



# **GLODIGAPP DATA PROTECTION AND PRIVACY POLICY**

## **Introduction**

GLODIGAPP needs to gather and use certain information about individuals accessing the site who opt in to sign in and use services provided by the site or GLODIGAPP LLC.

These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

## **Why this policy exists**

This data protection policy ensures GLODIGAPP:

- Complies with data protection laws and follows good practices
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach


## **Data protection law**

The Fair Information Practice Laws (as developed in the USA by the Department of Health, Education and Welfare) describes how organizations — including GLODIGAPP— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Fair Information Practice Laws underpinned by the following important principles. These say that personal data must:

- For all data collected there should be a stated purpose.
- Information collected from an individual cannot be disclosed to other organizations or individuals unless specifically authorized by law or by consent of the individual
- Records kept on an individual should be accurate and up to date
- There should be mechanisms for individuals to review data about them, to ensure accuracy. This may include periodic reporting
- Data should be deleted when it is no longer needed for the stated purpose
- Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited
-  Some data is too sensitive to be collected

## Policy scope

This policy applies to:

- The head office of GLODIGAPP
- All branches of GLODIGAPP
- All staff and volunteers of GLODIGAPP
- All contractors, suppliers and other people working on behalf of GLODIGAPP

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Fair Information Practice Laws. This can include:

- Names of individuals
- Addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

# Data protection risks

This policy helps to protect GLODIGAPP from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

# Responsibilities

Everyone who works for or with GLODIGAPP has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that GLODIGAPP meets its legal obligations.
- The GLODIGAPP Chief Security Officer is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data GLODIGAPP holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The GLODIGAPP Chief Operating Officer is responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.

- Evaluating any third-party services the company is considering using to store or process data. For instance, Cloud computing services.
- The GLODIGAPP Chief Marketing Officer is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

## General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- GLODIGAPP line managers will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

## Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to GLODIGAPP Chief Security Officer.

GLODIGAPP does not store any paper documents or any physical records.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- GLODIGAPP operates in a digital cloud environment (hereinafter referred to as “Cloud”). It means that no physical servers, storage devices, network or any other hardware will be used to store and process User information. GLODIGAPP employees will use designated Personal Computing devices (PCs, laptops, tablets or mobile devices) to access applications and data stored in the Cloud via secure connections (TLS/SSL over Public Internet or over Private VPNs) with industry-standard Identity and Access Management policies.
- GLODIGAPP contracts and employs established Cloud service providers with verified and audited policies for physical security and shared infrastructure. GLODIGAPP complies with Cloud providers’ “Shared Responsibility Principles” for data and system protection and extends their provisions to its Users and Customers.
- Users of GLODIGAPP applications and web sites may be required to provide personal information for authentication and authorization purposes. Such information will be required in the format of a personal profile. Access to the profile information from External sources (outside of GLODIGAPP) must be protected by Users through creating and maintaining a strong password. Access to the profile information from GLODIGAPP Internal resources will be protected by Authorization and Access Policies governing employee and system access to such information.
- GLODIGAPP implements Role-Based Access Control (RBAC) policies to all its systems and data in the Cloud. User data will be stored in Cloud (virtual) servers and systems without direct (“raw”) access to such systems. Access to such storage systems will be implemented through applications with the applied RBAC policies, preventing external hacking or internal tampering with data and records.
- GLODIGAPP will not require that Users provide or store any critical data. GLODIGAPP does not warrant and does not guarantee that any User data is protected from accidental deletion (“crash”). GLODIGAPP advises that User keep their local copies of all data provided to GLODIGAPP.
- User data will not be saved to any Non-Cloud provider servers or systems.

## Data use

GLODIGAPP will not use User Personal (Profile) information for any purpose other than Authentication, Authorization and/or Personalization of offered services. Specifically, GLODIGAPP will not:

- Sell Profile information to any parties
- Shared Profile information to any parties
- Disclose or make public in any way Profile information

GLODIGAPP reserves the right to aggregate and analyze Profile information for Statistical, Analytical and Research purposes without identifying individuals on which such aggregated information is based.

## Data accuracy

GLODIGAPP is not responsible for data accuracy of User Profile data. GLODIGAPP does not verify or validate data provided by Users for the purpose of Profile creation. Any issues resulting from incorrect or inaccurate User data that prevent execution of GLODIGAPP applications and services must be addressed by Users.

GLODIGAPP provides Users with the technical capabilities to update or completely delete their User Profiles in accordance with principles described above.

## Subject access request

All individuals who are the subject of personal data held by GLODIGAPP are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to GLODIGAPP Chief Security Office.

Individuals will be charged \$10 USD per subject access request. GLODIGAPP will aim to provide the relevant data within 14 days.

GLODIGAPP will verify the identity of anyone making a subject access request before handing over any information. Verification documents include but are not limited to: a valid passport, a valid driver's license or state issued ID card, other.

## Disclosing data for other reasons

In certain circumstances, the User personal data to be disclosed to law enforcement agencies without the consent of the data subject.

GLODIGAPP will disclose requested data upon court subpoena and will notify the User of such disclosure (as applicable by laws of the United States and the State of California).