# GENERAL DATA PROTECTION REGULATION (GDPR) FAQ

February 2019
Version 3.0

## What is GDPR?

The **General Data Protection Regulation** (**GDPR**) (EU) 2016/679 is the new regulation in EU law focusing on data protection and privacy for all individuals within the European Union. It replaces the 1995 Data Protection Directive (Directive 95/46/EC).

## When did GDPR take effect?

GDPR becomes enforceable starting 25 May 2018.

## To whom does GDPR apply?

GDPR applies to every business that processes personal data within all EU member states. GDPR also affects businesses outside the EU who process the personal data of EU residents and offer them goods and services, irrespective of whether payment is required; or where the processing by a business relates to the monitoring of the behavior of EU residents in so far as their behavior takes place within the EU.

## What about the UK and Brexit?

GDPR will go into effect before the leave deadline of Brexit and therefore UK firms must comply with GDPR. After Brexit, UK firms that offer goods or services to EU residents still need to comply.

## What information does GDPR apply to?

GDPR applies to 'personal data', which means any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as - name, email address or location, and also online identifiers like IP address, types of website cookies and other device identifiers. Personal data also applies to special categories which need to meet higher criteria for collecting and processing. This is primarily data on race, ethnic origin, trade union membership, sexual orientation, health data, political affiliation and religion or beliefs as well as criminal convictions.

## What is RDC's purpose of processing?

RDC processes personal data to provide RDC's services in order to assist subscribers with their regulatory compliance obligations.

## What is a Controller, Processor or Sub-processor?

GDPR applies to data controllers, processors and sub processors alike.

- Data controllers direct the collection of personal data.
- Data processors provide services to the data controller in accordance with each data controller's instructions on processing personal data.
- Sub-processors or third-party businesses performing data processing for other companies are also accountable for protection of personal data, and work at the direction of the data processor. Sub-processors are subject to the same controls and direction from the data controller and data processor.

## Is RDC a Data Controller or Data Processor?

RDC operates as both a data controller and data processor. For our subscribers, RDC processes personal data on their behalf and at their direction. In this case RDC is a data processor and its subscribers are data controllers. For the curation of RDC's GRID database,

RDC is a data controller and directs its employees and any sub-processors on all aspects of handling the content and any personal data that may become part of the GRID database.

## RDC as Data Controller (Products and Services)

Personal data collected by RDC is curated from various public sources including:

- National and local governmental watch lists such as OFAC, sanctions actions and other law enforcement lists.
- Public sector information - directories or registries such as sex offenders and human trafficking lists.
- News sources are used to gather and process risk-relevant information on individuals and organizations and can include financial crimes such as money laundering, fraud or bribery as well as violent crimes like assault or murder.
- Profiles on Politically Exposed Persons (PEPs) are assembled using the guiding principles of collection aligned to global and regional PEP definitions formed by authorities such as the Financial Action Task Force (FATF) FATF and the Wolfsberg Group.

Personal data that may be collected includes name, address, date of birth, country of origin and other profile information. RDC may also include religion, political affiliation, nationality and criminal activities as necessary to assist our subscribers in meeting their regulatory obligations and to properly identify the appropriate risk-relevant individual.

## RDC as Data Controller (Website)

RDC collects personal data when subscribers and non-subscribers initiate a request for product information, demos, white papers, or webinars and may include name, address, IP address, and device information. All communications with RDC include an initial opt-in by the person whose data will be collected; the opportunity to later opt out of such communication is provided as well. Direct op-out requests may also be sent to privacyofficer@rdc.com.

## RDC as Data Processor (Handling our Subscribers' Data)

As part of our business our subscribers may provide us with their own data, such as their customer's personal data, so that we may offer them a product or service. Personal data provided by our subscribers is processed only under strict direction from the subscriber with a commitment to the privacy and protection of that information. Handling of that information is governed by an agreement between the subscriber and RDC and reflects compliance with GDPR.

## Does RDC use Sub-Processors?

The personal data that RDC collects and processes comes from public and publicly available sources. In certain cases, RDC also employs sub-processors and content aggregators to assist in the curation of our products on behalf of our subscribers. Those sub-processors or third parties are under agreement with RDC and are subject to the same GDPR policies as RDC.

## How does RDC collect personal data?

RDC employs different methods for collecting personal data including both manual extraction and automated methods for monitored lists, website inquiries as well as feeds from vendors such as news aggregators.

## What personal data does RDC collect?

For RDC products and services:
Personal data that may be collected includes name, address, date of birth, country of origin and other profile information. When collecting adverse news, RDC may include religion, political affiliation, nationality and criminal activities as necessary to assist our subscribers in meeting their regulatory obligations and properly identify the appropriate risk relevant individual.

From our subscribers:
Personal data of their users may include name, address and email address as needed to execute an agreement with RDC. Information provided to RDC by our subscribers is typically limited to name, address and date of birth.

## Does RDC collect sensitive data?

Yes, but it is limited to religion, political affiliation and nationality only as needed to identify an individual. RDC does not seek to systematically collect any information in relation to a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic or biometric data unless that information is necessary to fulfill the purpose of correctly identifying a risk relevant individual, such as would be necessary in our database of Politically Exposed Persons (PEPs)

## Does RDC collect criminal data?

Yes, as part of our adverse news products and services, RDC will collect criminal information for specific criminal categories such as fraud, bribery, money laundering, terrorism and other crimes as requested by our subscribers to meet their regulatory obligations. RDC does not curate a comprehensive criminal register.

## With whom does RDC share personal data?

RDC may share personal data in the following ways:

- Processors/Sub-Processors with whom we have entered into commercial agreements to help achieve a leading competitive position internationally in providing business information.
- Subscribers – businesses with whom we enter into agreements to license or access our data for the purpose of meeting their regulatory compliance obligations.
- Resellers – we license information to authorized resellers and third party businesses.
- Service providers – including customer support services, auditors, advisors, consultants, and contractors, to support RDCs business operations. We contractually require service providers to use personal data only for the intended purpose of disclosure, storage, data handling, processing and erasure.

## How does RDC safeguard the personal data it collects?

RDC takes the protection of personal data seriously and has protections in place to ensure the security of the data including internal data handling policies and information security policies.

## What physical access controls does RDC have in place?

RDC has established controls to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (such as databases, application servers and related hardware), where our subscriber's personal data is processed, including:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control systems (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers, etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitors, intrusion alarm systems; and
- Securing decentralized data processing equipment and personal computers.

## What virtual access controls does RDC have in place?

RDC has established virtual controls to prevent data processing systems from being used by unauthorized persons, including:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of **one** master account per user, user master data procedures, per data processing environment; and
- Encryption of archived data media.

## What data access controls does RDC have in place?

RDC has data access controls in place to ensure that persons entitled to use a data processing system gain access only to such personal data in accordance with their access rights, and that such personal data cannot be read, copied, modified or deleted without authorization by the subscriber. These data access controls include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary actions against employees who access personal data without authorization;
- Reports of access;
- Access procedures;
- Change procedures;
- Deletion procedures; and
- Encryption in transit and at rest.

## Will RDC Notify its Subscribers if There is a Data Breach?

RDC will notify subscribers within 72 hours if their information has been compromised. If a breach of GRID data occurs, RDC will notify the appropriate Data Protection Agency.

## What is RDC's data retention policy?

Personal data is stored for varying lengths of time depending on the nature and purpose for which it was collected. We store personal data in line with any applicable statutory minimum periods, and then review it annually to ensure retention is still necessary for the purpose for which it was collected. This includes adverse media, which is used to develop risk-relevant profiles. Where there may be adverse news for an associated profile, the originating article is linked. Those links are maintained until it is determined that the profile or the adverse media associated is no longer necessary for our subscribers.

## Does RDC have a Data Protection Officer?

Yes, as recommended by the GDPR, RDC has appointed a Data Protection Officer who can be reached at privacyofficer@rdc.com.

## Has RDC Staff Been Trained on the Importance of GDPR?

Yes. While data privacy and protection has always been a core tenet of RDC and an important topic during employee training, extra training regarding the significance of GDPR has been provided for all current employees and will be covered during the onboarding of new employees going forward.

## Does RDC Have a Certificate of GDPR Compliance?

No certificate of GDPR compliance currently exists.

## Why Does My Company Have to Sign an Addendum?

Any company that processes personal data from EU citizens (whether residing in the EU or abroad) are required to comply with GDPR. This includes ensuring that there are agreements between, the "Controller," and RDC as the "Processor."
Additionally, companies that have an "establishment" in the EU (including UK), is subject to GDPR regardless of the citizenship of the individuals for which personal data is collected.
The Addendum outlines the obligations of both parties relative to the privacy, protection, and security through the GDPR lens.

## Will I See Any Change to My Service With RDC?

Because RDC has always been and continues to be sensitive to the rights, protections, and privacy of the personal data we collect and that of our subscribers, you should not see any changes to the quality and performance of our products and services.

## Do RDC's Efforts Guarantee My Company's Compliance With GDPR?

No. While RDC, as a data processor, has made thorough efforts to comply with GDPR, many aspects of the law may fall under the control of the company that ultimately benefits from, and makes decisions about, the collection of personal data. You must work with your privacy officer or legal counsel to ensure compliance.

## How do I make a request to find out if my personal data is stored by RDC?

Pursuant to GDPR all individuals wishing to access their personal data that may be processed and stored by RDC should submit requests as follows:

1. Questions regarding RDC's privacy and data handling policies may contact the Data Protection Officer at privacyofficer@rdc.com
2. Any requests for information on whether or not your personal data is available through RDC products and services as well as any request for deletion or corrections to that personal data must be made by submitting this Request Form via email to GDPRRequest@rdc.com, or mailed to:

   Regulatory DataCorp, Inc
   211 S. Gulph Road #125
   King of Prussia, PA 19406

3. RDC will need to have the information required in the Request Form before we can begin our research.

4. You should receive all the information that has been located and can be released in accordance with the law, along with an explanation for any information that cannot be provided within 30 days.

5. RDC does not release information held about individuals without their consent, unless there is a legally supported reason to do so. Therefore, if information held about you also contains information related to a third party, RDC will make every effort to anonymize the information. If this is not possible, and RDC has been unable to secure the relevant consent, RDC reserves the right not to release the information.

6. Where possible, RDC will act on requests from individuals including right to erasure and accuracy of data. However, if RDC determines that retaining such personal data is necessary for its intended business purposes, RDC will provide the information and reasoning for the retention.