identifee

SECURITY & COMPLIANCE

Identifee is a cloud-based software platform that relies on state-of-the-art technologies for maximum security and availability.

January 2022

Table of Contents

identifee

Technologies

Cloud Infrastructure

Identifee's production systems are hosted by **Amazon Web Services** whose multi-layered approach to securing their cloud services and infrastructure meets the strictest industry standards.

Identifee's backups are hosted within **Amazon Web Services (AWS) Elastic Compute Cloud (EC2) and Simple Storage Service (S3)**. It consists of a multi-tier, virtualized architecture comprised of Linux-based application and database servers, storage and content delivery systems, server and application monitoring and logging tools. Our cloud infrastructure providers maintain recognized security certifications and abide by key compliance frameworks including but not limited to:

- **ISO 9001, ISO 27001, ISO 27017, ISO 27018**
- **SOC1, SOC2, SOC3**
- **PCI-DSS**
- **Privacy Shield**

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

Security

Preventive Security

Deployment Checklist

Identifee has adopted the OWASP Secure Coding Practices Checklist as a part of the development process. Identifee has also prepared a Privacy by Design checklist that product managers and engineers follow to design and build features in a secure and compliant manner. Teams complete this checklist to ensure that proper controls are in place for any project that they are working on.

Incident Response

Identifee has documented detailed procedures for handling any security incidents that might arise. Execution of and compliance with these procedures is regularly practiced with scenarios and exercises run by external security experts on a quarterly basis. This ensures that Identifee is prepared to promptly address all types of incidents by mitigating their impact, investigating the causes and applying corrective measures to prevent similar cases in the future.

Data Storage & Retention

Encryption

Data at Rest

Data at rest is encrypted with 256-bit Advanced Encryption Standard (AES-256) at the application and database level.

Data in Transit

Identifee uses HTTP Strict Transport Security (HSTS) to protect data in transit via Transport Layer Security (TLS 1.2) provided by HTTPS. Identifee plans to move to TLS 1.3 in the near future.

Backups & Monitoring

Application data is continuously backed up to geographically redundant data centers, ensuring that our services remain available or are easily recoverable if necessary. Our servers are spread across multiple availability zones located in the United States and Germany. Identifee maintains its own continuous monitoring services in order to ensure control and availability of customer data, including:

- **Database monitoring**
- **Application monitoring**
- **Error reporting and monitoring**

Data Storage & Retention

Accessibility

Identifee's product and processes are designed with the mindset that your data belongs to you. If you ever choose to move to another platform, we will not hold your data hostage. Our convenient export features allow you to generate and download .CSV files or Excel spreadsheets of your deals, people, organizations, activities, notes and products, as necessary.

Identifee provides secure API access to all customers regardless of the chosen plan. This means that you are free to use the extensive set of endpoints for more complex actions on your data or to extract any and all data elements in your account.

Data Retention

Clear data retention rules are an essential part of minimizing the risk of sensitive data being compromised. By default, Identifee will keep your data as long as your account is open and for 6 months after it is closed. After that, the data will automatically cycle out of our daily backups within 3 months. Identifee has established configurable baseline data retention rules. These rules will be configured for you upon implementation. As an exception, if you would like us to permanently delete any data in your account, our customer support engineers will do this for you promptly with our purpose-built internal tools. All data retention events are logged.

Compliance

Personally Identifiable Information

Identifee users store Personally Identifiable Information that is relevant to their sales process in our CRM application. The application has a certain amount of default fields like name, email address, phone number and address, which qualify as PII or Personal Data. Users can also create custom fields to save other necessary information. Identifee also stores PII or Personal Data about its users, such as your name and email address to enable logging in and communication with Identifee. We also keep various metrics on product and website usage to facilitate improvements. We do not collect health data or other special categories of personal data. Identifee always seeks to comply with regulatory requirements or precedent pertaining to a person's rights and ownership over their own data. Moreover, we firmly respect privacy and your ownership of your data. Therefore, per our Terms of Service, Privacy Policy and internal policies, Identifee provides data subjects with the ability to request, rectify, or delete their personal information.

Authentication

Login Options

Password

Authentication using only a password is the default option to help you get started quickly. It is important to understand that in this case your account's security depends largely on the complexity of your password. Due to this, we have set 8 characters as the minimum for any passwords used to access Identifee accounts. Also, we display a simple password strength indicator to give users immediate feedback when they are setting up their password and suggest ways to improve password security. Any and all credentials stored by Identifee are encrypted with 256-bit Advanced Encryption Standard (AES256).

Two-factor Authentication

To further protect your account, we recommend using the two-factor authentication feature, which is available under all our plans. When enabled, logging into Identifee will prompt an email to be sent to the email address you use to log into Identifee, with a verification link that will allow you access to your Identifee account. Identifee has chosen email-based two-factor authentication because it has been proven to be more secure than SMS-based systems. That same email will provide you with information about where that verifiable login occurred in the world.

Single Sign-On

To help you save on-boarding time and overhead, we have developed a SAML 2.0 protocol based Single Sign-On — or "SSO " in Identifee.

Access Controls

Visibility Groups

Limiting users' access to various information serves a dual purpose of ensuring confidentiality where needed and decluttering the user interface so users can conveniently see just the information that is relevant for them. To help you achieve this, Identifee offers a feature called 'visibility groups' that provides you with control over what data is visible to particular users. The level of flexibility you have with your visibility groups is dependent on which subscription plan your company account is using in Identifee.

Permission Sets

When managing a team, there will be occasions when you will want certain users to not perform certain tasks, to reduce the chance of mistakes or duplication of a user's workload. To allow you to categorize your users and dictate what actions they will be allowed access to, Identifee offers Permission Sets. This way you have total control over what actions users can perform with the data and which features they can use.

Audit Capabilities

Comprehensive and Easy-to-Read Logs

Full History of Contacts and Deals

To see the full history of a contact or a deal from the point of creation, you simply navigate to the relevant details page where all the interactions are provided in a convenient feed.

User Actions Log

The users' statistics pages have a tab that shows you the recent actions of that specific user within your Identifee account. This page is available to Administration Users by default, however access can be shared further to regular users.

Export Log

Identifee logs all exports of data from your account. Administration Users can export the contents of your account into convenient .csv or .xls files and may also delegate certain exporting rights to other users. Copies of the export files are kept for 2 weeks so you can check which data was exported.

Access Log

A history of logins with relevant device data is available to customers on the Settings page in Identifee to identify any anomalies and to serve as the starting point for any investigations if an incident occurs.

Audit Capabilities

Security Event Log

Identifee logs over 50 types of authentication, permissions, visibility, export and user management events. Administration Users can review on the Settings page.

Security Assessment

Administration Users have access to a summary assessment of security-related aspects of the account such as user password strength, adoption of security-enhancing features, and a reminder of permissions that have been granted.

Data Retention Logs

Identifee logs all data retention events that occur based upon the data retention rules that have been established for your account. Administration Users can review these logs on the Settings page.