GDPR Readiness FAQs

The General Data Protection Regulation (GDPR) comes into effect on 25 May 2018. It has been called the biggest shake-up of EU data protection laws for twenty years. Not only will it introduce new laws and enhance existing ones, but it will give regulators the power to impose substantial fines for non-compliance.
We expect our customers will want reassurance that Orlo and the services we provide will be GDPR compliant by the time the new law comes into effect.

As a provider of social media management tools, our business depends on the continued provision of secure, reliable and compliant services that protect customer data and promote customer trust. These FAQs should reassure you that we take our privacy obligations – both legal and contractual – very seriously and that we are active in ensuring GDPR compliance.

How is Orlo structured to ensure data protection compliance?

The protection of our clients' data is at the heart of our business. We have a strong culture of compliance, which is embedded within our software, systems and processes.

We have worked hard to establish a GDPR compliance framework with internal policies and procedures that are kept under review. Our personnel are trained to understand the importance of data protection and to apply its principles within their roles.

We have a designated privacy officer to guide our business on compliance and have specialist external advisers that we can call on for additional support.

Compliance is monitored through various activities, including internal auditing and analysis of incidents. We maintain records of our processing activities in compliance with Article 30 of the GDPR.

What is Orlo's role in respect of our data?

You are the data controller of all personal data held in our application under your account and Orlo is merely your data processor in respect of all the services provided to you. Our processing of your personal data is only on your documented instructions as set out in the contract between us. We do not use any of your personal data for anything that is not in the contract.

What personal data is stored within the Orlo application?

Our application only holds basic information about your authorised users, this being name, email address, password, last login, IP address browser and device details. If you opt for two-factor authentication, we will also store the user's mobile phone number.

Your social media followers may include any type of information (including personal data, images and videos) in their messages to you and your users can add free text to social contacts and messages. We don't use any of this information for any of our own purposes other than to create aggregated statistics, which do not identify any individuals. Our system is merely a place to store their messages to you and to enable you to manage and retrieve them. You are the data controller of your followers' messages and your users' free- text additions. As such, it is your responsibility to ensure you use these in compliance with data protection and other laws.

Is our data held separately from that of other Orlo clients?

Data is not physically separated within the Orlo application but it is logically separated. We have security policies and code that is automatically tested with every deployment to ensure that your data is not mixed with other clients' data.

Are the systems used by Orlo GDPR compliant?

We carried out a Privacy Impact Assessment of our software, systems and services and have made changes to ensure we meet and, in some cases, exceed GDPR requirements.

Our system architecture was developed with data protection and data security in mind. The databases in which your personal data is stored are only accessible by a small division of the internal development team who are internally vetted and have worked for us for a substantial amount of time. We do not use live data for testing and it is never stored on local machines.

What does Orlo do to protect login credentials?

We offer a number of login options:

- SAML (Security Assertion Markup Language) – this allows you to use SAML authentication single log in services such as OKTA and One Login . On request we can add other providers

- Two Factor Authentication (2FA) – this requires users to enter a code sent to them by SMS when logging into the system

- Google Account Login (Single Sign On / SSO) – this allows users to log in via Google Accounts if your organisation is using Google Business apps to manage its email accounts. Using this option allows your users to utilise Google's own security around the log-in procedure.

Ultimately, you are responsible for ensuring your users keep your account log-in credentials secure and for any activities or actions occurring under your account. Our application offers the ability to require “strong” passwords (passwords that use a combination of upper and lower case letters, numbers and symbols) for your account. Administrators can disable email/password as a means of logging into the application and force one of the above options instead.

What does Orlo do to keep customer data secure?

We have a suite of security measures in place. These are kept under review and, wherever we consider it appropriate, they are enhanced. These are:

- Encryption. Network devices are managed within a secure management network and servers are secured by firewalls. In both instances SSL/TLS secure encryption protocols are used. Data in transit is always encrypted to a minimum standard of 256 bit.

We use Cloud KMS (a cloud-hosted key management service), which lets us manage encryption keys for our services. This allows us to generate, use, rotate and destroy AES256 encryption keys.

For all administration based services, 2FA is enabled.

- Resilence. Orlo’s infrastructure is designed to be as resilient as possible. Our main database is ‘highly available’ which means that, if for some reason one server was to go offline the other servers would not only be able to pick up the work but would also contain replica data to ensure there is no downtime. We also run other databases that are built and configured so that, if one was to go down, there is already another ready to ‘hot swap’ and step in. All servers that serve our application are load balanced and so can distribute load/requests to a at least 3 servers.

- Monitoring. All of the servers we manage have antivirus and malware scanners installed and have updates applied frequently. We perform daily port scanning on public IP addresses to ensure there are no unexpected changes. Configuration management is dealt with by scripts with are kept and managed in our private version control system.

- Security testing. Orlo has its entire application scanned by external technically skilled individuals. Their remit is to try to break, gain unsolicited access and “hack” our systems in a safe way in order to find flaws or potential weaknesses in our platform. If you would like to see the raw and unedited report with you, please speak to your account manager.

We have some continual end-to-end testing of our server cluster to ensure specific key indicators are working correctly and use software to log and track with a combination of active checks and, for some

things, such as back-ups, passive checks. Our set up allows use to detect unexpected behavior early and team members are alerted if an expected behavior has not executed as expected.

Our code is written to log any critical events for our developers to address.

What back-ups does Orlo take?

Orlo carries out backup continuously. Whilst our main datastore holds replicas of data at all times, we also run our other databases with duplicate data in ready to swap over should the need arise.

Multiple snapshots of the entire database are taken every day and we store them on a separate server from the one that holds live data.

From these various back-ups, we are able to restore the entire database in the event of a major incident. We test our disaster recovery at least annually.

Will you need access to our systems?

We do not need access to your system unless requested for training or demo purposes.

Does Orlo rely on third parties to provide its services?

To date Orlo has not used external developers and intends to use only in-house developers moving forward. This may change in the future but, if so, external developers would be given only limited access to code bases, no access to live data and all code/contributions would be vetted before been deployed.

We use Cloud KMS to manage encryption keys for our services. We currently use leading providers, Rackspace, Amazon Web Services and Google Cloud Services, to provide hosting services. They have all been vetted and authorised by a designated approver within Orlo as part of our supplier on-boarding process and we have written contracts with each of them incorporating appropriate data protection provisions to protect your personal data.

What audit trails are maintained to protect our data?

Our software normally maintains a record of your users' activities in our application such as which of your users created a post to send out, who edited the post, and who created any free text notes on your followers' messages. You can view these audit logs through the application.

What procedures does Orlo have in place to deal with data breaches?

We are proud of our record of having no reportable data breaches to date. However, we know the importance of being prepared for an incident.

All security incidents and platform wide issues will be recorded in a Major Incident Report which will cover: the nature of the incident, the impact on your business and data subjects the resolution and any preventative action planned to avoid recurrence. We will also make an assessment as to whether the breach must be reported to the Information Commissioner and/ or affected individuals.

In the event of a data breach affecting your personal data, we will report this to you without undue delay through our normal support process.

Where will our personal data be processed by Orlo?

We use three of the leading providers to host our data and applications, RackSpace, Amazon Web Services and Google Cloud Services. All of the live data is stored within the UK and a limited number of back-ups are stored within the EU.

Where our designated staff are permitted access to your data to fulfil their roles, they do so only from our premises or specific machines.

What happens to our data at the end of the contract?

You are able to export your social inbox whenever you wish during your contract term. Our reports are printable and downloadable.

Once our contract with you has ended, we expunge all of your data (other than your shortened links) which then propagates through our backups. The deletion process can take up to a month to be completely removed from backups.

We retain your shortened links after our contract so that any social posts created from within our application using our link shortening service continue to redirect users to the correct location. No other information is retained or stored.

Will Orlo help us comply with data subject rights?

You have full control over your user data and data from followers so you should be able to manage all data subject rights yourself just by using the application. If you need any specific guidance on how to do this, you can use our 'help' feature in the application or consult our user guide or use our online chat facility.

Will we be able to audit Orlo premises and systems for compliance?

You will appreciate how important it is that our systems and premises ensure confidentiality for all of our clients and we do not normally allow clients to have access. We do, however, engage an external specialist to check our systems and provide a report on compliance each year and we are happy to make that available to you for your peace of mind.

Of course, if a court or regulatory body requires us to give you access, we will honour that requirement but will require you comply with our security and health and safety requirements in doing so.

What changes can we expect to see in our contract and services?

Your services will continue unchanged although you may see some new features within our application and we may make additional security checks when you seek our support.
The GDPR requires you, as a data controller, to include additional things in your contracts with data processors. We have, therefore, prepared new data protection provisions, which will replace those in our current contract with you. We will be in touch with each of our clients to provide details of the changes so that we can all be satisfied that we are meeting our legal obligations.