ActivityInfo

Data Security at ActivityInfo

Last updated February 24th, 2024.

Introduction

This document provides a high-level overview of our policies and strategies at BeDataDriven B.V. for protecting Customer Data. Our company is exclusively focused on ActivityInfo, a data management platform focused on the Social Sector, which includes the United Nations, NGOs, and Government actors in humanitarian relief, international development assistance, health care, conservation and climate justice, and other social purposes.

Our certification and a full list of controls we implement is available from our Trust Center.

Our information security management system

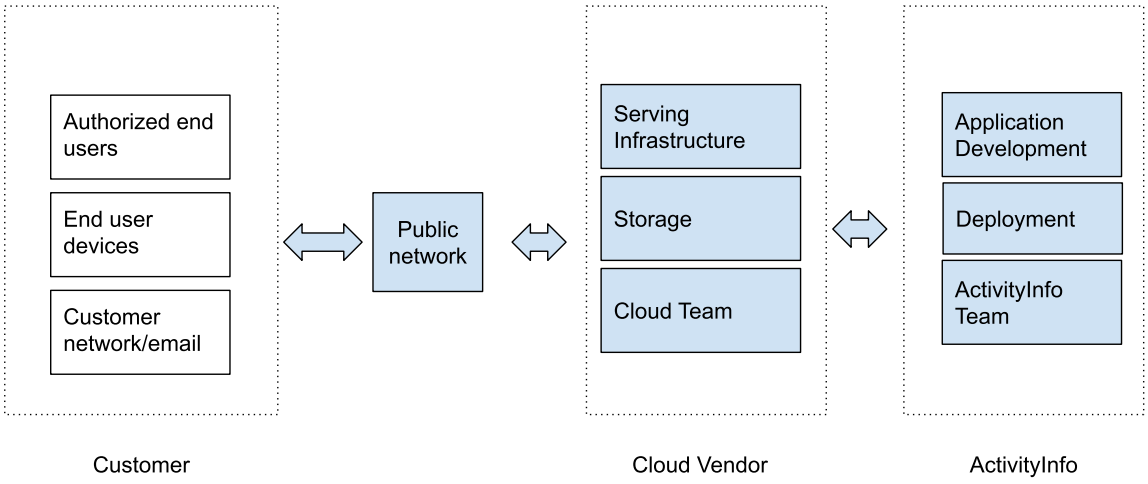
Information security management (ISM) describes controls that we implement to ensure that we sensibly protect the confidentiality, availability, and integrity of assets from threats and vulnerabilities.

The ISO/IEC 27001 standard provides the key principles around which we have designed our Information Security Management System (ISMS) for protecting both our own information and the information entrusted to us by our customers in our platform. Our ISMS is certified as ISO-27001 compliant and regularly subject to external audits.

A strong ISMS is dynamic, rather than static, revised constantly as new risks are identified and mitigated. At BeDataDriven, we follow a Plan-Do-Check-Act cycle that includes the following process:

Plan: Threat modeling and risk assessment

The starting point of our risk assessment is a thorough Threat Model (pictured below) that helps enumerate vulnerabilities and their associated risks.



Threat model

We complement the threat model with a malicious actor profiling exercise in which we seek to enumerate the motivations and capabilities of those who would seek to undermine either our customers or our customers.

Risks are then assessed in terms of their likelihood and potential impact to obtain a final risk score and tracked in our risk register.

Do: Process and feature development

For risks that are too high to be accepted, we develop a risk treatment plan to mitigate the likelihood and impact.

Policies include ensuring that our own staff use only devices which benefit from full-disk encryption, in order to mitigate the risk posed by lost or stolen devices, and are required to use two-factor authentication.

This might include features, such as upcoming improvements to session management, or to internal policies, such as projects underway to move as much of our team as possible away from Ubuntu and Windows to managed ChromeOS devices.

Check and act: Security review

We employ a number of tools and processes to review the mitigations we put into place and ensure that they have desired effect.

These include both automated tools and external reviews, such as:

Regular penetration tests, carried out by external firms

- Internal and external audits of our ISMS
- Google Cloud Security Command Center, which provides an audit of our platform configuration
- Google Web Security Scanner, which automatically scans for a number of known web application vulnerabilities,
- Qualys SSL Labs, which assesses the security of our encryption-in-transit
- Snyk.iol, which checks our application's dependencies for vulnerabilities (CVEs) in our application's dependencies and alerts us to new threats.
- Vanta, an automated compliance management system

We also speak regularly with our customer's information security focal points to update our malicious actor profiling. We have worked closely with our customers in refugee response, for example, to monitor the rise of state-sponsored cyber attacks, and update our threat model accordingly.

Infrastructure strategy

As a matter of strategy, we have chosen to outsource management of networks, servers, software, and all other relevant information technology components to the maximum degree possible. This allows the ActivityInfo team to focus on developing and securing the application layer, and mitigate a wide array of risks by contracting global leaders in computing such as the Google Cloud Platform.

For example, we have a blanket policy against running even virtual machines where our team would be responsible for applying operating system patches. Instead, we deploy our software using the Google AppEngine Platform Service as Platform (PaaS) where the operating system and other infrastructure is entirely managed by GCP.

Policies and procedures

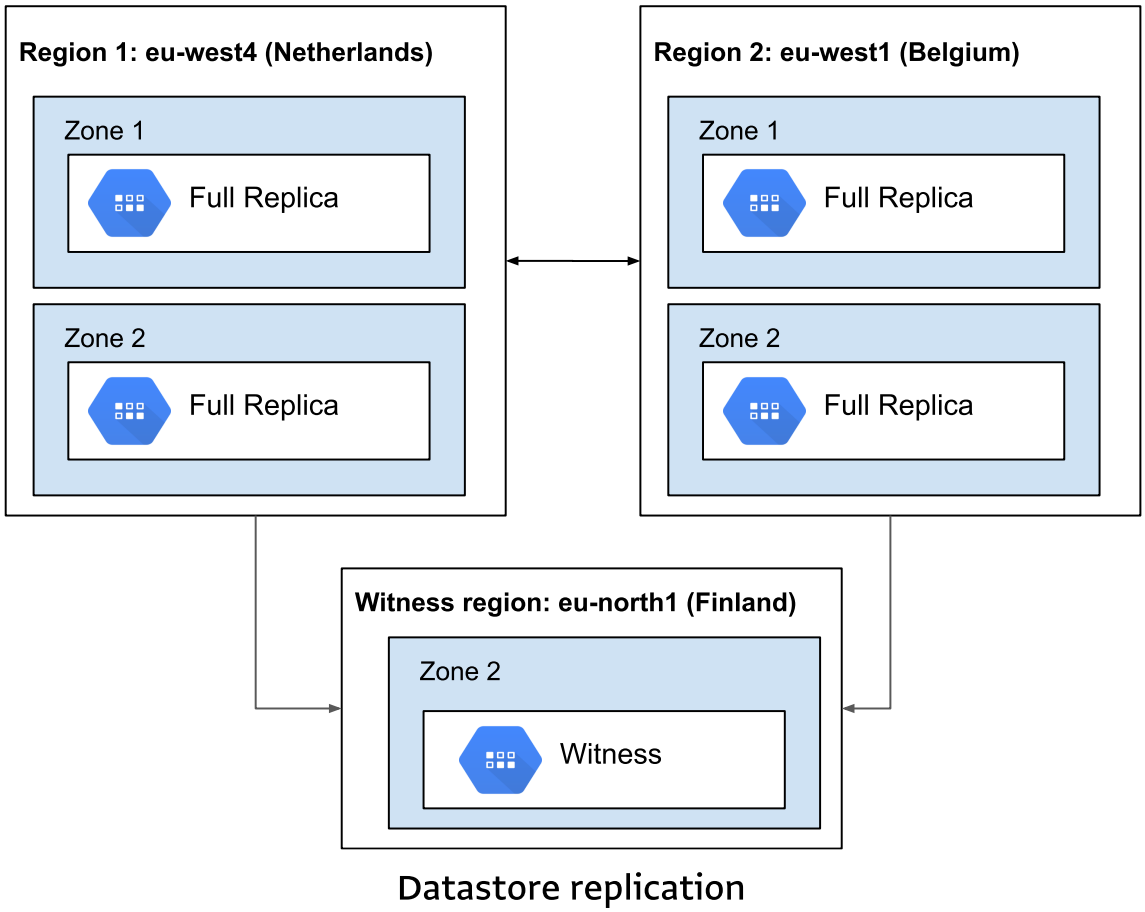
Our Information Security Management System (ISMS) includes a number of ISO-27001 compliant policies that help our company protect our company, and our customer's data. The following are summaries of some of these policies. Full policies are available upon request.

Information Security Management (ISMS) Policy

This policy provides a framework to be applied when establishing, implementing, maintaining, and continually improving the information security management system ("ISMS"), as defined in 01-ISMS Scope of the ISMS, in accordance with the requirements of the ISO/IEC 27001 ("ISO 27001") standard.

Business Continuity and Disaster Recovery Plan

We consider any level of data loss to be unacceptable and have designed our platform accordingly. When a customer sends an update to the ActivityInfo platform, it is fully replicated across at least two “zones” in each of two different data centers, separated by at least 100km. A third geographic data center serves as a “witness” node in the event that communication between two of the data centers would fail.



Datastore replication

This ensures that in the event of hardware failure, or natural disaster, that failover is automatic and instant.

A full edit history is also stored within the replicated database to ensure that the data is safe from inadvertent errors on the part of users, or the actions of malicious actors within our customer’s organizations.

This allows Database Owners to restore versions from any previous point in time.

Data Management Policy

Our Data Management Policy ensures that information is classified, protected, retained and securely disposed of in accordance with its importance to the organization and to our customers.

Our Policy defines four levels of classification. The highest designation is “Protected” and includes any data stored by our customers in the ActivityInfo platform. Access to Protected Data by our team is strictly controlled and only granted on a temporary basis to key staff members for the purpose of resolving issues that cannot otherwise be resolved.

All records stored in an ActivityInfo Database, and their full history, is retained until either our contract with the customer ends, or the Database Owner deletes the database.

Once an ActivityInfo database has been deleted, we retain copies of the data for at least an additional 60 days, unless deletion is explicitly requested earlier by the customer. This provides time for customers to correct inadvertent deletion or to realize that required data has been deleted.

Incident Response Plan

This document establishes the plan for managing information security incidents and events, and offers guidance for employees or incident responders who believe they have discovered, or are responding to, a security incident.

Third-Party Management Policy

This policy ensures protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external

parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

See our list of third-party processors for details.

Human Resource Security Policy

This policy ensures that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.

All new employees undergo a background check as well as a competence assessment to ensure they are suited to the role.

We provide security awareness training to all staff members no less than once a quarter, where we cover social engineering awareness and review relevant policies. All new employees receive this training immediately.

Compliance with national and regional privacy regulations

Our product, ActivityInfo, is used by organizations working in more than seventy countries, often to store personal information about their beneficiaries. Many of these countries have passed national regional privacy legislation, ranging from the EU General Data Protection Regulation (GDPR) to the Philippines Data Privacy Act, to Law 2157 in Colombia.

Under the terms of the GDPR and similar national regulation, BeDataDriven has responsibilities as both a Data Processor and a Data Controller.

When our customers collect personal data that falls within the remit of privacy legislation, they act as a Data Controller for the purposes of the legislation.

When our customers use our software to collect, store, and analyze Personal Data, we act as a Data Processor under the GDPR, and sign a separate Data

Processing Agreement (DPA) with our customers.

As a Data Processor, we have a number of obligations with which we work to comply. These include, but are not limited to,

- We only process personal data stored in ActivityInfo on the instructions of our customers, the Data Controller.
- We obtain permission, through the Data Processing Agreement, for all subprocessors and assume full liability for failures of subcontractors to meet the requirements of GDPR.
- We delete or return all personal data to our customers at the end of the service contract.
- We take all reasonable steps to secure data, including encryption, stability and uptime, backup and disaster recovery, and regular security testing.
- We undertake to notify our customers without undue delay should we learn of a data breach.

We also have a role as a Data Controller under the EU GDPR, as we collect a limited amount of personal data about our customers themselves in order to operate our business. This includes only the full name and email addresses of our customers and the users they invite to use the platform. We retain and store this information on the basis that is necessary for the performance of our contract to which the users are party. More information is available in our privacy policy.

Individual information rights

In most cases, we ourselves do not collect data on individuals, but support our customers in respecting the rights of the individual data subjects.

With regard to the limited personal data we collect about our own customers, we have procedures in place for Data Subject Requests (DSR) to ensure that

individuals can exercise their right to access, rectification, erasure, to restrict processing, data portability, and to object.

Designing for security

A significant source of risk to data entrusted to our platform lies on the customer side. Such risks range from user error, to insider attacks, to insecure customer networks and devices.

We have designed the ActivityInfo software with functionality intended to help customers reduce these risks. Such features include the following:

Highly-granular permissions

Customer-designated administrators can set highly-granular permissions for the data they store in ActivityInfo by defining their own roles, and apply record-level permissions where needed.

Permissions for the following operations can be assigned per folder, form or subform:

- View form and records
- Add new records to a form
- Edit existing records
- Delete records
- Export records
- Manage users
- Manage reference data
- Lock records
- Add forms or folders
- Edit forms or folders

- Delete forms or folders

Role-based access

The Database Owner can also define one or more roles that include a set of permissions logically grouped. A user can then be granted that role for one or more folders or forms.

For more information, read Understanding roles in our documentation.

Record-level permissions

A particularly powerful feature of ActivityInfo's User Access Model is the ability to grant record level permissions with a user-defined condition. For example, if the customer defines data collection forms with a "Partner" or "Province" field, then users can be granted view or edit permissions only for records that meet a specific condition, such as "When Partner is NRC" or "Province is North Kivu or Province is South Kivu."

Audit log

ActivityInfo's audit log retains a log of all changes made to the database, the identity of the user making the change, and specifically what was changed. This allows administrators to easily revert deleted folders, forms, or records arising from user error or insider attacks. With the help of support staff, a database or form can be rolled back to any point in time.

The Audit log is retained until the database is deleted.

Single Sign On

ActivityInfo integrates with Azure Active Directory (AAD), Google Workspace and Okta for authentication. Where possible, we require users to exclusively authenticate through their organization's identity provider, ensuring that

organization-level 2FA requirements are enforced for accessing ActivityInfo, and that users lose access to ActivityInfo when they leave the organization.

Support access

None of our team members have “superuser access” to customer data. Designated support staff can only access a customer’s database with their permission and are then granted access to the database just as any other user would be. Their actions are logged and transparent to the data owners.

ActivityInfo team security

The following section provides an overview of the measures we have put into place within our team to mitigate vulnerabilities related to our role as developers, managers and administrators of the software.

Social Engineering training

All staff members' devices are required to have adequate Anti-Virus and Anti-Malware protection. Ingoing and outgoing email is automatically scanned for viruses. Our team is subject to a monthly Phishing simulation to test the effectiveness of our training program and identify staff members who require additional training.

Anti-Virus, Anti-Malware, and Anti-Spyware

All staff members' devices are required to have adequate Anti-Virus and Anti-Malware protection. Ingoing and outgoing email is automatically scanned for viruses.

Intrusion Detection

BeDataDriven staff uses Google Workspace for identity management, email and document management. Google Workspace provides advanced analytics to detect anomalous activity by staff members.

For our platform, we use the Google Cloud Security Command Center, and in particular the Event Threat Detection service, which automatically scans various types of logs for suspicious activity in our infrastructure. Using industry-leading threat intelligence, we can quickly detect high-risk and costly threats such as malware, cryptomining, unauthorized access to Google Cloud resources, outgoing DDoS attacks, and brute-force SSH.

Vulnerability scans of workstations and servers

We use the Google Cloud Security Command Center to regularly scan all servers and other cloud-based resources for vulnerabilities. Built-in security analytics and threat intelligence assesses the overall security state and activity of our virtual machines, network, and storage buckets and surfaces vulnerabilities in your applications. These insights help us take proactive measures to reduce our exposure to risks.

We do not manage our own servers.

Encryption

All customer data managed with our platform is encrypted both in transit and at rest.

All traffic between our users and the platform is encrypted using TLS1.2 or above. After assessing the impact on our users, we recently disabled TLS1.0 and TLS1.1 out of an abundance of caution.

We use the Google Cloud Datastore and Google Cloud Storage for storing customer data on our platform. Both products encrypt stored data at rest.

ActivityInfo.org is served with HTTP Strict Transport Security (HSTS) and is loaded into the preload list used by most browsers. This ensures that users with modern browsers cannot establish an encrypted connection to activityinfo.org, even on first access. This protects users in the very specific case of accessing ActivityInfo.org for the first time on an unsecure or attacker controlled network.

Physical security measures

All customer data is stored in Google's world-class data centers, which are protected with several layers of security to prevent any unauthorized access to customer data. Google uses secure perimeter defense systems, comprehensive camera coverage, biometric authentication, and a 24/7 guard staff.

We also take the physical security of our own team's assets seriously. All staff member devices are required to use full-disk encryption to mitigate the risks associated with lost or stolen data devices. We ensure that no devices are left unsecured in our own office in the Hague.

Role-based access controls

In addition to the role-based access controls we provide to our customers in the platform, we control access to our internal resources using similar role-based controls.

Each member of our team is granted access to key resources through membership of specific roles, such as "Developer," "Tester," or "Support agent."

Systems monitoring

We exercise centralized monitoring of all our systems using the Google Cloud monitoring suite, and have many alerts in place for conditions which require action on the part of our staff.

We also use an external third-party tool, Statuspal.io, to measure and alert on general availability of our platform, which is available on our public status page.

Wireless network security

Our office wireless network is secured using WPA2, and more broadly by employing a “Zero Trust” or “Perimeterless” approach to security.

Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Backing up personal data

We apply the same rigorous method of backup for all data, regardless of the type of data. Data stored with our platform is backed up across at least four full replicas.

Transferring data and records

We do not transfer data or records outside of our primary data store. Customer data is replicated across at least four separate data center zones across two data centers.

Authorized users are able to export data from the platform, if they have the appropriate permissions. Exports are served across an encrypted connection.

Questions? Contact us