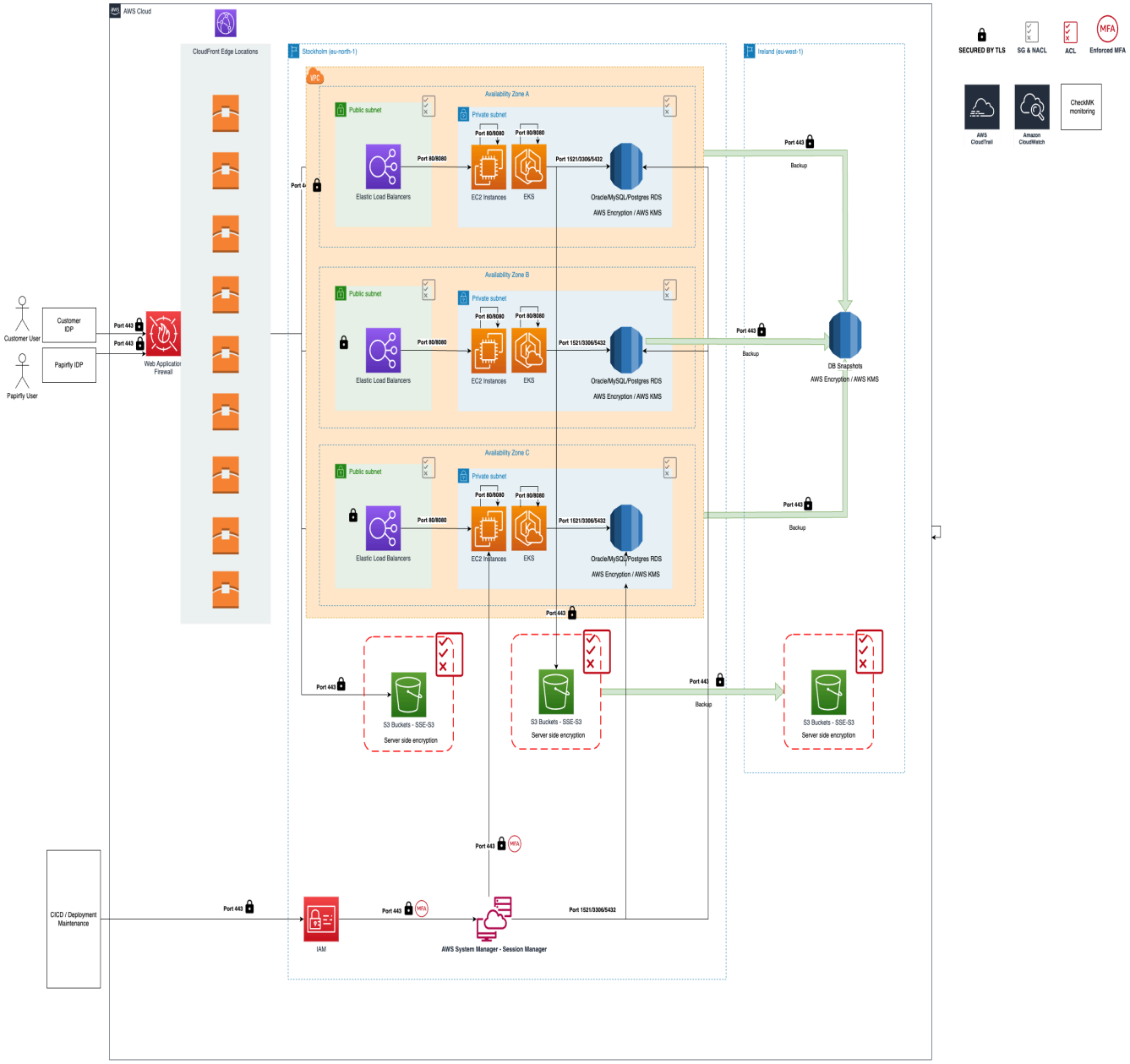
2. API integration
   For developers and technical users, Papirfly offers comprehensive REST API integration. This enables programmatic access to the platform’s features, allowing seamless integration with other systems and applications. Developers can leverage these APIs to automate workflows, synchronize data, and build custom solutions.

3. Collaboration Tools
   Papirfly includes a suite of collaboration tools designed to enhance team productivity and streamline workflows.

Cloud Infrastructure

The Papirfly Platform operates on a robust and scalable infrastructure provided by Amazon Web Services (AWS). Utilizing AWS’s extensive suite of cloud services, Papirfly ensures high availability, security and performance for its users

The following diagram provides a simplified representation of the data flow within the Papirfly platform, highlighting key components and processes involved.



Security Highlights

Infrastructure Security

The Papirfly Platform leverages the robust security infrastructure provided by Amazon Web Services (AWS) to ensure the highest levels of security and compliance for its users. AWS infrastructure security is built upon a multi-layered approach that encompasses physical, operational, and software measures to protect data and ensure service reliability.

Physical Security

AWS data centers are housed in nondescript facilities with strict access control mechanisms. They use multiple layers of physical security, including 24/7 surveillance, intrusion detection systems, and multi-factor authentication for access.

Network Security

AWS employs advanced network security measures, including firewalls, encryption in transit, and private networking options like Virtual Private Cloud (VPC). These measures ensure secure and isolated communication channels within the cloud environment. Common authentication protocols may be used to access the Papirfly solution including OAuth 2.0, SAML 2.0, ADFS 2.0, OpenID.

Data Security

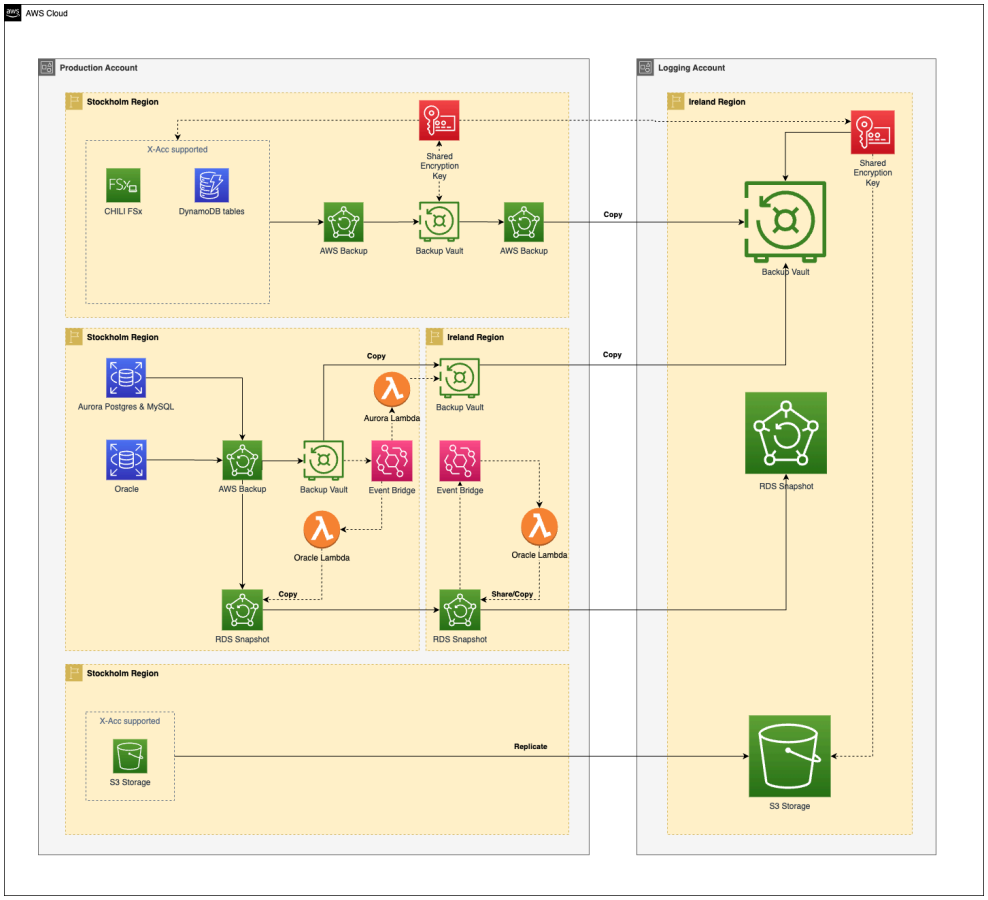
Data stored on AWS is encrypted both at rest and in transit using advanced encryption standards. AWS Key Management Service (KMS) allows Papirfly to create and manage cryptographic keys for enhanced data security using Amazon's S3 managed keys (SSE-S3) that feature AES-256 bit encryption.

Compliance

AWS participates in numerous compliance frameworks to provide assurance to customers across various industries. These frameworks include GDPR, HIPAA, FedRAMP, and many others, ensuring that AWS services meet stringent regulatory requirements. Papirfly itself complies with GDPR by hosting all customer data within the EU and employing a DPO and Compliance Manager to monitor and maintain compliance across all the different countries it operates in.

Data Backup and Recovery

The following diagram provides a representation of data backup workflow.



The following resources are backed up in AWS on a daily basis and transferred to a Backup Vault.

- Databases
- S3 Buckets
- Chili FSX file system
- AMIs

- EC2s

Papirfly has a robust and fully audited business continuity plan that ensures availability is maintained at all times during a disruptive incident. There is a standard RTO and RPO in place in case of a severe event when a disaster recovery plan may be activated by restoring backups from an alternative hosting location within the EU if required.

Certification

Papirfly currently has ISO 22301 Business Continuity Management System certification and has recently started the ISO 27001 Information Security certification process. Papirfly also uses Amazon Web Services (AWS) as a hosting provider and therefore benefits from all the AWS ISO certifications and SOC reports.