Data and Security

Mopinion is committed to providing its customers with the data and security assurance they need to be confident in doing business with us. Our compliance with the ISO 27001 standard perfectly validates this commitment to our customers, while simultaneously providing transparency around data security processes.

ISO 27001 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System (ISMS) which defines how we perpetually manage security in a holistic, comprehensive manner. This widely-recognised international security standard specifies entities:

– Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities

– Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks

– Adopt an overarching management process to ensure that the information security controls meet our information security needs on an ongoing basis

Conformity with this internationally recognised standard lies at the core of Mopinion's approach to implement as well as manage information security. This achievement proves the completeness and accuracy of security controls, while simultaneously providing customers increased assurance.

The Mopinion ISO 27001 certification can be downloaded here.

Web Application Hosting

At Mopinion, we embrace a **multi-cloud strategy** to give our customers choice, performance and peace of mind. Whether you prefer a global cloud provider or a European alternative, our platform ensures that all data is stored securely within the European Union. This approach allows us to meet the highest standards for scalability, reliability and compliance with EU data protection laws.

Your cloud options:

Amazon Web Services

Mopinion utilizes Amazon Web Services (AWS) to provide customers with a highly available and scalable feedback solution. The collaboration enables us to offer a secure, fast, and reliable infrastructure, ensuring the best possible experience on our platform. Data is stored within European AWS datacenters by default.

Scaleway

Mopinion partners with French cloud provider, Scaleway, to offer a solution that is fully hosted in Europe by a European company. This ensures our customers benefit from a secure, sovereign infrastructure that complies with existing and envisioned EU data regulations.

With Scaleway, we provide a fast, reliable and privacy-conscious platform experience for organisations that prioritise data residency and digital independence within the EU.

"Security, performance and flexibility are core to our user feedback solutions. We embrace a multi-cloud strategy by working with both AWS and Scaleway, ensuring all customer data remains in Europe and fully complies with EU regulations."

Floris Snuif – CTO, Mopinion

The AWS ISO 27001 certification can be downloaded here.
The Scaleway ISO 27001 certification can be downloaded here.

For both AWS and Scaleway a SOC2 Type 2 attestation report can be requested from respective parties. Due to confidentiality agreements, we are not at liberty to share these directly.

Data storage

Mopinion's customer data is stored within the European Union by default. Depending on your region, alternatives can be discussed for enterprise customers. Mopinion's data policy complies with GDPR (General Data Protection Regulation) and adheres to the European Union's standard for privacy and data protection, known as SCC (Standard Contractual Clauses). Mopinion customers retain full ownership of their data. For more details on SCC (Standard Contractual Clauses), click here.

Data

Which information is collected?

Mopinion collects user data when a user (such as a website visitor) participates in one of our surveys. This may occur, for instance, when a user submits feedback through a Mopinion feedback form or takes part in an exit survey on a website or inside a mobile app. Mopinion will store the information provided by the user, such as feedback ratings, satisfaction scores and open comments.

The specific data collected depends entirely on what the feedback form's owner seeks to learn from their visitors and customers. Additionally, we collect certain metadata, including the URL where the survey was submitted, the user's browser or operating system, and the date and time of the submission.

How is the information used?

The information collected is accessible only to Mopinion customers who have logged into their dedicated Mopinion account. None of the collected data is publicly available. All information within a Mopinion account can be exported to file formats such as Microsoft Excel and CSV, or via API connections and native integrations with third-party tools (when set up by the customer). It is the responsibility of the Mopinion account holder to manage these exports securely once the data is exported from our infrastructure.

How are user accounts protected?

Mopinion user accounts are secured by a user-created password, and reasonable precautions are taken to ensure the privacy of your account information. Additionally, we offer optional security for personal accounts via Single Sign-On (SSO) and Multi-Factor Authentication (MFA). It is the responsibility of the Mopinion account holder to keep their password confidential and to change it periodically.

Mopinion implements reasonable measures to protect the information stored in our databases, including encrypting Personal Identifiable Information (PII) collected from survey respondents. Access to this information is limited to employees who require it to perform their job duties, such as technical staff. Additionally, all data transactions between Mopinion users and the Mopinion infrastructure are encrypted using SSL technology.

Non-Personal Information and Aggregated Data

Mopinion may share non-personal, aggregated data with third parties. For example, Mopinion may share an aggregated overview of the number of feedback items or number of feedback buttons being displayed to business partners. Because this form of data does not identify particular users, these third parties will not be able to contact you (or your customers) solely based on this data. The information that we collect may be used in aggregate form in various ways to optimise and improve Mopinion's services. We will not identify particular users while collecting and aggregating this information. We may use this information for website management, administration and security, promotional activities, and research and analysis.

What measures do we provide to store and remove privacy sensitive data?

Data privacy and security is of the utmost importance to Mopinion and our clients, therefore measures can be taken to ensure that sensitive data remains confidential when survey respondents are submitting their feedback.

The following functionality is available within the Mopinion products:

- Survey respondent contact information, such as a name or email address (PII), is stored encrypted in our databases.
- Survey respondent IP addresses are not stored.
- We offer functionality to automatically delete contact information (PII) after a specified number of days in accordance with GDPR requirements.
- For more details on GDPR compliance, please refer to our privacy policies.

How do we report and monitor security related issues?

While we take extensive measures to protect your information, we cannot guarantee absolute security. Factors such as unauthorized access, hardware or software failures, and other unforeseen events may compromise the security of your data. In the event of a security issue, incidents will be reported according to

the Service Level Agreement (SLA) that is in place with the customer. Examples of potential incidents that we report on are:

- Unauthorized modifications to source code, databases, servers, middleware, or network components.
- Failures in continuity, backup, and recovery processes due to economic or political instability, or natural disasters.
- Unauthorized connections to API's.
- Corporate information leaks.

We utilise Security Information and Event Management (SIEM) tools for continuous monitoring and alerting.

Malware protection software is included in our standard build and is updated automatically. We have an organisation-wide patch management process that covers obtaining, validating, testing, deploying, and reporting updates. This process includes a policy for handling exceptions.

Our change management process is standardised across the organisation, with required scripts and tests. The incident management process is also standardised, using templates for collection and analysis. We have a comprehensive data breach procedure in place. All security related processes and procedures are part of our Information Security Management System (ISMS) according to our ISO 27001 certification and are available on request.

How is access and security management organised?

Environment Separation
Development, testing, acceptance and production environments are distinct. Processes are automated, and documentation is kept current.

Access Control
Users with privileged, admin, or super-user rights undergo background checks. Automated user provisioning and access management are in place, with manual access logging and review. Strong authentication is required for all privileged users.
The Privacy Officer manages security and access. Regular (external / third party) audits and reviews are conducted to ensure compliance with ISO 27001.

Electronic Communications

An internal acceptable use policy is published and communicated to all staff. Messaging systems are configured to baseline standards, and only corporate messaging products are permitted, with non-corporate options blocked. Cryptographic keys are centrally managed, and an inventory of solutions is maintained according to the latest ISO 27001 standards.

External Suppliers
Contracts (and SLAs where applicable) with all external suppliers are regularly reviewed, and suppliers must comply with baseline security arrangements. Mopinion utilises leading cloud providers such as Amazon Web Services (AWS) and Digital Ocean, both ISO-certified cloud providers.

Cryptographic key rotation
Automated cryptographic key rotation is a critical security measure that ensures the continuous protection of sensitive data by periodically updating the cryptographic keys used to access systems like databases or encrypt private data. Powered by AWS, this process leverages AWS Key Management Service (KMS), which automates the generation, rotation, and management of cryptographic keys. AWS KMS allows for seamless, secure, and automated key rotation without disrupting ongoing operations or requiring manual intervention.
By regularly rotating keys, we mitigate the risk of key compromise and limit the exposure of encrypted data. Additionally, AWS KMS ensures that rotated keys are securely archived and managed according to industry best practices, providing robust protection for our SaaS product's data infrastructure. This automated approach not only enhances security but also ensures compliance with regulatory requirements, maintaining the integrity and confidentiality of sensitive information.

Security Audits and Backups
Security audits cover business applications, security controls, and the information security function. An organisation-wide Business Continuity Plan (BCP) and Disaster Recovery (DR) plan are in place, with identified triggers for activation.

Development Practices
Development is guided by security and risk considerations, including architecture. Agile development with Scrum methodology ensures rapid, high-quality feature development. Continuous feedback from end users is used to refine designs and improve future work.

General Information

Stack

At Mopinion, we leverage a modern and robust technology stack to deliver high-quality solutions. Our architecture is built around a comprehensive API ecosystem supported by diverse code repositories. We ensure rigorous security standards with ISO 27001 certification and compliance with GDPR regulations.

Storage technologies:
For storage, we utilise a range of technologies including Redis, MySQL, MongoDB, InfluxDB, SQS, and AWS S3, providing flexible and scalable data management.

Backend:
Our backend is powered by multiple languages and frameworks, such as Python, PHP, Node.js, and Go, enabling us to handle various use cases efficiently.

Frontend:
On the frontend, we employ React (JS) to build dynamic and responsive user interfaces. For mobile development, we provide native SDKs in Swift and Kotlin, along with cross-platform solutions like React Native, Cordova, Flutter, and Ionic Capacitor to maximise reach and performance.

Cloud deployment:
Mopinion utilises a suite of deployment and orchestration tools, including Jenkins, Kubernetes, GitHub Actions, and Docker, to streamline our CI/CD processes and maintain a robust development pipeline. This diverse and sophisticated stack allows us to innovate rapidly while maintaining high standards of performance and security.

Performance

We strive to provide our customers with 99.5% server availability, covering both the Mopinion application and data access. To ensure optimal performance, we collaborate with several partners, including Pingdom, Sentry, and Amazon Web Services, among others, to monitor and maintain system efficiency.

SSL

As a software company compliant with EU GDPR regulations, we prioritize the security of our web services by ensuring that all are protected with SSL (Secure

Socket Layer) encryption. By law, GDPR requires platforms like Mopinion to operate exclusively with SSL to safeguard user data during transmission.

SSL encryption plays a critical role in securing our software environment by establishing an encrypted connection between the user's browser and our servers, preventing unauthorized access to sensitive information. Both the Mopinion user environment, accessible via app.mopinion.com, and customized customer portals, such as 'customername'.mopinion.com, are SSL-certified (https), ensuring secure and trusted interactions across our platform.

Backups

In line with our policies under our ISMS and ISO 27001 certification, we ensure the protection and integrity of customer data through a robust backup strategy. For critical systems and servers, data is mirrored across multiple Availability Zones or maintained in a load-balanced setup to guarantee redundancy.

Periodic backups of all production system data are conducted using snapshots, with databases on AWS backed up and duplicated at a data center in a different physical location from our production data storage. These backups are regularly checked as part of our daily operations, including routine data restoration attempts. All backups are retained for a period of at least 7 days, ensuring prompt data recovery when needed while adhering to our data retention policy.

Vulnerability

To ensure the security and integrity of our systems, Mopinion collaborates with third-party partners to conduct thorough vulnerability testing. In addition to this, we also perform internal vulnerability research regularly, both manually and through automated processes.

Mopinion works closely with an external agency, SecWatch, which is the designated partner for conducting structured penetration tests and vulnerability scans periodically. The professionals working at Secwatch are Certified Ethical Hackers (CEH) and licensed as Security Analyst & Licensed Penetration Tester (ECSA/LPT) and Offensive Security Certified Professional (OSCP) amongst other specialised certifications for security testing (i.e. Owasp / GWAPT, GPEN, CISM, CIPM and CIPP/E).

Additionally, enterprise-licensed customers may conduct their own security audits, provided this is stipulated in their contractual agreement.

For those planning to perform security research, we recommend contacting Mopinion in advance to discuss research methods and scope. We can offer guidance on the best practices and areas for testing to ensure that our production environments remain unaffected. Mopinion maintains an isolated and mirrored environment specifically for such testing purposes, ensuring that our live systems remain secure and stable.

For more details on our penetration testing and security audit policies, please refer to the legal section on our website or contact us at support@mopinion.com.