OpenMarket and the General Data Protection Regulation (GDPR)

This document explains how the GDPR will change the way we handle personal data and what this means for you.

On May 25, 2018, the General Data Protection Regulation (GDPR) came into force.

It's the most significant piece of European data protection legislation to be introduced in 20 years and it replaces the 1995 EU Data Protection Directive. It gives every EU citizen new powers over their personal data and aims to unify data protection laws across Europe, regardless of where that data is processed.

All OpenMarket product offerings are compliant with GDPR. And we're committed to helping our customers with their compliance journey. That's why our services and contracts are built on robust privacy and security protections.

Your responsibilities as a customer

It's likely you'll act as the data controller for any personal data you share with us. That means you'll determine the purposes and means of processing this data.

We'll assume the role of data processor, meaning we'll process personal data on your behalf when you're using our Application Programming Interfaces (APIs). This applies to all of our services.

You'll be responsible for implementing appropriate technical and organizational measures to ensure and demonstrate that data processing is being performed in compliance with the GDPR. Your obligations will relate to things like:

- Lawfulness
- Fairness and transparency
- Purpose limitation
- Data minimization and accuracy

You'll also have to fulfill data subjects' rights with respect to their data.

You can find guidance related to your responsibilities on your national or lead data protection authority's website. It may also be worth browsing publications from data privacy associations such as the International Association of Privacy Professionals (IAPP).

OpenMarket commitments to the GDPR

If you're a data controller, you're required to use data processors that implement GDPR-compliant technical and organizational measures. Here are some things you may want to consider when you're assessing our services.

Expert knowledge, reliability, and resources

We employ a team of information security and privacy experts who maintain our defense systems, develop security review processes, build security infrastructure and implement our security policies. We also employ information privacy and regulatory compliance experts who look after privacy and security compliance. These teams engage with customers, industry stakeholders and supervisory authorities to shape our services so that customers can meet their compliance requirements.

Data protection commitments

Data processing agreements

Our data processing agreements clearly articulate our commitments to customer privacy. And we regularly update them based on feedback from our customers and regulators. We have updated them to reflect the GDPR. We hope they'll help you assess your compliance status when using our services.

Processing according to instructions

Customer data entered into our systems will only be processed in accordance with the customer's instructions, as described in our data processing agreements.

Personnel confidentiality commitments

All of our employees are required to sign a confidentiality agreement and complete confidentiality and privacy training, as well as our Code of Conduct training. Our training specifically addresses responsibilities and expected behavior with respect to the protection of information.

Use of subprocessors

We exchange messages with mobile phones across the world. And we must directly or indirectly connect with the domestic or international wireless carrier who provides service to these handsets. Sometimes we have to route messages through one or more intermediaries before the message arrives at the carrier. Each of these carriers and intermediaries might be considered "subprocessors" under the GDPR. The list of such "subprocessors" is constantly changing due to market circumstances. Many of these subprocessors will not allow you to conduct an audit of their operations directly, but OpenMarket will take measures to ensure they comply with the GDPR and other internationally acceptable security standards.

Security of the services

The GDPR demands that both data processers and controllers implement technical and organizational measures that ensure their services are adequately protected from data leaks and breaches.

We operate a global infrastructure designed to provide security through the entire information processing lifecycle. This infrastructure is built to provide secure deployment of services, secure storage of data with end-user privacy safeguards. It also provides secure and private communication with customers over the internet and safe operation by administrators. OpenMarket services run on this infrastructure.

Our security infrastructure is built in layers that support one another. The physical security of our data centers supports the security protections of our hardware and software, which supports the processes we use to control operational security. This layered protection creates a strong security foundation for everything we do.

Availability, integrity, and resilience

We've designed the components of our platform to be highly available so our customers are protected from data loss. All of our data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. And if our hardware, software, or network does fail, services are automatically and instantly shifted from one facility to another. That way operations continue without interruption.

Testing

Our infrastructure and application teams test our disaster recovery system on an annual basis. This involves testing communication plans, failover scenarios, operational transition and other emergency responses. Every team involved in these exercises develops testing plans and post mortems which document the results and lessons learned.

Encryption

We protect data in transit using IPsec or TLS. And we have seamlessly encrypted customer content stored at rest using one or more encryption mechanisms.

Access controls

Our employees' access rights are based on job function and role. And we use the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives.

Vulnerability management

We scan for software vulnerabilities using a combination of commercially available tools, intensive automated and manual penetration testing. We also use quality assurance processes, software security reviews and external audits.

Data return & deletion

Administrators can download customer data via our Dashboards and Reporting at any time during the term of our agreement.

Most personal data in our systems is retained for four months by default. This retention period is necessary for us to comply with various legal obligations, such as billing and invoicing. We can't delete this data, even if requested by the customer. But once the retention period expires, we will automatically delete it, regardless of whether the customer has requested deletion.

Assistance to the controller

Data protection team

We have a dedicated team to handle data protection-related enquiries. Customers should direct their inquiries to OpenMarket Global Support support@openmarket.com

Notifications

We've provided contractual commitments around incident notification for many years and we'll continue to inform you of incidents involving your customer data under the terms in our current agreements.

International data transfers

The GDPR demands that data owners apply a certain standard of protection to personal data when it's transferred to a third country.

Standards and certifications

ISO 27001 (Information Security Management) is one of the most widely recognized, internationally accepted independent security standards. We've earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centers that make up our platform.

We are OpenMarket
As an Infobip company, we help the biggest brands in the world use mobile messaging to connect with people in the moments that count. When they need to be helpful and responsive in real time. When customer experience isn't just a buzzword, it's an obsession. We'd love to do the same for you.

Visit www.openmarket.com for more information.

OpenMarket
An infobip company