What is GDPR?

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. The changes that GDPR makes to data protection legislation are far reaching and the GDPR introduces a number of new legal concepts.

GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. All organisations that process European citizen’s personal data will need to be compliant with GDPR as of 25 May 2018.

I**t is important to note that GDPR does not have an accredited certification method.** This means, there is no GDPR-approved way to demonstrate compliance. If you have questions regarding our compliance please reach out to gdpr@salesorder.com and we’ll happily answer any questions you may have.

The principles guiding our GDPR implementation are:

- **Integrity:** Securing and safeguarding personal data using appropriate technical and organizational security measures.
- **Lawfulness:** All our trading partners must, among other things, ensure they have a legal basis for processing personal data, and process that data in a fair and transparent manner.
- **Limited Use:** Personal data may only be collected for specific, explicit, or legitimate purposes.
- **Data Minimization:** Only collect data that is relevant and necessary for its intended use.
- **Accuracy:** Personal data must be accurate and up-to-date.
- **Storage Limitation:** Subject to relevant exceptions, maintain personal data only for as long as is deemed necessary and reasonable.

Because we operate mission critical software as a service maintaining your trust and keeping your personal data private and safe is an imperative.

To **ready ourselves for** GDPR we’ve:

- ✓ made sure that decision makers and key people are aware of GDPR and its impact.
- ✓ conducted a GDPR audit and gap assessment to create a plan to comply with GDPR.
- ✓ appointed an interim Data Protection Officer DPO whilst we consider a permanent solution. To contact our DPO - gdpr@salesorder.com.
- ✓ implemented a company-wide data protection training module for all Salesorder team members.
- ✓ made sure all Salesorder team members sign a confidentiality agreement and complete mandatory confidentiality and privacy trainings.
- ✓ made sure all Salesorder team members have reviewed and have access to our Data Protection Policy.
- ✓ conducted a data-mapping exercise that tracks personal data flows throughout our infrastructure and platform.
- ✓ reviewed the GDPR readiness of third-party data processors to make sure we have the right contractual protections in place.

- ✓ put in place processes to service subject access requests and the right to request deletion.
- ✓ Published and made available a GDPR compliant Data Processing Agreement (DPA)
- ✓ updated our privacy notice to be GDPR compliant and concise and transparent about how we process personal data
- ✓ updated our incident response procedures to bring them into line with GDPR
- ✓ set up a method to regularly review GDPR best practises and changes to the regulations.
- ✓ put in place a plan to introduce regular training to specifically address responsibilities and expected behavior with respect to the protection of information.

It is important to note that GDPR does not have an accredited certification method. The logical conclusion is compliance is a moving target.

The GDPR defines us as (1) and (2)

1. **Data Controller:** an organisation which collects and processes the data is the 'data controller' and has the main responsibility for compliance and accountability for the data it holds.

2. **Data Processor:** under GDPR, 'Processor' means: 'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.' (Article 4)

This means the personal data we 'hold' falls into two distinct categories, the data we control and the data we process. For the purposes of clarity we define these respectively as **Codata** and **Prodata.**

Codata is the personal data we keep about you our lead, prospect or customer for to conduct our commercial relationship.

Prodata is data we process on your behalf. **Processing means:** 'any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' (Article 4) This definition is very broad and is likely to encompass the vast majority of business activities which use personal data.

There are new requirements in GDPR designed to make processors share the accountability for data protection compliance. They will also, for the first time, **be jointly liable for breaches** which require compensation of individuals for damage caused by non-compliant processing.

From a privacy perspective, you the customer are the controller of **Prodata,** and we are a processor. This means that throughout the time you use or subscribe to our services, you retain ownership of and control of your Prodata.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We may disclose personal data to respond to subpoenas, court orders, or

legal process, or to establish or exercise our legal rights or defend against legal claims. We may also share such information with relevant law enforcement agencies or public authorities if we believe same to be necessary in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Master Subscription Agreement or as otherwise required by law.

We maintain an up-to-date list of the names and locations of all sub-processors used for hosting or other processing of Codata, Prodata or both.

Where's my data and what are you doing with it?

For a breakdown of what data we capture, where we capture it, what we do with it and who we trust to store it see our Data Tracking page.

Data protection and security

To help you maintain the privacy and control of your Codata and Prodata a we pragmatically apply common sense and industry standard information security and data protection best practices in the design and testing of our infrastructure and platform:

- **Data security:** In order to safeguard a Codata and Prodata from unintended disclosure or misuse we use strong data protection controls including encryption of data whilst in transit or at rest.
- **Data hosting and backup:** All Codata and Prodata related to customers whose businesses operate in the EEA/EU is kept at Rackspace Data centres in UK.
- **Access management**: We do not access or use Codata and Prodata for any purpose other than providing, maintaining and improving our service. We only disclose Service Data to third parties where disclosure is absolutely necessary or is required by law.
- **Data Protection Policy:** All of our team follows and refers to our rigorous Data Protection Policy - a copy is available on request at gdpr@salesorder.com