medida.

“Data Privacy, Security, and Storage” Policy 2023

At Medida, we are committed to protecting the privacy of our clients and their data. This data privacy policy explains how we collect, use, and protect the personal and non-personal data that our clients entrust to us.

We are committed to maintaining the highest levels of data security for our clients and implementing appropriate technical measures to protect their data.

Data Definitions

Medida collects 4 types of data, defined with examples below:

	Definition	Examples
Personal Client Information	Personal data about the organizations we serve or their employees	Names and phone numbers of organization employees. Addresses of organizations
Non-personal Client Information	Non-personal data given to us directly by our clients	Data about the way the organization would like to organize their programs. Feedback data about our training program.
Usage Data	Metadata describing the way in which our clients use our platform	Number of logins, time spent in platform, which users performed which actions
Program Data	All the data that our clients store in our platform	Beneficiary demographic and impact data, data on programs such as enrollment and attendance

Data Collection

First and foremost, we will not collect any unnecessary or extraneous information. The minimization of information collected to that which is absolutely necessary for service provision is a central element in our data security risk reduction strategy.

The data we do collect is collected in the following ways:

- Personal and non-personal client data
    - Interviews and meetings we have with our clients
    - Client websites and other public, promotional material
    - Forms our clients fill out as part of the onboarding and training process
- Client usage data
    - Third-party tracking software such as Logrocket as well as our own internal application monitoring
- Program data
    - Collected by the clients themselves and stored in our database

Data Access and Usage

We cannot emphasize enough that the Medida team has access to Client Program data. Every member of the Medida team has signed a non-disclosure agreement prohibiting the sharing or discussing of client data outside of the context of our day to day operations. We will use the data that we collect from our clients solely for the purpose of providing them with the requested services. This may include using the data to:

- Set up and manage their accounts
- Provide training and support
- Analyze and improve our services

As part of our terms of service, the client also allows us to use anonymized data to report on services delivered. For example, we might report on the number of surveys filled out using Medida in a given year as part of our newsletter or promotional materials. However, we will never report on the content of that data or on who created that data unless given explicit permission to do so by the organization. We might ask for said permission if we wanted to use an organization's data for a case study, for example.

We will not share, sell, or otherwise distribute our clients' data to any third parties, except as may be required by law.

Data Storage

We store your data using the following third-party services

- Google Drive (Personal and non-personal client information)
  - https://policies.google.com/privacy
- Medida - our own environment (Personal and non-personal client information)
- Digital Ocean Managed Database (Program data)
  - https://www.digitalocean.com/legal/data-processing-agreement
- Ottomatik Database backup (Program data)
- Logrocket Application Monitoring (Usage data)
  - https://docs.logrocket.com/docs/security

Data Protection

We take the protection of our clients' data seriously and have implemented appropriate physical, electronic, and managerial measures to safeguard and secure the data we collect. The following have been organized by platform-specific and HR-specific safeguards:

Platform-Specific

- Data Encryption: Encrypting data, both at rest and in transit, to protect it from unauthorized access.
- Secure Networks: Using secure networking protocols, such as SSL/TLS, to protect data as it is transmitted between devices.
- Data Back-up and Recovery: Implementing data backup and recovery measures to ensure that our clients' data can be restored in the event of a disaster or data loss.

- Software Updates: Keeping all software and systems up to date with the latest security patches and updates to protect against known vulnerabilities.
- Password Policy: Implementing strong password policies to ensure that our users choose strong, unique passwords.
    - Passwords must be at least 8 characters in length and must contain at least one number, one capital letter, and one lowercase letter.
    - Passwords are encrypted and no one anywhere, including on the Medida staff, will be able to see them.
- Organizations can choose to enforce strict logout mode on certain users, in which those users are logged out automatically after 5 minutes of inactivity. This is useful in cases where the user is dealing with highly sensitive data.
- Users can choose to enable two-factor authentication on their accounts, providing an extra layer of security. We’ll provide training on how to do this.
- Users and Roles: Through the platform’s system of users and roles, organizations can determine who sees what data and with what permissions, ensuring sensitive data is only seen by those you absolutely need to see it.

Medida HR-Specific

- Non-Disclosure Agreements: We require all employees to sign a non-disclosure agreement prohibiting them from sharing any data they may have access to.
- Training: We are developing a comprehensive and mandatory data security and privacy training program. All Medida employees will be required to complete the training and demonstrate the appropriate level of comprehension.
- As a rule, Medida staff will only access specific data when doing so is necessary to assist the client.

In the unlikely event of a data breach, we will do everything possible to:

1. Quickly contain the incident by identifying and isolating the affected systems, and determining the extent of the damage.
2. Identify the cause of the breach and analyze the type and amount of data that has been compromised.
3. Notify affected clients and provide them with information about the incident and what steps they can take to protect themselves.
4. Remediate the issue to prevent similar incidents from happening in the future. This may include updating software and systems, implementing new security measures, and providing additional training for employees.
5. Comply with any regulatory requirements and notification laws applicable to the incident.

Data Retention

If a client decides to stop using Medida, we will explicitly ask them for consent to continue holding on to their data. The benefit to the client is that they will be able to pick up where they left off if they decide to start using Medida again in the future. The client’s data will still be subject to this data policy and any changes to this policy will be explicitly communicated to the client. The client retains the right to ask us to delete their data at any time.

Data Rights

Our clients have the right to access, correct, or request the deletion of their personal data at any time. They can also withdraw their consent for the use of their data at any time.

To exercise any of these rights, clients can contact us at contact@medida.io.

We encourage our clients to extend the same data rights to their beneficiaries, including providing them with the data stored on them upon request and giving them the option to opt out of having their data stored. We also encourage our clients to familiarize themselves with the data laws in the country in which they are operating. For example, EU citizens are afforded certain rights under GDPR.

Data rights and regulations are rapidly changing in this day and age; Medida commits to an intentional and ongoing audit of regulations and best practices so that we operate in accordance with our values as an organization

Contact Us

If you have any questions or concerns about our data privacy policy, you would like to better understand some aspect of our policy, or you think there is something missing from our policy, please do not hesitate to contact us at contact@medida.io.