MangoApps

OFFICE CHAT GDPR GUIDE (BY MANGOAPPS)

MangoApps - 2018

Table of Contents

What is GDPR?

The EU General Data Protection Regulation (“GDPR”) is a new comprehensive data protection law that updates existing EU laws to strengthen the protection of “personal data” (any information relating to an identified or identifiable natural person, so called “data subjects”).

If you are processing personal data in the context of an organization established in the EU, the GDPR will apply to you, regardless of whether you are processing personal data in the EU or not. “Processing” means any operation performed on personal data, such as collection, storage, transfer, dissemination or erasure. If you are not established in the EU, the GDPR applies to you if you are offering goods or services (whether paid or free) to EU data subjects or monitoring the behaviour of EU data subjects within the EU. Monitoring can be anything from putting cookies on a website to tracking the browsing behaviour of data subjects to high tech surveillance activities.

Under European data protection law, organizations processing personal data are divided into “Controllers”, the entities which control the personal data, and “Processors”, the entities that process personal data only on the instructions of the Controllers. The GDPR applies to both Controllers and Processors.

MangoApps Commitment to GDPR

Since our inception, MangoApps approach has been anchored with a strong commitment to privacy, security, compliance and transparency. Similar to existing privacy laws, compliance with the GDPR requires a partnership between MangoApps and our customers in their use of our services. We have analyzed the requirements of the GDPR, and have made enhancements to our products and processes to support compliance with this regulation.

To further earn our customers’ trust, we have a Data Processing Addendum (“DPA”) for our customers with contractual commitments regarding our compliance with the provisions required by the GDPR. Our commitment guarantees that customers can:

- Respond to requests from data subjects to correct, amend or delete personal data.
- Be made aware of and report personal data breaches to relevant supervisory authorities and data subjects in accordance with GDPR timeframes.
- Demonstrate their compliance with the GDPR as pertaining to MangoApps Services

To support our customers with their efforts to be GDPR compliant please refer to our list in the “More Resources” section below. We continue to add product features that assist our customers with their privacy & data protection rights when using our services.

Office Chat GDPR Readiness

Office Chat has a proven history of ensuring data privacy and trust of our customers. This trust and commitment has continued in our journey to be GDPR ready. Here are some of the key steps done to be ready for GDPR and other privacy & data protection regulations

1. **Office Chat is hosted on AWS cloud**:

   Office Chat utilizes 100's of security & compliance features of AWS to maintain the highest-level data security and protection requirements. Some of the key ones include

   - Access Control: Access to only authorized admins allowed using multi-factor authentication (MFA) and fine granular access to different AWS services
   - Monitoring & Logging: Asset management and configuration with AWS Config along with compliance auditing using AWS CloudTrail
   - Encryption: Encryption of data at rest with AES256, centralized key management (by AWS region) and IPsec tunnels into AWS

2. **Office Chat Security & Compliance Features**:

   With ongoing product innovation, we have added features and functionality to the Office Chat platform and it's now ready to support customers with their GDPR compliance programs. Using Office Chat advanced security & compliance features, customers can implement their compliance program covering transparency, accountability, data access, data portability, data rectification, right to be forgotten, restriction to processing etc. of the GDPR requirements. Additionally, Office Chat comes in-built with disaster recovery & encryption features for all our customers' data.

3. **Office Chat Organization Controls & Processes Upgrade**:

   MangoApps security team regularly reviews and measures it's technical and organizational controls & processes along with its compliance policies to ensure that they are robust and up to date. This includes:

   - Patch Management: Latest security patches applied for OS and applications on a regular basis and a record maintained.
   - Configuration Management: Configuration review of AWS EC2, RDS and other AWS services regularly done
   - Network & Firewall Configuration: Office Chat uses the AWS VPC advanced security features including security groups and network access control lists, with inbound and outbound filtering. Additionally, the most restrictive access is configured to AWS S3 where customer files are encrypted and stored at rest
   - Awareness & Training: Data protection & privacy training for employees is regularly done

4. **HIPAA Compliance Ready**: Office Chat comes with the ability to configure it for Health Insurance Portability and Accountability Act ("HIPAA")

GDPR Requirements & Actions

Below are the features and functionality available in Office Chat that supports GDPR compliance. Here we've clarified key GDPR requirements by grouping them into two different action categories: "Customer" and "Shared". Customer actions are requirements that only the customers of MangoApps can perform, shared actions are those that need to be performed by both MangoApps and the customers of MangoApps.

GDPR Requirement	**Actions**	**How Office Chat (By MangoApps) helps address the requirement? ***
1. Transparency	Shared	**Office Chat**: The Office Chat platform is designed to provide users with full control of their content and how it's accessed. Office Chat (By MangoApps) takes several measures to provide customers with transparency around how their personal data is managed: i. Privacy Notice: Office Chat privacy notice is easily accessible on the company's website and communicates our privacy practice. Office Chat also offers ways for customers to communicate directly with the Office Chat team regarding their data protection and other privacy-related issues. ii. Terms of Service: Office Chat provides an enhanced level of transparency with the easily accessible terms of service document on the company's website. iii. Release Notes: Through the Office Chat online release notes, customers can see what major feature changes and product releases are coming out. This provides a clear and accessible way for customers to know about new features and functionality to help them manage their content in Office Chat.

		Customer: Through the Office Chat platform, customers can control how content is organized, managed and accessed. Customers can grant or deny access to their Office Chat account and content, which means customers control who can and cannot access their content. Customers are responsible for providing an appropriate level of transparency regarding the personal data of the data subjects they manage on the Office Chat platform.
2. Data Protection by Design	Shared	**Office Chat**: Office Chat is responsible for developing and delivering the platform and how content is processed by the platform. Office Chat makes efforts to instill privacy by design throughout the organization, through internal privacy by design training and internal privacy reviews and assessments. To demonstrate even a greater deal of security Office Chat platform comes with features like two-factor authentication(2FA), complexity of passwords, Touch ID on mobile devices, custom IP ranges to limit access, disable and wipe out date remotely on mobile & desktop apps and auto-deletion/self-destruct capabilities. **Customer**: Users are responsible for how content is managed through the Office Chat platform. Organizations should periodically review their use and configuration of the Office Chat platform to validate data protection has been considered by design.
3. Data Protection Impact Assessment	Customer	If required by the GDPR, customers may need to appoint a data protection officer to ensure their compliance with the GDPR. Office Chat does not offer data protection officer services.
4. Data Encryption	Shared	**Office Chat**: All content posted in Office Chat is over HTTPS and is encrypted at rest using AES 256-bit encryption.

		Customer: Customers are responsible for ensuring Office Chat native encryption meets their requirements.
5. Data Rectification	Customer	Through its platform, Office Chat allow data subjects to have access to their profiles to amend inaccuracies and delete content they have posted.
6. Data Inventory	Customer	Office Chat platform enables users to control what content is shared & stored in Office Chat. Customers are responsible for maintaining an inventory of the personal data stored in the Office Chat platform and can user the admin portal to manage the user information.
7. Subject Access Requests	Customer	Office Chat provides multiple ways to customers wanting to access the personal data of users stored in Office Chat. While customers need to define their own policies and processes to fulfil a data subject access request, Here are some of the methods customers have available to them: . . i. Log exports: Customers can export logs through their domain admin portal (e.g., User access log, audit log, security log) . ii. Third-party integrations: Customers can quickly view and manage all their third-party integrations through the domain admin interface and settings . iii. Files download: Every file stored in Office Chat can be easily downloaded using download file feature. iv. Search: Users can use the search feature to access & find the content stored in Office Chat
8. Right to be Forgotten	Shared	**Office Chat:** Office Chat provides a feature to permanently delete a user which deletes all the content posted by the user. **Customer**: Users can any delete content that they have posted at any time. Additionally, customers

		are in control of the content stored in their instance of the Office Chat platform. This includes setting the appropriate timelines in Office Chat to manage the retention of their content. Based on the parameters set by customers, Office Chat will retain content before they begin to be processed for deletion. Office Chat retention settings are not applicable to content outside of a customer’s Office Chat instance or if customer’s content is processed in another system. Customers have control over content retention and can configure delete/self-destruct settings. Users have control over deleting the content they have posted and remove information about themselves from their profile.

***Since these key requirements are just a subset of the GDPR, please ensure your internal teams review all the GDPR requirements so you maintain compliance. This is not intended as legal advice and customers must seek appropriate legal advice to ensure their implementation of the requirements is in accordance with the GDPR.**

More Resources

We’re dedicated to evaluating and meeting the highest bar for data privacy globally and that means developing features and capabilities to ensure our customers world-over meet data privacy obligations. Here is a list of some more resources to help you on your GDPR journey with Office Chat

- Terms of Service and Privacy Policy
- Security & Compliance Features
- HIPAA Compliance