Factbird Data and Application Security FAQ

This document serves as an overview of data security and how Factbird processes and stores data. Factbird is more than happy to answer any additional questions.

Email: support@factbird.com

Table of Contents

1 General Information

1.1 Company name:

Factbird ApS

1.2 Company country:

Denmark

1.3 Physical address of the company:

Nyropsgade 37, 3rd Floor, 1602 Copenhagen V, Denmark

1.4 What type of cloud does Factbird use?

A.1 Factbird uses a public cloud hosted by AWS (Amazon Web Services), which may or may not be restricted to the individual customer. In all cases, however, data are strictly restricted to each customer. For large installations we also offer user-owned AWS cloud.

1.5 What type of Cloud Computing model is the solution based on?

A.1 Software-as-a-Service (SaaS).

1.6 Is Factbird sensor data transmitted on the customer's own network?

A.1 Factbird data may either be transmitted on the customer's own network, on a separate dedicated cellular Wi-Fi hotspot, or by using the built-in cellular network in the Factbird hardware.

1.7 Are any external audit reports available?

A.1 Yes. Please contact *support@factbird.com* if you want to see it or are interested in doing an audit yourself.

2 Security policies and procedures

2.1 Does your organization have documented and approved information security and privacy policies and standards that describes the security controls for the information systems and the rules of behaviour for individuals accessing the information systems.

A.1 Yes, documents are in place, and employee contracts contain clear rules regarding confidentiality and related financial penalties for the individual.

2.2 Does your organization have a risk management program that identifies, manages, and tracks information security risks?

A.1 Yes, it is reviewed as a fixed agenda item on the Board of Directors meeting (minimum quarterly meetings)

2.3 Does your organization have a vulnerability management program that identifies, manages and tracks vulnerabilities in IT systems?

A.1 Yes, issues are logged and followed up in our management system.

2.4 Does your organization have a security assessment program to assess implemented security controls and evaluate and improve, where necessary, the effectiveness of security controls and safeguards?

A.1 We are utilising both AWS provided tools, and another tool provided by an external US based company, to continuously evaluate our security posture.

3 Human resources

3.1 Are employees, contractors, 3rd parties, and temporary employees made aware of the security risks associated with their activities and the applicable security standards and required to sign a non-disclosure agreement and abide by the organization's security and privacy policies.

A.1 Yes. We have no external software contractors, own employees are trained during on-boarding.

3.2 Is there a formal disciplinary process in place for employees, contractors, 3rd parties or temporary employees who have violated organizational policies and procedures?

A.1 Yes. Penalties are embedded in employee contracts.

3.3 Are employees, contractors, 3rd parties, and temporary employees responsible for handling sensitive information, manage critical systems, applications or networks, subject to background checks and vetting prior to engagement or provision of these responsibilities.

A.1 Yes. We verify their educational documentation. The type of information we are handling is not high-risk data.

3.4 Are procedures in place to ensure the timely removal of access rights and the return of assets when employees, contractors, 3rd parties and temporary employees change job responsibilities or leave the organization?

A.1 Yes, we have a check-out form, signed by the employee leaving – The process is supported by our legal responsible.

4 Data center security

4.1 Are all production and test computer/server equipment located in the data center(s)?

A.1 All servers are cloud based and hosted by AWS.

4.2 Is there a backup power supply and Uninterruptible Power Supply (UPS)?

A.1 AWS has best in class redundancies in place, to ensure uptime.

4.3 Are the data center(s) subject to any independent third party security audits, assessments, or certifications (e.g. SSAE 16, SOC2, ISO 27001, BS25999)?
If yes, please list the relevant certification and audit reports

A.1 Yes, please see https://aws.amazon.com/compliance/programs/

4.4 Does the data center(s) fulfill the requirements for a Tier IV data center according to the Uptime Institute classification (i.e. a fully fault tolerant data center).

A.1 AWS has chosen not to have a certified uptime institute base tiering level. We refer to the statement from Amazon:"AWS operates our data centers in alignment with the Tier III+ guidelines, but we have chosen not to have a certified Uptime Institute based tiering level so that we have more flexibility to expand and improve performance. AWS' approach to infrastructure performance acknowledges the Uptime Institute's Tiering guidelines and applies them to our global data center infrastructure design to ensure the highest level of performance and availability for our customers. AWS then improves on the guidelines provided by the Uptime Institute to scale for global operations and produce an operating outcome for availability and performance that far exceeds that which would be achieved through the Uptime Institute tiering guidelines alone. Although we do not claim alignment with Tier 4, we can ensure that our systems have a fault tolerant sequence of operations with self-correcting mitigations in place."
https://aws.amazon.com/compliance/uptimeinstitute/

5 Network and operational security

5.1 Is there a formal operational change management process to ensure that all hardware or software changes or updates are tested, evaluated and authorized before being implemented?

A.1 To reduce the number of bugs and issues in the production environment, we implement the following practices:

- Pull request reviews: All changes and developments are reviewed by at least one developer.
- Automated tests are executed on every code change
- Staging environment: Before deployment, all changes are tested and verified on a staging environment, simulating the conditions on a production environment.
- Blue-Green UI deployment: This technique maintains two identical environments – one of which is idle, and the other live. New features are deployed to the idle environment, where final verifications and testing takes place. If all is confirmed, the idle environment will be switched to the live environment. Should problems occur, a switch back is possible.

5.2 Are security measures in place to limit the risk of unauthorized access. Such measures may include but is not limited to network firewalls, application firewalls, intrusion detection or prevention systems (IDS/IPS) and network segmentation.

A.1 Yes

- Factbird's security is built around AWS IAM with the principle of least-privilege in mind.
    - Factbird employees' AWS user accounts only have the privileges that are required for them to do their work.
    - The external Factbird application can only be accessed by being an authenticated user.
    - Internal Factbird services are made up of a series of independent services, that each do a sub-set of the whole Factbird feature-set. Each service is given IAM permissions on a least-privilege basis, so that it only has the minimum permissions needed to function.
    - AWS IAM policies are created via infrastructure-as-code and are reviewed as part of code review.
- Automatic audit scans of code dependencies are in place to limit risk of malicious code.

- Server patching & physical security is handled by AWS. For details, please see With AWS focusing on patching servers, and physical server security, we can focus on application security.

5.3 Are security measures in place to limit the risk of malicious code e.g. using anti-virus software and malware protection?
A.1 Yes. See above answer.

5.4 Are there procedures in place to ensure that security updates (patches) to operating systems, databases, applications and other software are assessed and implemented in a timely manner.
A.1 Yes, AWS is providing maintenance of the infrastructure services we are using to run Factbird.

5.5 Do IT systems generate audit logs to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized, or inappropriate activities?
A.1 Yes, we have relevant logging/audit trail of strategic events in the Factbird system e.g. who is changing system settings, monitoring of system load, etc.

5.6 Are IT systems and log files actively monitored for signs of unlawful, unauthorized or inappropriate activity?
A.1 Yes, automatic alerts are sent to developers if flagged activity occurs.

5.7 Are all data communication (except for publicly available web pages) between users and IT systems or between different IT systems transmitted over public networks protected from unauthorized interception or tampering (e.g. through the use of SSL/TLS or other industry acceptable methods)?
A.1 Yes, we are transmitting from devices with MQTT over TLS. In the cloud database environment, the communication is handled by AWS. All data from AWS to the user are transferred over TLS. For details, please see https://aws.amazon.com/security/

5.8 Is user data in IT systems in the data centre encrypted?
A.1 Yes, managed by AWS.

5.9 Are all data media (including removable media, hard disks and backup tapes) sanitized or destroyed before disposal or release for reuse to prevent data from being retrieved from discarded equipment or data media?
A.1 Employee computers/phones and removable media are wiped in accordance with our company security policies.
A.2 All data are stored in AWS, a cloud environment.

5.10 How and which security measures have been built into your API's
A.1 We use OAuth and API keys to handle permissions for API access to third parties.
A.2 MQTT security is based on certificates.
A.3 Third parties are given API access based on API keys.

6 Access control

6.1 Does the application enforce of a strong password policy:
- Minimum length of 8 characters
- Contain 3 of 4 levels of complexity (upper case, lower case, numeric, special character)
- Initial or reset password must be changed immediately upon the next successful logon

A.1 Yes, we use AWS Cognito which allows us to configure requirements individual for each customer.

6.2 Does the application provide support for ADFS?
A.1 Yes.

6.3 Does the system support multi-factor authentication (e.g. password + token or SMS code)
A.1 Yes. If using our AD integration the Active Directory can be configured with multi factor authentication.

6.4 Are all passwords transmitted over a network encrypted using SSL/TLS or other industry acceptable methods?
A.1 Yes, all passwords and user access is handled with AWS Cognito. For details, please see https://aws.amazon.com/cognito/
A.2 Transport to and from AWS's network is encrypted.

6.5 Are all passwords stored on the system encrypted using a non-reversible encryption algorithm (e.g. secure password hash)?
A.1 Yes.

6.6 Can the application be set to automatically log a user off the application after a predefined period of inactivity?
A.1 Yes, it can be setup as a company requirement, but cannot be individualised for the user, it is either all or nothing.

6.7 Is the logon mechanism protected from brute force password guessing (e.g. through account lock out, timeout between logins, captcha or similar)?
A.1 Yes.

6.8 Can the application be set to lock out an account after a number of failed logon attempts?
A.1 Yes.

6.9 Are system administrators and other personnel with privileged user rights working for the Supplier required to use two factor authentication and VPN or similar when connecting to systems remotely for maintenance and support purposes.
A.1 Yes.

7 Incident management

7.1 Does a formal information security incident response and escalation procedure exist that is reviewed, maintained and documented?

A.1 Yes, incidents are logged in our management system and there are quarterly reviews by the Board Of Directors.

7.2 Does a reporting procedure exist to ensure that the customer is notified without undue delay in situations, where the confidentiality, integrity or availability of data may be or have been adversely affected?

A.1 Yes, and we have established a method to rapidly push information to all relevant users.

8 Backup, business continuity and disaster recovery

8.1 Are systems and procedures in place to minimize disruption due to data loss or system failure (e.g. backup and restore systems and procedures and/or data duplication and automatic failover)?

A.1 Yes, Factbird performs daily automatic backups of all production data using AWS. For details, please see: https://aws.amazon.com/dynamodb/backup-restore/

8.2 Are back-up media stored at a secure off-site location?

A.1 Yes, AWS uses best-in-class standards for data security and platform redundancy. For details, please see above link.

8.3 Are all backup media that may contain customer data encrypted?

A.1 Yes, all data stored is encrypted, all of which is handled by AWS. For details, please see: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/EncryptionAtRest.html

8.4 Is there a business continuity and disaster recovery plan in case of a major disaster?

A.1 Yes, due to the cloud-based nature of AWS and the Factbird application, multiple redundancies are in place in the event of a major disaster. For details, please see https://aws.amazon.com/disaster-recovery/

8.5 Have the business continuity and disaster recovery plans been evaluated and tested within the last 12 months?

A.1 Yes, we have recovered based on raw data, and please see the answer to 8.4.

8.6 Do you have an alternative data centre that would house customer data and services in the event of a crisis? If yes, please identify the location and party that operates the facility.

A.1 Yes, please see the answer to 8.4.

9 Third party security

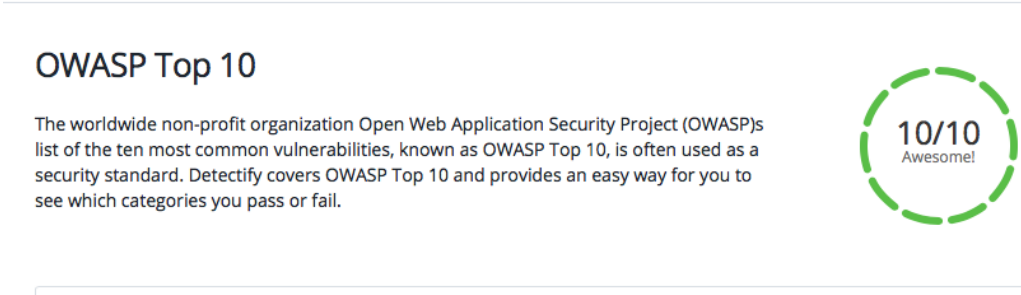
9.1 Do you ensure that third-party providers and sub-contractors used by you to deliver services to the customer employ adequate security measures to protect information, applications, and/or services (e.g through audits, assessments and contractual requirements)?

A.1 We are using two service providers:
AWS - Data services are provided by AWS, they are leaders in cloud computing services and comply with the highest industry standards.

10 Assurance

10.1 Is your organisation subject to any independent third party security audits, assessments or certifications (e.g. SSAE 16, SOC2, ISO 27001)?
A.1 No

10.2 Are systems and applications subject to regular vulnerability / penetration tests performed by independent third parties?
A.1 Yes. Factbird uses Detectify to perform such tests on a weekly basis. The system scan s for 500+ known attacks, and is constantly adding more. We are automatically notified about potential vulnerabilities. For details, please see: https://detectify.com/
Our current OWASP Top 10 score is 10/10 on our main site cloud.factbird.com according to Detectify:



10.3 Will your organisation on request provide the customer with sufficient information to enable the customer to ensure that the appropriate technical and organizational security measures have been implemented (e.g. in the form of descriptions and documentation of security measures, and/or third-party certifications or audit reports)?
A.1 Yes.

10.4 Is it possible for the customer at its own cost to appoint an expert to perform and audit of your data processing facilities, and documentation to ensure that appropriate technical and organizational security measures have been implemented (The expert shall treat all information obtained or received from the Supplier confidentially, and may only pass on its conclusions to the customer)?
A.1 Yes, please contact support@factbird.com

10.5 Is it possible to export/download all customer data in a readable format on a regular basis to ensure availability of data, if the system/service becomes unavailable for whatever reason (Data Escrow)?
A.1 Yes.

10.6 Is Factbird compliant with the EU General Data Protection Regulations (GDPR)?
A.1 Overview: Factbird does not store sensitive personal data. However, Factbird does store personal data in the form of e-mail, names, subscriptions and accesses, as well as what may be left by users in plain text fields. These data are handled with the utmost care, and never distributed to third parties.Breach Notifications: In the unlikely event of a data breach, customers and relevant authorities will be notified.
A.2 Right to Access: Upon request, a data subject may be given full insights into, what their data is used for in addition to a copy of the data.

A.3 Right to be Forgotten: Upon request, a data subject may have their personal data deleted from the Factbird system.
A.4 Data Portability: Upon request, a data subject may receive an electronic copy of their data in a common electronic format.
A.5 Privacy by Design: Factbird restricts access to personal information to those who require access for business-critical processing. Factbird does not process or store data not pertinent to the customer's business needs.
A.6 Data Protection Officers: Factbird has appointed Nicole Sowe, Emendo Consulting, Denmark, as it's Data Protection Officer.