

Rosslyn's Commitment to GDPR

We are committed to providing our Data Analytics solutions to our Clients in compliance with applicable laws and regulations in general and data privacy laws such as the EU General Data Protection Regulation (GDPR) in particular. We seek to partner with our Clients and their users to help them understand how we achieve data privacy compliance as processor and how the RAPid platform enables our Clients to achieve data privacy compliance as controller.

GDPR and what it means for you

Effective as of May 25, 2018 the GDPR will replace the currently applicable EU Data Protection Directive. Unlike the Data Protection Directive, the GDPR will have direct effect in all EU member states without any need for local implementing legislation and it will override existing national privacy laws.

Besides strengthening and standardizing user data privacy across the EU nations, the GDPR will require new or additional obligations on all organisations that handle EU citizens' personal data, regardless of where the organisations themselves are located.

Whenever the Data Protection Directive or the GDPR applies to our Clients they are deemed the controller of the personal data included on the RAPid Platform and RDT is deemed the processor. As such, both RDT and our Client have to comply with their respective obligations under the Data Protection Directive and the GDPR accordingly. One side of these obligations relates to the controller-processor relationship, while the other side relates to the controller obligations vis-à-vis the data subject, typically the user of the RAPid Platform (i.e. employees, contractors and partners of our Clients).

We expect our Clients and their users to comply with all applicable laws and regulation in connection with the use of the RAPid Platform, in particular making sure, that our Clients have all rights and consents necessary to allow RDT to use and process such data.

As a service provider, RDT is committed to supporting our Clients in their compliance activities, including as outlined in GDPR Chapter III (Rights of the data subject), most notably the rights of access and rectification (Art. 15 + 16 GDPR), right to erasure or 'right to be forgotten' (Art. 17 GDPR), right to data portability (Art. 20 GDPR), and right not to be subject to automated decision-making, including profiling (Art. 22 GDPR).

Our top 5 priorities for GDPR compliance

*The following section refers to the Gartner Blog "Smarter with Gartner" on GDPR) Gartner lists the top 5 priorities for organisations to focus on to ensure compliance when GDPR comes into effect. Below we explain RDT's position relating to these priorities:

#1 Determine your role under the GDPR

As a cloud-based data analytics solutions provider, RDT is processing data on behalf of its Clients using the RAPid Platform; therefore RDT is seen as a data processor under the GDPR. In light of existing data privacy laws and data security measures generally expected from a global cloud service provider such as RDT, we have already implemented an information security program consisting of

policies and procedures to help ensure that RDT is acting in accordance with current and new compliance requirements when providing our services.

#2 Appoint a Data Protection Officer

The GDPR will require some organisations to designate a Data Protection Officer (DPO). Organisations requiring DPOs include public authorities, organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organisations who process what is known as sensitive personal data on a large scale. At RDT we have appointed a Main Board member to this role.

#3 Demonstrate accountability in all processing activities

Our RDT compliance program is already comprehensive and based on globally accepted standards. Its effectiveness is periodically attested to by 3rd parties under various compliance certifications (e.g., ISO 27001, ISO 9001, CREST). RDT has implemented an information security program consisting of policies and procedures that define how system information is entered, managed, and protected. RDT's current information security program is further specified in our Master Subscription Agreement (MSA) as well as our Data Processing Agreement (DPA). In particular, RDT commits to monitor, analyse and respond to security incidents in a timely manner in accordance with RDT's standard operating procedure, which sets forth the steps that RDT employees must take in response to a threat or security incident. RDT continues to invest in a growing global security capabilities.

#4 Check cross-border data flows

Both the Data Protection Directive and the GDPR permit personal data transfers outside of the EU subject to compliance with defined conditions, including conditions for onward transfer. When a Client contracts with RDT, we can enter into a Data Processing Agreement (DPA) with applicable Clients. In the DPA, we agree with our Client on the terms for the compliant processing of Client personal data, including the description of our security and data privacy policy and the EU standard contractual clauses.

#5 Prepare for data subjects exercising their rights

Within the RAPid Platform, our Clients use the personal data of their users to interact with each other in order to better manage their data analytics. These acting individuals are the data subjects and our Clients - acting as data controllers - need to be able to answer certain legitimate requests under the www.rosslyndatatech.com info@rosslynanalytics.com • www.rosslynanalytics.com GDPR. As such, our Clients will look to RDT as service provider and data processor to offer functionalities within the RAPid Platform that enable our Clients to achieve compliance. Our internal product design processes are focused on the user and their positive and productive experience on the RAPid Platform. In light of GDPR, RDT periodically reviews the RAPid Platform features in order to validate that the RDT platform provides the required functionalities to our Clients.

Staying current

Ensuring the privacy and security of our Client's data is an ongoing commitment for RDT. We will continue to update this document to reflect any GDPR-related developments.