zapflow

Security whitepaper

Updated Sep 28, 2023

Subject to change without prior notice.

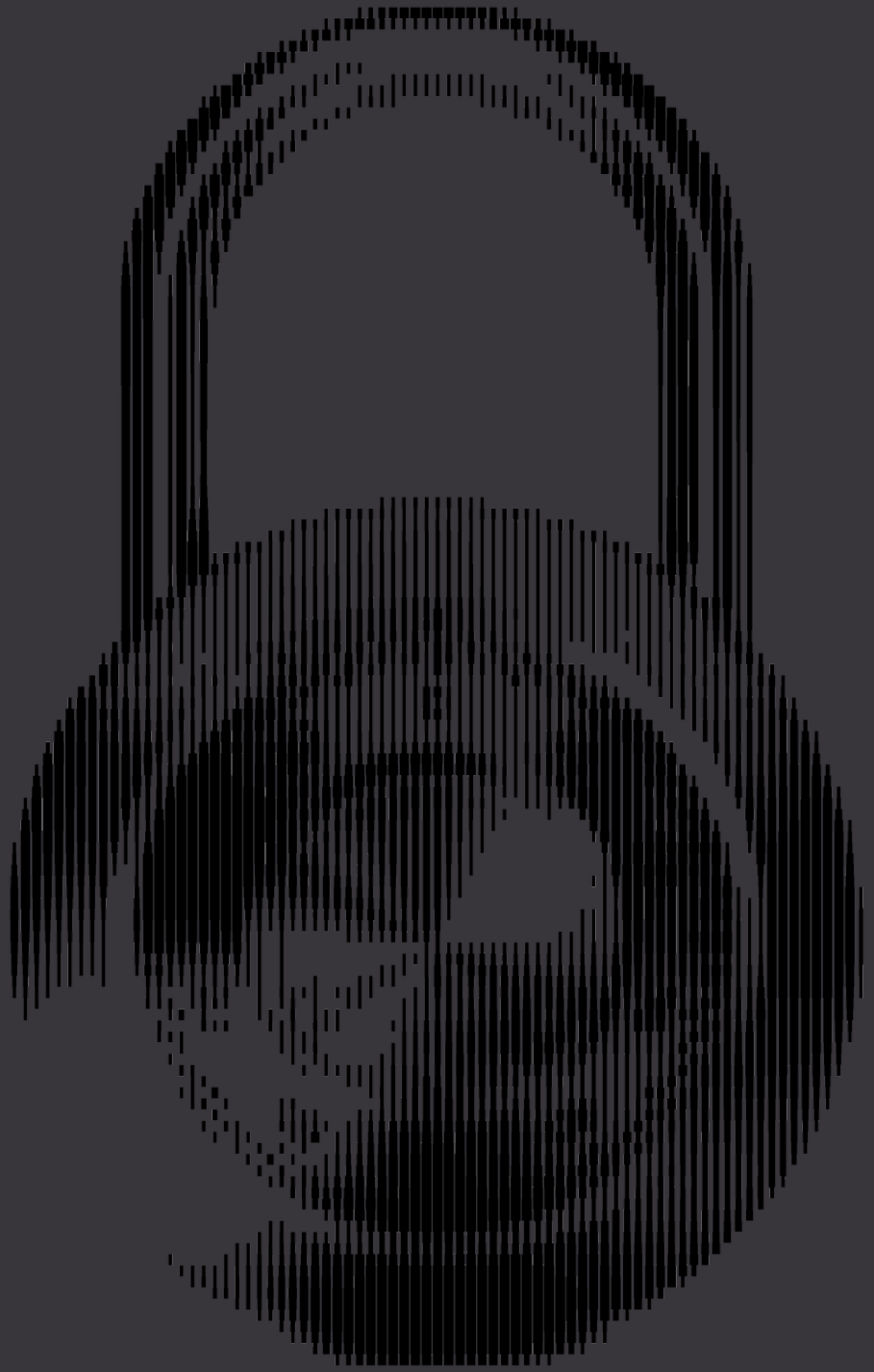

Table of contents

ZAPFLOW

Zapflow is a secure tool for investment professionals to efficiently manage deal flow, fundraising and portfolio monitoring all on one platform.

Certifications

- GDPR Compliant
- SO/IEC 27001

Product Offering

Zapflow offers a range of plans that provide users with affordable, easy-to-use technology to help you run your investment operations. Our suite of tools help you raise your next fund quicker, conduct due diligence, manage tasks, and seamlessly collaborate within your firm.

Front Office Edition

For teams who want the most essential features and require only a few services.

Enterprise

For teams, and organizations, which demand an exceptional competitive edge and may have special requirements.

TECHNOLOGY

Zapflow is a cloud-hosted web application which utilizes best-in-class providers for maximum security and availability.

Cloud Infrastructure

Zapflow's production systems are selectively hosted by Amazon Web Services (AWS), the industry's leading provider of cloud infrastructure. Building on AWS ensures the most secure and reliable global infrastructure with the assurance that control of all our data remains firmly in our hands.

AWS enables a multi-tier virtual encapsulated cutting-edge architecture comprised of AWS Elastic Compute Cloud (EC2) application and database servers, message brokering systems, caching servers, and monitoring tools. Backups of our encrypted data are stored in AWS Simple Storage Service (S3) which provides a durability of 99.999999999%.

AWS as a cloud infrastructure provider maintains recognized security certifications in alignment with the best security practices and IT security standards. The following is a partial list of assurance programs AWS complies with:

- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27017, ISO 27018

More information can be found at https://aws.amazon.com/security

TECHNOLOGY

Third-Party Vendors

All third-party vendors are carefully vetted by our security professional before integrations. Each decision to enter into a contractual agreement with a third-party vendor is discussed with the utmost diligence to ensure we can continue to promise our customers a rigorous security profile.

In addition to AWS providing our cloud infrastructure, our technology utilizes the following third-party vendors to extend our customer offering:

oneflow

Service Provider for e-signatures and contract management (optional).

twilio

Service Provider for SMS notification service (optional).

Clearbit

Service Provider for optional add-on Data Enrichment and Opportunity Matching Engine features. Customer's use of these features involves data transfers subject to EU Commissions Standard Contractual Clauses (optional).

INTERCOM

Service provider for customer support conversations, qualifying as a processor for Customer Data if you provide Customer Data in conversations with our Customer Success team.

nylas

Service Provider for optional add-on Email Synchronization feature. Customer's use of these features involves data transfers subject to EU Commissions Standard Contractual Clauses. (optional)

Proactive Security Practices

Automated Scanning

Zapflow uses aggressive automated application scanning tools to investigate and monitor its potential attack surface. Any revealed vulnerabilities are immediately escalated to be mitigated by Zapflow's CISO, ensuring our application's security via a human-augmented approach.

Business Continuity Plan

Zapflow developed and implemented a set of procedures to ensure Business Continuity, despite any potential threats and malicious activities. Business Continuity Testing performed at least annually to guarantee SLA level and effectiveness of Business Continuity Plan.

Security

Zapflow adheres to rigorous information security practices and is compilant with industry-standard certification ISO/IEC 27001

Certifications

To stay compliant, Zapflow undergoes an assessment every six months, and a re-certification every three years, both of which are conducted by a reputable third-party.

Zapflow is pursuing certification in the Data Privacy, Data Protection and IT Security mandates of the EU GDPR Certification to ensure its data handing practices are fully compilant with GDPR regulations.

ISO 27001 CERTIFICATION EUROPE™

GDPR

SECURITY

Secure Software Development

Standard best-practices are used throughout our software development cycle from design to implementation, testing, and then to deployment. All code is checked into a permanent version-controlled repository, access to which requires strong credentials and Two-Factor Authentication (2FA). Source code changes are always subject to Senior Engineer peer-review and continuous integration servers run on every code update to test for potential issues. All changes released into production are logged and archived.

Network Isolation

Zapflow's systems supporting testing and development activities are hosted in a separate network from systems supporting Zapflow's production application. Customer data only exists and permitted to exist in Zapflow's production network, its most tightly controlled network. All network access between production hosts is restricted using security groups to only allow authorized services to interact in the production network.

Minimal Access Rights

Zapflow's production servers and data are protected by a small number of our Senior Engineers having direct access, in addition to network isolation and strong authentication mechanisms. Those selected engineers use a combination of strong passwords, passphrase-protected SSH keys, a Virtual Private Network (VPN), and Two-Factor Authentication (2FA) before accessing production systems.

SECURITY

Independent Audits

At least once a year Zapflow undergoes a comprehensive third-party security assessment. The auditor performs a full range of hostile investigative activities including, but not limited to, infrastructure scans, vulnerability checks against the latest CVE (Common Vulnerabilities and Exposures) records and penetration tests.

Internal Audits

At least once a year Zapflow's CISO performs their own security audit covering not just the technical infrastructure but also the digital office services that Zapflow employees use. For the Zapflow platform, they use the leading Open Web Application Security Project (OWASP) Testing Guide methodology, among other cybersecurity standards, for guiding their security audit. Quarterly, CISO performs a 'controls and configuration' check to ensure that Zapflow employees are abiding by up-to-date preventative security recommendations.

Employee Equipment Security

A set of policies and procedures have been implemented to address the security of employee computers. We require computers to have strong passwords, full disk encryption and automatic lock when absent. Every Zapflow employee is provided with a secure password manager account and is required to use it to generate, store, and enter unique and complex passwords which helps avoid password reuse, phishing, and other behaviours that reduce security.

Continuing Education

Effective security often starts at the human-level, so Zapflow's employees are required to understand and follow internal policies and standards. This is enforced by our employees attending a compulsory security training every quarter, emphasizing their duties and personal obligations to the securing of our customers' data. In addition, our CISO carefully curates a weekly newsletter with the most notable stories from the Information Security industry, allowing even our non-technical team members to stay abreast of important events.

DATA STORAGE & RETENTION

At Zapflow, protecting our customers' data is amongst our highest priorities. We abide by industry-standard best practices to ensure the data we are entrusted with is kept confidential, pure and highly available

Data At Rest

Data at rest is encrypted with the industry-standard encryption scheme of 256-bit Advanced Encryption Standard (AES-256).

Data In Transit

Data in transit between client and server is protected by HTTP Strict Transport Security (HSTS) via Transport Layer Security (TLS) provided by HTTPS.

Backups & Monitoring

Application data is regularly backed up to geographically redundant data centers, ensuring our services remain operational or recoverable, if necessary. Our servers are spread across multiple availability zones in Ireland.

Zapflow uses a combination of third-party services and our cloud provider's integrated monitoring to gain insight into the integrity of our customers' data. This involves monitoring our databases, application, and error reporting on a real-time basis.

Accessibility

Zapflow aims to reinforce the reality that your data belongs to you. This means that if you wish to leave the Zapflow ecosystem we provide functionality for exporting your data. Our export feature allows you to generate .csv or Excel spreadsheets containing all your data in a coherent and structured format.
Customers on Enterprise edition are provided with secure REST API access which enables them to perform more complex actions for interacting with the data in their account. These interactions can involve both pulling data from or pushing data to the Zapflow application.

Employee Access

No customer data persists on Zapflow employees' devices. All access to systems and customer data is limited to those employees with a specific business need and predefined level of seniority. A best effort is made to troubleshoot issues without accessing customer data; however, if such access is necessary, all actions taken by the authorized employee are logged. Upon termination of work at Zapflow, all employee access is immediately revoked.

Data Retention

By default, Zapflow will retain your data for as long as your account is open. In the case of account closure, your data is held for 30 days before being automatically cycled out of our databases and backups. We retain your data for this allotted period to avoid issues with inadvertent account issues, closures, or terminations. We also allow for the possibility that our customers may request that their data are deleted upon account closure, in which case our technical team will ensure all traces of your data is removed with immediate effect.

COMPLIANCE

Effective use of Zapflow's functionality necessitates the storing of personal information which is subject to various laws and regulations. Staying compliant with these requirements is an ongoing process requiring transparency on the part of both the providers and consumers.

Personally Identifiable Information (PII) or Personal Data

Zapflow users collect and store Personal Data relevant to their venture opportunities in their Zapflow account. The application provides the capability to store typical identifying information like names and means of contact, which can qualify as PII or Personal Data. Zapflow users can also request the creation of custom fields from the Zapflow technical team; each of these added fields are reviewed on a case-by-case basis and are private to the requesting customer by default.

Zapflow as a company also stores Personal Data about its users, both prospective (as part of the sales process) and established (to enable logging in and further communication with Zapflow). We track various structured interactions within the Zapflow application to inform potential improvements. Zapflow does not collect restricted identifying information like Social Security Numbers (SSNs) and Personal Identity Codes (PINs), or other special categories of data. Zapflow strives to comply with national and international regulations pertaining to a person's rights and ownership over their own data. Consequently, Zapflow respects our customers' right to their privacy and ownership of their data. As per our Terms of Service, Privacy Policy, and internal policies, Zapflow provides customers with the ability to request, amend or delete their Personal Data.

COMPLIANCE

GDPR Compliance

As a GDPR compliant data processor Zapflow abides by the regulation's security measures to ensure your data remains both safe and under your direction. To codify this commitment, our customers can read our Data Processing Addendum which directly addresses the GDPR requirements on our website. The main databases of our customers are held in Dublin, Ireland, and any non-EU sub-processors we utilize must demonstrate adherence to the strict data transfer requirements imposed by the GDPR. All of Zapflow's own data handling practices are described in detail in our Privacy Policy.

Zapflow's CISO has received a certification as a GDPR Compliant Data Protection Officer to oversee the company's internal processes through a data protection program and to act as a liaison in interactions with data subjects and authorities.

AUTHENTICATION

Authentication is a key point of concern given that its proper handling is crucial for most security measures. Zapflow provides several mechanisms for users to securely access to their accounts.

Login Options

Zapflow acknowledges that their customers have diverse needs and requirements concerning internal policies, processes, and the sensitivity of their account's data. To account for this variation, Zapflow provides several options for user authentication ranging from the traditional password-based login to SAML-based Single Sign-On (SSO).

Password Authentication

Using a password is the default option to get Zapflow's users started quickly but we highly recommend leveraging extended protections like our provided Two-Factor Authentication (2FA) capabilities. In any case, relying on a password to protect a user's account depends on the complexity of the chosen password. To assist with meeting current recommendations for a strong password, Zapflow uses a set of rules that are checked against the proposed password at the point of set-up. These rules enforce a minimum password length and the addition of character cases and special characters. Thereafter, all credentials stored by Zapflow are encrypted with 256-bit Advanced Encryption Standard (AES-256).

AUTHENTICATION

Two-Factor Authentication

To further protect your account, Zapflow recommends using the 2FA feature which is included as a feature in our plans. When enabled, login attempts will prompt the user to enter a random numeric code generated by a paired 2FA device such as Microsoft Authenticator or Authy (available, among other 2FA solutions, as mobile applications from the Google Play and App Stores).

Single Sign-On

Zapflow provides Single Sign-On (SSO) capabilities for larger teams under the Enterprise edition, thereby reducing the friction of managing multiple accounts across many applications. To assist with onboarding teams with many members, Zapflow integrates with Microsoft's SAML 2.0 SSO mechanism enabling customers who elsewhere use Microsoft products to login to Zapflow with their existing Microsoft account credentials. In line with the extensive and dedicated support promised by the Enterprise edition, Zapflow's technical team will assist with configuring this integration.

ACCESS CONTROLS

Zapflow provides various privacy mechanisms to ensure that your data is managed by and accessible in the ways that you determine to be appropriate.

Role-Based Privileges

The ability to personally limit certain application features and actions upon your data ensures that each member of your team can interact with what is sufficient and necessary to their workflow. To enable this level of control, Zapflow makes use of role-based privileges that allow you to grant access permissions on a modular basis. The flexibility and granularity of control that you have over your team members as an administrator is dependent on the pricing tier that you are subscribed to.

Per-User Data Visibility

Zapflow provides the capability to toggle the visibility of certain sets of data on a per-user basis. This is an implicit security mechanism designed to allow our customers to maintain selective confidentiality on data of their choosing. This fine-grained control over the information visible in your environment allows you to ensure that each user is seeing exactly what they need to see. Whilst this feature arises from security considerations, this conscious design choice is an excellent demonstration of Zapflow's commitment to streamlining the investment professionals' workflow: professionals are afforded with the data they need, identified at your discretion, and no more.

ACCESS CONTROLS

Front office edition

The Front office edition does not include role-based privileges functionality by definition: as the sole user you have full access to the application's modules and your data.

Enterprise

The Enterprise edition includes role-based privileges, teams-based authorization, guest user access and read-only access. Enterprise tier also allows for managing read/write permissions for teams and individual users on a field-by-field basis. This fine level of control over every datum is ideal for teams with the most demanding compliance requirements.

AUDIT CAPABILITIES

A full record of your both incoming and outgoing data, as well as your users' operations, is sure to encourage your users adhere to proper practices and principles concerning data usage. A well-kept and clear automatic record enables you to identify where and why errors may have occurred in cases of issues.

Extensive Logging

Zapflow takes care to maintain an automatic record of all the actions that have occurred within your account. These are always ready to be accessed and cover a range of expected interactions which are essential to have recorded for compliance reasons.

Access Log

A history of login attempts is available for identifying anomalies and being the first point of investigation in the case of an incident.

Export Tracking

You can view all export actions taken on your account's data.

Email Communications

If you have chosen to connect and synchronize your email account with Zapflow, you can view the full chain of communication between yourself and the opportunity's representative in that entity's dedicated page. Emails can be correlated with a given entity, a Deal, for example, through the presence of easily configurable metadata in the email's addressing fields.

'Write' Trail

You can view the history of all modifications or insertions (with any single modifying action known as a 'write') to any entity's data from the point of creation under the 'History' section of that entity's dedicated page.

zapflow