GDPR Readiness:

The General Data Protection Regulation

May 2018

Overview

Throughout this document, we will discuss the basic elements of the GDPR. We will address responsibilities of both Sparta Systems, Inc. and those of you, our Customer. Please reach out to your Account Executive or GDPR@spartasystems.com if you have additional questions.

For those already familiar with the General Data Protection Regulation (GDPR), we have assembled this Quick Reference Table which covers our products and our roles in ensuring compliance.

	Solution				
	TrackWise On-Premise (and +1's)[1]	**TrackWise Supplier Collaboration**	**TrackWise Digital**	**TrackWise Digital DMS**	**TrackWise Digital eMDR**
Data Controller	Customer	Customer	Customer	Customer	Customer
Data Processor	IT Partner (Optional)	Sparta Systems	Sparta Systems	Sparta Systems	Sparta Systems
Data Sub-Processor	N/A	AWS	SalesForce.com	Box.com	AWS

** For the TrackWise Digital application Sparta Systems does not have access to or process any Personal Data. For this application, access to Personal Data and all data processing functions are restricted to Sparta's Sub-Processor Saleforce.com.*

The most important thing to understand is that Sparta's products are already built with "Data protection by design and by default", or Privacy by Design (PbD), to help comply with this new regulation. We have built our systems to comply with the Title 21 CFR Part 11 and its associated rules around data integrity and data security. This is true for all of Sparta's products.

Terminology

As you prepare for, or continue on, your journey towards GDPR readiness, you might have some questions on the products that Sparta offers. Let's first start with some terminology.

Is Sparta ready for the GDPR? What has Sparta done?

Before we can discuss responsibility and ownership, it is important to know the four main actors is this scenario. These are defined in ***Article 4 of the GDPR: Definitions*** (sub-sections included below)

7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
8. 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

How a Sub-Processor Defined, per ***Article 28 of the GDPR: Processor*** (sub-sections included below)

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor…shall be imposed on that other processor by way of a contract or other legal act…in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation…

In short, Processors are required to obtain a specific or general prior written authorization of the data controller in order to engage sub-processors.

[1] The term +1's refers to associated products that function with TrackWise such as Quality View, Web Services, AEP, and others. For the purposes of this discussion, these products require TrackWise to function and are fully supported by customer controlled infrastructure.

When such authorization is obtained, the processor must (i) impose the same data protection obligations on the sub-processors as set out in the data processing agreement between the controller and the processor, (ii) ensure that the sub-processor does not process personal data except on instructions from the data controller, and (iii) inform the data controller of any changes to sub-processors and give the data controller the opportunity to object to these changes.

Sparta will not engage a sub-processor to process Customer Personal Data without the relevant customer's prior specific or general written consent. Sparta will inform the relevant customer company of any intended changes concerning the addition or replacement of other sub-processors and provide customer companies an opportunity to object to such changes. Sparta requires any sub-processors to provide data protection at a level equal to Sparta's own policies.

Sparta will only process Customer Personal Data to the extent necessary to provide the services requested by its customer companies and only in accordance with the relevant customer company's instructions. This includes any transfers of Customer Personal Data outside the European Economic Area. Sparta will keep a written record of data processing that clearly sets out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of individuals whose personal data will be processed; and
- the relevant customer's obligations and rights in relation to the personal data.

Assignment of Responsibility

In short, for our products, *you are the Data Controller*. You define the configuration, own the configured processes, administer access, and define what happens with the data. This is true for all products you purchase or subscribe to from Sparta. This is, generally speaking, true of most systems you would have within your organization.

The *Data Processor role* is where things can get more complex:

- Let's start with fully On-Premise products, which include ***TrackWise*** and its associated products such as ***QualityView, Web Services, AEP***, and others. For any products of which you control the Infrastructure, you take on the functions of a Data Processor. With respect to the GDPR, you will still only be considered a Data Controller, as all functions would be under the same legal entity. If an eternal hosting provider or an external IT function is leveraged, they would then be your Data Processor, and be subject to the requisite GDPR controls and assessments.
- Next we can move on to "Platform-based" solutions, including **TrackWise Digital (TWD)**, which is based on the salesforce.com platform. While this seems different to On-Premise TrackWise, there are a number of similarities that make this behave more so like an On-Premise solution than a traditional SaaS solution, so far as the GDPR is concerned.
  - In the scenario of TWD, Sparta provisions you an account, available on a subscription basis. This is the functional equivalent of a Hosting Provider (processor) for TrackWise On-Premise.
  - Once provisioned, the customer can download and install the TWD application, similar to the downloading and installation of a TrackWise ISO. Remember, like TrackWise, Sparta has no access to your account under any normal operating conditions. We cannot collect, record, organize, structure, store, adapt or alternate, retrieve, consult, use, disclose by transmission, disseminate or otherwise make available, align or combine, restrict, erase or destruct your data sets.
  - Regardless of Sparta's lack of access to any data, **Sparta is the Data Processor**, and salesforce.com is the Sub-Processor. Salesforce has their own GDPR site available for your review.
  - To this end, Sparta Systems will issue a Pass Through DPA (Data Privacy Addendum) to ensure controls and assurances in place by our sub-processors are passed through to you via your direct agreement with Sparta Systems.
- For Sparta's SaaS based products **(TrackWise Supplier Collaboration, TWD DMS, TWD eMDR)**, *Sparta is your Data Processor*, with box.com and AWS as Sub-Processors to Sparta, who administers these solutions.

For instances where Sparta is a Data Processor for your organization, Sparta will assist you by appropriate technical and organizational measures for the fulfilment of your obligation to respond to requests for exercising the data subject's (transparency and access to information, rectification and erasure, restriction of processing, data portability, right to object).
Sparta will provide all necessary and reasonable assistance to the relevant customer:

- to enable the relevant customer to comply and respond to a request, query or complaint from an individual in relation to his/her personal data; and
- to enable the relevant customer to carry out any data protection impact assessment, including any privacy by design and privacy by default techniques employed in relation to the processing of Customer Personal Data.

This naturally leads us to the next topic for discussion…

Data Obfuscation and 21 CFR Part 11 Compliance

What about this "Right to be Forgotten"? How do I delete data in TrackWise, TWD, or some other quality system?

The short answer is: **You don't.**
Again, let's start by understanding ***Article 17 of the GDPR: Right to erasure ('right to be forgotten')*** (sub-sections included below)

1. The *data subject shall have the right to* obtain from the controller the *erasure of personal data* concerning him or her without undue delay and the controller shall have the obligation to erase personal data *without undue delay where one of the following grounds applies:*
   a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
   c. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
   d. the personal data have been unlawfully processed;
   e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
   f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. *Paragraphs 1 and 2 shall not apply* to the extent that processing is necessary:
   a. for exercising the right of freedom of expression and information;
   b. *for compliance with a legal obligation* which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
   d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
   e. for the establishment, exercise or defence of legal claims.

These basis for these rules are defined in Article 6 of the GDPR: Lawfulness of Processing (sub-sections included below)

1. ***Processing shall be lawful only if and to the extent that at least one of the following applies:***
   a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   b. ***processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;***
   c. ***processing is necessary for compliance with a legal obligation to which the controller is subject;***
   d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
   e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Per Article 6.1.c and Article 17.3.b, the majority of our customers have a legal obligation to be Part 11 compliant. According to Article 6.1.b, their employment contracts and supplier contracts allow them to collect and maintain employee and supplier data so far as they're employed/under contract and beyond such that it is done to be in compliance to their internal and predicate rule mandated retention policies. Individuals do not have grounds for the removal of this data per Article 17.3.b in order to comply to those predicate rules.

After exceeding those retention mandates, data can (and in most cases should) be removed. This may include archiving and deletion of the record archives. You cannot obfuscate data in a 21 CFR Part 11 system and remain complaint to that standard.

> *Title 21 CFR Part 11.10(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.* ***Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.***

Even if you overwrite a data field with non-identifiable name, Audit Trail will remain. Archiving out of the 21CFRPart11 systems is generally your only option for requests for removal.

Data Breaches

Under Article 33 of the GDPR, a Processor is required to notify the data controller without undue delay after learning of a data breach. Sparta has adopted and implemented a Data Security Incident Response Policy for data breach incidents.
In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data, Sparta shall immediately notify the relevant customer. Sparta shall provide reasonable assistance to the relevant customer to facilitate the handling of any such breach. In particular, Sparta shall assist the relevant customer with its obligation to notify:

- affected individuals; and
- relevant data protection supervisory authorities

.

Sparta's Internal GDPR Compliance and Readiness

In addition to Sparta's externally facing work in the GDPR space, Sparta has also undertaken steps to prepare for the impact to internal employees. Sparta is the Data Controller for our internal efforts and has completed the necessary Data Inventories,

Data Assessments, Data Retention plan, and Readiness Assessments which cover the information collected related to impacted employees. Sparta has also begun training employees to ensure every Spartan knows their role and impact with regards to the GDPR, both internally and externally facing.

Compliance Records

Under Article 30 of the GDPR, Processors are required to maintain a record of all categories of data processing activities carried out on behalf of a controller, that must contain a certain amount of information listed under Article 30 of the GDPR (including the categories of processing activities performed, a general description of the data processors' security measures to protect personal data, etc.).

Sparta will make available to customer companies (for which Sparta is a Data Processor) all information necessary to demonstrate compliance with its obligations in relation to Customer Personal Data, including allowing for and contributing to audits and inspections conducted by the relevant customer or another auditor mandated by the relevant customer, per existing agreements. Sparta will immediately inform customer companies if, in its opinion, an instruction in this regard infringes applicable law.

References

- **Sparta Systems**
  https://www.spartasystems.com/trust
- **Salesforce**
  https://www.salesforce.com/gdpr/overview/AWS
  https://www.salesforce.com/content/dam/web/en_us/www/documents/data-processing-addendum.pdf
- **Box.com**
  https://www.box.com/gdpr
- **Amazon Web Services**
  https://aws.amazon.com/compliance/gdpr-center/