NGM Group

GDPR

NGM Group is Committed to Your Data Protection

GDPR stands for the European Union's General Data Protection Regulation and replaces the Data Protection Directive. The purpose of GDPR is to ensure appropriate protection of personal data in a digital society. NGM Group is implementing processes to help customers prepare for GDPR before its effective date of May 25, 2018.

Customers will receive notifications of new functionality and changes to our policies via email, and we'll also be updating this page and sharing content over the coming months, so check back often. While NGM Group will be providing information related to GDPR, the most authoritative resources will always be those produced by data protection regulators or the European Union itself. The full text of the GDPR can be found here.

GDPR is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. Essentially, the GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

How does it affect our Customers?
NGM Group customers who have interactions with individuals in the EU will be affected. These companies will be evaluating their marketing, sales, IT, and data management processes closely. They will be looking to each of their processors and sub processors to provide the information they need to comply with the Regulation.

What is NGM Group doing to help Customers get ready?
Responsible data security has always been a priority of ours. We have been consulting experts to understand the regulations and how it affects us and our customers.

We understand that complying with the regulation will be high priority for a number of our customers so we have been developing an action plan to ensure that NGM Group is ready on time.

We have developed and implemented new tools to prepared and manage GDPR Regulations that include:

- Tools for managing data retention in accounts
- Tools for anonymizing data in accounts
- Updated terms of service and privacy notices
- Account configuration tips for customers who need to comply with GDPR
- Webinar providing an overview of GDPR updates for customers

Redacting Information (for GDPR and Privacy)
If you are under obligation to comply with General Data Protection Regulation (GDPR) or have other privacy concerns, you can enable redaction to manually or automatically remove personally identifying information from customer interactions in your account.

All About the GDPR
While deregulation has been a stateside trend over the past decade, the 28 members of the European Union are gearing up for a massive increase in regulations around data privacy in the form of the General Data Protection Regulation (GDPR) — and this regulation will make a splash across the pond as well.

Encrypted Data
NGM Group provides a number of options to keep data secure by encrypting its entire call tracking platform using Transport Layer Security (TLS). Data can be at risk even while at rest, and security demands that stored data be encrypted as well. NGM Group's platform uses encrypted volumes to safely store recordings, transcriptions, log files, and other call data.

On an ongoing basis we will continue to monitor and advance GDPR. Be on the lookout for updates and announcements across the next few months.

Logging
Any time call recordings are accessed or modified, that event is logged in the NGM Group platform by user, IP address, and timestamp. Each user's unique login credentials associate them directly to their activity within accounts. Every call recording playback is logged so that administrators know when a call has been reviewed.

Secure Notifications
Customize notifications so that certain fields containing sensitive information can be removed to prevent the distribution of this information. In addition, URLs linking to audio recordings inside notifications can have multiple layers of security so that only specific people with designated logins and secondary PINs can listen to calls.

Dedicated Servers
To maintain compliance, NGM GROUP'S uses dedicated servers to protect sensitive information. Dedicated servers are exclusive to NGM Group and not shared with outside companies, eliminating the risk of sensitive data being distributed to unauthorized sources.

Physical
A secure physical facility with round-the-clock surveillance, multi-factor authentication, redundancy zones, and secure logging are included with all NGM Group accounts. Amazon Web Services (AWS), where the platform is hosted, complies with AICPA SysTrust, ISO 27001, and other leading physical security frameworks.

Network
NGM Group employs best practices for network security by protecting customer data from application to the platform to thousands of carrier connections around the world. Preventative measures include network firewalls, denial-of-service (DoS) and distributed-DoS prevention, and network posture assessment.

Security Audits
NGM GROUP'S regularly scans for security vulnerabilities and performs third-party penetration tests. All access to production clusters is restricted to NGM GROUP'S engineers and is always logged and audited.

24/7 Incident Response
We strictly follow an incident policy for responding to and reporting of different vulnerability risks. A Security Incident Response Team monitors alerts from upstream vendors, on-call twenty-four hours a day, seven days a week.

Privacy Policies
Strict data privacy policies block access to sensitive data and ensure it is only used to deliver the services configured. All NGM Group employees are also trained on HIPAA and privacy policies and participate in regular security audits.

V050118