
# MOPINION

## DATA & SECURITY

Dear Mopinion user,

Thank you for choosing Mopinion as your feedback analytics partner for web and mobile. You are joined by leading companies such as TomTom, Ahold, Decathlon, which are all using the Mopinion platform for their global online feedback programmes.

In this document we've included more information about our data and security policy. At Mopinion we do our utmost to offer you a great user experience and make sure that data is stored in a safe environment.

If you have any questions regarding our data and security policy, feel free to contact us at support@mopinion.com.

Kind regards,

**Udesh Jadnanansing**
MD/ Co-Founder

# 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.

**Floris Snuif** - **CTO**: *" 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"*

## Security

One of the reasons Mopinion works with Amazon Web Services is that we can rely on the AWS security posture to boost our own security. AWS is internationally-recognised by ISO 21001 standards. 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 AWS perpetually manages 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

The AWS ISO 27001 certification can be downloaded here.

## 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 Privacy Shield please visit: https://www.export.gov/article?id=Privacy-Shield-Safe-Harbor

# Data

## What 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 the information is 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 used. First responders identified and trained; experts (eg forensics) identified and contracts in place. Organisation-wide breach notification process is in place. For more information about Mopinion's procedure for reporting and handling data breaches please visit: https://app.mopinion.com/assets/support/PDF/procedure-for-data-breach.pdf

## 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 CTO 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.

# Enterprise Service Level Agreement

For our Enterprise users we offer the following SLA Agreements based on urgency and impact. Depending on your license, we agree on specific support levels.

| Urgency | Description |
|---|---|
| High | Service is interrupted or not stable, users can not use the services undisturbed and there is (potential) loss of data. |
| Middle | Services are less stable. Work-around, temporary solution or adjustment needed to make work possible, minimal or no data loss. |
| Low | Customer organisation & relationships can continue working, no data loss |

| Impact | Description |
|---|---|
| High | There is a loss of production and/or becomes critical to the business process and/or disturbance affects more than 75% of the users. |
| Middle | There is imminent loss of production and/or the disturbance affects 25% to 75% of the users. |
| Low | There is no loss of production and/or the disturbance affects one or more users. |

Based on urgency and impact we have defined different priority levels:

| Priority List | Impact High | Impact Middle | Impact Low |
|---|---|---|---|
| Urgency High | PRIO 1 | PRIO 2 | PRIO 3 |
| Urgency Middle | PRIO 2 | PRIO 3 | PRIO 4 |
| Urgency Low | PRIO 3 | PRIO 4 | PRIO 4 |

The priority levels determine the time of response:

| Priority | Maximum time of response | Norm time to solution | Solution in % per year | Remaining solution guaranteed in |
|---|---|---|---|---|
| 1 | 2 hours | 1 work day | 95% | Remaining max. 5% till 2 days |
| 2 | 3 hours | 2 work day | 90% | Remaining max.10% till 10 days |
| 3 | 2 workdays | 10 workdays | 80% | Remaining max.20% till 15 days |
| 4 | 5 workdays | 20 workdays | 60% | Max.20% within six months and last max.20% within one year |

Availability by phone Service desk / 1st line support:

| Day | Opening Hours for Support | Contact Information |
|---|---|---|
| Workdays (Monday – Friday) | 08.30 am - 08.00 pm CET | +31 (0) 10 820 0075 |
| Weekends | Inapplicable, escalations through support | Support@mopinion.com |
| Holidays | Inapplicable, escalations through support | Support@mopinion.com |

Performance Indicator:

| Performance Indicator | Availability |
|---|---|
| Availability Mopinion environment | 99.5% |
| Availability front-end application & module | 99.5% |
| Maximum Downtime | 3 hours per quarter |
| Maximum # of Failures | 1 time per month with an interval of at least one week |

| Activity | Client | Mopinion | Description |
|---|---|---|---|
| Incident report and/or issue and/or modification request e/o problem (further notice) | RE | RE | Client can report at all times.<br>Since the ICT (components) are being monitored notification dual Accountability and Performance |
| Accept, register and prioritise | | RE | Mopinion records every report regardless of communication or timing |
| Rate on priority and classifying for initial support | | RE | Rating of priority and equipped with proper classification and priority. Reporter receives feedback with reference. |
| Matching | | RE | Making sure it's a Known Error and whether there is a Workaround |
| Analyse and diagnose | I | RE | Determining if the incident should be resolved in the 2nd line and whether it should be exalted to a problem (in relation to other customers of Mopinion) and/or dispatched. Client can have an active role in supplying information requested by Mopinion. |
| Dispatching / Perseverance | | RE | If necessary, push to external solution-organisations (hosting provider / software vendor (s) etc.) |
| Resolve and Repair | I | RE | Notification will be resolved in consultation with the detector.<br>Customer could have an active role in resolving the notification. |
| Shutting down | | RE | Shutting down and informing detector. Reporting for next session. |

I = Informative
E = Executive
R = Responsible

# 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:


## Monitoring
Next 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 the 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.