GDPR Basics: Are you GDPR ready?

This new EU regulation named General Data Protection Regulation (GDPR) is focused in the **protection of personal data and digital privacy** and takes effect on May 25, 2018.

This law is designed to accomplish two main things:

- Unify the current data protection privacy laws throughout the EU
- Enhance the rights of citizens of the EU to protect their personal information

Who the GDPR Applies to

The GDPR applies to any business that does one or both of the following:

- Offers products or services to citizens of the EU
- Collects personal information from citizens of the EU

Note that if you meet either of these criteria, it doesn't matter where your business is located. This means that for example a U.S.-based hotel that simply collects email addresses from EU guests will be required to comply with the GDPR.

What the GDPR Requires?

The GDPR requires to communicate information about how personal data is processed.

According to Article 12 of the GDPR, this information should be:

- Concise
- Transparent
- Intelligible
- Easily accessible
- In clear and plain language

Update your Privacy Policy

The previous can be accomplished with a Privacy Policy where you let your users know:

1. **Who your Data Controller is**: The data controller will likely be your business, unless your business operates as a data processor for other companies.

2. **Whether you use data to make automated decisions**: If you use personal data to make automated decisions – such as for credit scoring, loan screening, profiling users or making employment decisions – you need to disclose this to users.

3. **Inform users of the 8 rights they have have under the GDPR**: Most of these rights involve things like the right to access data, request changes, deletions and corrections. For example, if you collect email addresses to use our Guest Satisfaction Survey ("GSS") service, give users a chance to remove their email address from the service or allow them to update or change it.

4. **Whether providing data is mandatory**: Let users know whether they are required to provide you with personal data, and what happens if they don't.

5. **Whether you transfer data internationally**: If your business transfers personal data to a different country or international organization, you need to let users know this.

6. **What's your legal basis for processing data**: Under the GDPR, you need to have a lawful basis for processing any personal data. There are six available lawful bases, and each piece of data you process needs to fall under one of the six categories.

   The most common two would be:
   - The subject has given consent to have data processed for the specific purpose/s
   - Processing is necessary for pursuing a legitimate interest For example, sending satisfaction surveys to the hotel's guest with our Guest Satisfaction Survey ("GSS") service, can be alleged as a legitimate interest for the hotel.

Get your user's consent

Before you collect basic personal information (email addresses, names, financial information, etc.), you'll need to get clear, unambiguous affirmative consent.

The best way to satisfy this requirement is to always use checkboxes to get an opt-in consent. Make your users click a box next to a statement that says by clicking, the user is agreeing to your Privacy Policy terms. Link to your Privacy Policy here, as well.

Remember…

- Update the language of your Privacy Policy to drop the legalese and be easy to understand by your average user with the additional information required by the GDPR

- Use checkboxes to get clear, undoubted opt-in consent before collecting any personal data.

*This article is not a substitute for professional legal advice and does not create an attorney-client relationship, nor is it a solicitation to offer legal advice.

Subprocessors: Who do we work with? Discover our partners

At ReviewPro we are very committed to maintaining the privacy and confidentiality of the personal information we process during the provision of our services as a data processors.

To achieve that, we work with the most reliable partners, who have or potentially will have access to personal data during the provision of our services as a sub-processor.

Entity Name	**Type/ Purpose**	**Geographical locations**
Rackspace /Objestrocket	Hosting Storage of the information and resources related to the provision of the services.	US/ Germany
MailChimp	Mail services to send the surveys.	US
Google	Processing of the clients' emails and domains affected by the service.	US
Amazon Cloud Services	Hosting storage of the information and resources obtained related to the provision of the services	US/Germany
ExaVault	Service for the	US

	processing of PMS files with guest data sent by the client.	
MailGun	Mail services to send the surveys.	US
Microsoft Azure	Cognitive language API used for intent and entity detection.	US

Privacy Notes: How we handle the data at ReviewPro?

Where do we store the data during the provision of our services?

We use four datacenters, Amazon AWS USA, Amazon AWS EU and Rackspace-Objectrocket USA and Rackspace-Objectrocket EU.

Amazon AWS provides the cloud hosting infrastructure which powers the ReviewPro tool, services and data processing. Rackspace holds our data infrastructure. Amazon AWS provides a complete multi-AZ high availability to prevent a complete failure or data corruption.

How do we manage our infrastructure?

ReviewPro's infrastructure is managed via cloud provisioning, configuration management, application deployment and intra-service orchestration tools. In the event of catastrophic failure at the Amazon AWS region a duplicate version of the site will be brought up in an alternative Amazon AWS region. Amazon AWS has data centers located in 23 regions globally. Rackspace has enterprise-grade global data centers located in Chicago, Dallas, Northern Virginia, London, Hong Kong and Sydney (Frankfurt under development).

Service provider certifications

- **Amazon AWS:** ISO/IEC 27001, 27017, 27018, ISO/IEC 9001, CSA STAR CCM, SOC 1/2/3, PCI-DSS, FedRAMP, DOD CC SRG, HIPAA, IRAP, MTCS, C5, K-ISMS, ENS alto, OSPAR, HITRUST CSF, FINMA.
- **Rackspace:** ISO/IEC 27001, ISO 14001, ISO 18001, ISO 9001, SOC 1/2/3, PCI-DSS, FedRAMP JAB P-ATO, NIST 800-53, FISMA, NIST 800-171, CJIS, ITAR, FIPS 140-2, HITRUST, HIPAA, HITECH.

Moreover, our data center has the following features of interests:

- **Power**: power systems deliver conditioned power while protecting against sags, surges, swells, spikes and electrical noise. Uninterruptible power supplies (UPS) provide instant failover for continuity during a power outage. On-site, always-fueled diesel generators are prepared to pick up the load quickly during extended outages. Cooling: N+2 redundant chiller configuration uses a combination of centrifugal chillers, cooling towers, chilled water loop pumps and condenser water loop pumps — with redundant water sources.
- **HVAC**: precision Heating, Ventilation and Air Conditioning (HVAC) environment includes HEPA-equipped air handling units that remove dust and contaminants. In the event of an HVAC system failure, redundant HVAC systems are available for immediate failover.
- **Networking**: robust network includes nine backbone providers, allowing to shift traffic as needed. This configuration, co-developed with Cisco, guards against single points of failure at the shared network level.
- **Physical Access Security**: Each Rackspace data center is restricted by biometric authentication, keycards, and 24x7x365 surveillance. Rackspace is also ISO/IEC 27001 (information security management) certified which are reflected in their employee screening practices.

What is our Platform uptime?

Currently we have a more than 99% uptime record. Availability and Business Continuity are warranted by the following best practices:

- All systems are backed-up multiple times per day.
- All key systems monitored and fully redundant.
- Key systems such as Hadoop File System, Cassandra NoSql database, and Elasticsearch provide further safety via replication.
- System architecture deploys redundancy on all key layers; application, API, and data storage.
- System is load balanced for stability and redundancy.

ReviewPro is built in a distributed manner with multiple redundancies to guarantee stability and end user performance. As such, most of the maintenance and development tasks are performed without requiring any down-time and are transparent to the end user. In the rare case that downtime is required, advance notice will be given to the client with an established time window.

All ReviewPro data whether for end users or guests is transferred using strong encryption TLS/SSL. ReviewPro also uses the following additional security safeguards:

- Passwords are never stored by the system rather SHA2 based hash is used which includes a unique salt to avoid rainbow table lookup.
- Passwords are never sent in the open and are not known by ReviewPro staff.
- When storing sensitive user data, such API or third-party credentials, the data is always store encrypted.
- Surveys invitations are delivered in email with an encrypted link and surveys are always served with SSL.

How we do secure our platform?

We secure our platform from the Internet in the following 4 ways: Firewalls: All instances are locked down using software firewalls with only the minimal number of ports open and restrictions on which machines can access specific ports. Network segmentation: Incoming requests from open internet are blocked. In the case of public facing services, they are always routed through Amazon AWS cloud load balancers and only the required ports are exposed. All traffic from load-balancers to our services is routed through a nonpublic network. Further, service to service communication is done via a private network. Audit and Intrusion detection tools: all servers are monitored and analyzed by our IDS. Routine patching of systems against knows vulnerabilities.

We use Akamai for site acceleration and Akamai servers sit in front of ReviewPro. Akamai does provide features found in common WAF tools.

ReviewPro relies on secured cloud services for core business activities, mitigating the risks from disaster to our physical location, equipment and information systems. In the event of disaster at our physical location, business activity would continue with support from our global workforce.

Connectivity

Reviewpro service uses AWS Global Cloud Infrastructure with multi-AZ deployments to provide a secure, extensible and fault tolerance service. Our failure contingency plans include the ability to create new resources to other availability zones or regions and balance the service to avoid service disruptions. All connections between services, databases and integrations are done encrypted.

Our client support, engineering and other teams use networking infrastructure that uses multiple redundant internet service providers.

We use Akamai for site acceleration, Akamai servers and Akamai Web Application Firewall it in front of of ReviewPro’s to ensure that clients from around the world can use ReviewPro in a speedy, secure and responsive manner.