Panalyt

Panalyt Data Security Policy

1. Policy brief & purpose

Our Company Data Security Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

2. Scope

This policy refers to all parties (employees, customers, job candidates, etc.) who provide any amount of information to us.

3. Who is covered under the Data Security Policy?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

4. Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only Processed by the company within its legal and moral boundaries
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

5. Actions

To exercise data protection we're committed to:

5.1 Restrict and monitor access to sensitive data
5.1.1 All client data must only be stored on **Panalyt Google Cloud Platform** data storages (e.g. Cloud SQL, BigQuery, Datastore, Cloud Storage) with access rights being modified on approval by the Panalyt Data Security Officer.
5.1.2 All Panalyt Google Cloud Platform resources must have (a) access logs enabled and (b) file download functionality disabled, with an exception only to be made in case of a data audit requested by the client in writing, and approved by the Panalyt Data Security Officer.
5.1.3 Only members of the Panalyt engineering and data team have access to client data stored on the Panalyt Google Cloud Platform instance .
5.1.4 Access rights on either addition/ termination of a new employee must be approved by the Panalyt Data Security Officer.
5.1.5 Other Panalyt team members have access to client data via the Panalyt application, governed by the application's security processes.
5.1.6 Access rights to the client data via the Panalyt application is managed by the client's Panalyt administrator who is responsible for granting/changing the default access rights, as defined in Panalyt's Terms.
5.1.7. All audit logs for access to the client's data on the Panalyt Google Cloud Platform instance and the Panalyt application are reviewed on a monthly basis by the Panalyt Data Security Officer.
5.1.8. All users of the system that handles information client's data on the Panalyt Google Cloud Platform instance and the Panalyt application are provided with a unique ID as well as the minimum access rights and operation rights.

5.2 Develop transparent data collection procedures
5.2.1 All client flat files and API keys must be stored on the Panalyt Google Cloud Platform Instance.
5.2.2 All automated scripts should be run on the Panalyt Google Cloud Platform instance and should never include the API key directly.

5.3 Train employees in online privacy and security measures

5.3.1 All employees to undergo basic information security training during onboarding as conducted by the Panalyt Data Security Officer.

5.4 Build secure networks to protect online data from cyberattacks

5.4.1 All files, scripts and databases are only to be stored on the Panalyt Google Cloud Platform instance.
5.4.2 All Panalyt employee terminals should comply with the following security requirements:

- Enable password protection
- Enable 5 minutes screen lockout
- Enable automatic software updates (at least for security patches)
- Enable hardware encryption (e.g. enable FileVault for mac users)
- Install Endpoint verification Chrome extension
- Install an approved antivirus solution

5.4.3 All communication channels used for communicating client's data must be encrypted using standard encryption methods.

5.5 Establish clear procedures for reporting privacy breaches or data misuse

5.5.1 Panalyt employees are encouraged to report any privacy breaches or data misuse internally to the Panalyt Data Security Officer who will take the appropriate disciplinary action.
5.5.2 The Panalyt App Intercom chat widget can be used by clients/ users to directly report any privacy breaches or data misuse discovered externally by the client to the Panalyt Data Security Officer. Alternatively the client can also contact the email contact@panalyt.com
5.5.3 The Panalyt Data Security officer shall conduct a thorough investigation and report their findings and recommendations to the Panalyt CEO within five working days of any reported or suspected breach of confidential data. Any material breach of confidential client data shall be reported to the related client within 48 hours of the report submission.

5.6 Include contract clauses or communicate statements on how we handle data

5.6.1 The data handling policies referred to in this document will be regularly circulated amongst Panalyt employees as reminders and will be explained to new hires as a part of the new hire onboarding process

5.7 Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

5.7.1 All Panalyt employees must follow the data access rules for client data mentioned in 5.1
5.7.2 All Panalyt employees must ensure any files with sensitive data(not necessarily client related) are only shared internally via the Panalyt Google Cloud Platform Instance after password protection
5.7.3 All files containing sensitive data and API tokens from a client should be password protected and loaded directly into the Panalyt Google Cloud Platform Instance and not be sent via email. The Data Team Lead should be responsible for handling this.
5.7.4 In the event that the client requests a data audit, only the Data team is allowed to export the data out of the Panalyt system and store it as a password protected file on the Panalyt Google Cloud Platform Instance. The scripts responsible for doing this should be run on the Panalyt Google Cloud Platform instance. All data must be deleted from the Data team member's machine after the audit is completed using a secure non-recoverable deletion procedure. Also, transfer of client data must be performed through encrypted channels using standard encryption methods.
5.7.5 Any Panalyt employee dealing with sensitive client data should make sure that their screen is not visible to other members of the Panalyt team or any other party and should lock their screen before leaving their laptop unattended. In addition, Panalyt terminal must be configured with an auto screen lock of 5 minutes.

5.7.6 No confidential client data must be printed out or stored in any other medium apart from the data storages on the Panalyt Google Cloud Platform Instance.

5.7.7 All client's data must be encrypted at rest using standard encryption methods.

6. Termination Procedures

In addition, in the event of termination of the employee/contractor relationship, the Data Protection Officer shall:
6.1 Retrieve the laptop (or similar asset)
6.3 Wipe the memory of laptops (and similar assets) using a non-recoverable method.
6.4 Close the relevant access accounts for GSuite (Gsuite SSO covers most tools including Google Cloud Platform), Jira, Github, Last Pass, Wix, CircleCI, MixPanel, Microsoft Teams, Postman, Jupyter, Intercom, Zeppelin, Lingohub, Airtable, Sentry, Salesforce, Currency Layer.
6.5 Close access to Client Keys
6.6 Close access to any Development tools

**Please refer to https://cloud.google.com/big-data/security-governance/ for a more extensive explanation of how Panalyt leverages the Google Cloud Platform to leverage industry best practices for data security*
Our data protection provisions will appear on our website.

7. Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

8. Revision

The Panalyt Data Security Policy is reviewed and updated on a regular basis in line with new loopholes to prevent potential security-related incidents from occurring.

Daniel J West
Founder and CEO
Panalyt

Last update: 2022/05/06