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: 2017 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.
The AWS ISO 27001 certification can be downloaded here.

Web Application Hosting

Amazon Web Services

Mopinion partnered with AWS Amazon EC2 for highly available and scalable web hosting. This way we can offer you a secure, fast and reliable infrastructure that will give you the best experience on our platform.

"Choosing to work with Amazon Web Services as our cloud partner was never a difficult decision. For our leading feedback analytics platform, security, performance and flexibility are key to delivering a great user experience. This matches the vision and services of AWS"

Floris Snuif – CTO

Storage

Your data is stored in Ireland. For enterprise customers, depending on your region, we also offer storage in the US and China. Mopinion's data policy is aligned with the European Union standard of privacy and data protection known as the US-EU Data Protection Privacy Shield. Our customers have complete ownership of the data. For more information on the EU-U.S. Privacy Shield please click here.

Data

Which information is collected?

Mopinion collects user data when a user / visitor participates in one of our surveys. This can be for example when a user shares a review with a Mopinion feedback form or participates in an exit survey on the website. We will store the input given by the user (e.g. feedback rating, open comment). The type of information stored solely depends on what the "owner" of the feedback form wants to know from his / her visitors and customers.

How is the information used?

The information collected is only available to users with access to their Mopinion account with their username and password. None of the information collected is available publicly. All information within the Mopinion account is exportable to a Microsoft Excel format. It is the responsibility of the Mopinion account holder to handle these exports with care.

How is information protected?

Mopinion accounts are secured by a user created password, in which case reasonable precautions are taken to ensure that your account information is kept private. The Mopinion account holder is responsible for keeping this password confidential and changing the password periodically. Mopinion uses reasonable measures to protect the information stored within our databases, and we restrict access to such information to those employees who need access to perform their job functions, such as our project managers and technical staff. All data transactions between the Mopinion users and the Mopinion infrastructure will be encrypted by 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 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 take to block privacy sensitive data?

Privacy is of the utmost importance to Mopinion and our clients, therefore measures can be taken to ensure that website visitors' sensitive data remains confidential when sharing their feedback. The following options are available within the Mopinion tool:

– Exclude IP-addresses from being logged

– Disable storage of users' contact information (e.g. hashed email address)

All actions taken in the list above have an impact on the implementation process.

How do we report and monitor security related issues?

Despite all our efforts as stated above, please note that we cannot ensure or guarantee the security of your information. Unauthorised data entry, hardware or software failure, and other factors may compromise the security of your information at any time. Security issues of the following kind will be reported immediately:

1. Mutations of unauthorised source code, databases and data, servers, middleware and network components

2. Continuity and backup and recovery fails – Issues caused by economical / political instability, or natural disasters

3. Unauthorised connections

4. Corporate information leaks

On a monthly basis, Mopinion reports who has access to crucial parts of the Mopinion platform and IT infrastructure. Mopinion has deployed tools such as Security Information and Event Management (SIEM) for continuous monitoring and alerting. We do manual reviews of event logs.

Malware protection software is implemented as part of standard build and is automatically updated. An organisation-wide patch management process is published, which includes obtaining, validating, testing, deploying and reporting. An exception policy is also in place. Our Change management process is distributed across the organisation, with mandatory scripts and tests. Our Incident management process is distributed across the organisation. Standard templates for collection / analysis are used. First responders identified and trained; experts (eg forensics) identified and contracts are in place. An organisation-wide breach notification process is in place. For more information about Mopinion's procedure for reporting and handling data breaches please visit this document.

How is access and security management organised?

Development and testing are separated from production and operation responsibilities. We apply separate development, test and production environments. Processes are automated and documentation up-to-date. Users with privileged, admin or super-user rights have been screened / undergone background checks. Our DPO is responsible for security and access management. Mopinion works according to the agile principles of the Secure Development Lifecycle.

Mopinion uses automated user provisioning and access rights management; manual access logging and review. Baseline security requirements are included in all contracts; standards may be referenced. All privileged users use strong authentication; manual access logging and review.

Regular audit and review. In terms of the protection of electronic communications and the use of cryptographic solutions: An acceptable use policy is published internally and all staff made aware. Messaging clients and servers are configured using a baseline standard. Only corporate messaging products are allowed; others are blocked (e.g. webmail). An inventory of solutions is maintained; copies of cryptographic keys held centrally. Contracts (or SLA) are in place with all external suppliers. All external suppliers can demonstrate compliance with the common baseline arrangements and provide regular evaluation. Additional information security arrangements are adopted based on changes in risk and business impact.

Mopinion works with internationally recognised and leading cloud provider AWS. All providers have SLAs in place and are ISO certified. All suppliers are audited on a regular basis.

Mopinion follows a security audit process, covering business applications, security controls and the information security function. Information risk analysis is used to identify audit targets. Backup systems such as Grandfather-Father-Son (GFS) are implemented for all systems. An organisation-wide BCP / DR plan has been published; triggers for implementation are identified.

Development is shaped by security and risk considerations (including architecture); feedback is used to improve and refine designs and future work. Our SaaS and security development is based on agile development with the scrum methodology. This enables the organisation to rapidly develop features in relatively short time frames at a high level of quality. We continuously develop based on short feedback loops from the end user.

General Information

Stack

Mopinion works with a Linux operating system and an Apache web server. The site data is stored in a MySQL and MongoDB databases, and dynamic content is processed by PHP, Python.

Performance

We do our utmost to deliver our customers a 99.5% server availability. This includes the Mopinion application and unlocking data. To make sure everything runs smoothly we work with several partners to keep track of performance:

- Pingdom
- Zabbix
- Amazon Web Services

Monitoring

In addition to our own set of tools Mopinion teamed up with a 3rd party monitoring service provider. This way our servers and overall performance of the platform is being monitored 24/7. In case of any incidents – depending on your license – we can act immediately and minimise potential risks for our customers.

SSL

By law regulation (GDPR) platforms such as Mopinion only work with Secure Socket Layers. The Mopinion user environment app.mopinion.com and 'customername'.mopinion.com are both certified with SSL(https).

Backups

Mopinion runs mirrored database backups to prevent customers from data loss. Daily full backups are stored for 7 days. Backups are stored for a period of one month.

Vulnerability

Mopinion works with 3rd party partners to test system vulnerability and safety. SecWatch is assigned as a Mopinion partner to run structural pen tests. Also, enterprise customers are allowed to run their own security audits. Please contact support@mopinion.com for more information about pen tests and audits.