Data Loss Prevention (DLP) Notice to Employees

To comply with business standards and industry regulations, RGA needs to protect personal data and prevent its inadvertent disclosure. RGA's Data Loss Prevention (DLP) system is based on policy templates that are implemented across RGA's network (email, network drives, RGA Information Assets, etc.). These policy templates assist RGA in the identification of personal data and the prevention of unauthorized disclosures through monitoring the movement of personal and sensitive data.

What is considered personal data at RGA?

Personal Data is any information or combination of pieces of information that could reasonably allow an individual to be identified. It includes information that can be used to identify a person, directly or indirectly, by reference to another piece of data. It includes 'Sensitive Personal Data' that is subject to additional protections.

What is RGA's Legal Basis for processing?

It is in RGA's legitimate interest to utilize DLP technology on its network. The overall intent is to protect the confidentiality and integrity of company sensitive and personal data and consequently aid in compliance with data protection regulations and requirements, such as GDPR.

What information will be collected by RGA's DLP tool?

RGA will be collecting the following data elements via the DLP tool:

- Internet Protocol (IP) Address
- Login Credentials (Username)
- Personal Data
- Device Information
- Email Addresses

What is the purpose for the information collection?

- To prevent unauthorized disclosure of personal data
- To exercise, defend and protect our legal rights or the rights of our clients or third parties
- To comply with legal obligations and to cooperate with regulatory bodies to which we are subject

How will DLP work at RGA?

Through the combined efforts of RGA's Privacy and IT teams, a set of DLP policies have been created. These policies are designed to identify personal data contained on the RGA network, including email. DLP Policies are being developed in accordance with RGA's Acceptable Use Policy. The DLP tool will monitor data to prevent unauthorized disclosure of information. CLICK HERE to see all of RGA's current DLP Policies.

DLP for Email

Generally email is one of the easiest way to accidently send personal data outside of RGA causing an unauthorized disclosure. To enhance the protection of the personal data RGA has implemented an Acceptable Use Policy which governs the use of RGA Information Assets which includes the use of physical information assets, applications, databases, other electronic storage location and data. While RGA has implemented robust procedures and policies to protect personal data and prevent inadvertent disclosure, the DLP tool allows RGA to identify, monitor and automatically protect personal data like never before.

With whom do we share your personal information?

Your personal data is only shared internally within the RGA group of companies as necessary. We operate as a global business, so we may share your personal information with companies within the RGA group who may use this information for the purposes described in this privacy notice.

What are your rights regarding this processing activity?

You have certain rights regarding your personal information, subject to local law. These include the right to:

- access your personal information;
- rectify the information we hold about you;
- erase your personal information;
- restrict our use of your personal information;
- object to our use of your personal information;
- receive your personal information in a usable electronic format and transmit it to a third party (right to data portability); and
- lodge a complaint with your local data protection authority.

RGA has developed a Data Subject Rights portal where you can easily exercise your rights. This can be accessed by visiting https://www.rgare.com/dsr-intake

How long do we retain the information collected as part of this processing activity?

The log records will be retained for 3 years. After the expiration of the 3 years, the log records will be destroyed in accordance with RGA's policies and procedures.

Where do we process your personal information?

The DLP System Servers are located in St. Louis, London (UK), and Tokyo Data Centers. The backups are replicated to Toronto for all regions.

How do we make changes to this privacy notice?

You may request a copy of this privacy notice from us using the contact details set out below. We may modify or update this privacy notice from time to time. If we make a significant change to this privacy notice, we will notify you and, where appropriate, give you sufficient advance notice so that you have the opportunity to exercise your rights (e.g., to object to the processing).

You will be able to see when we last updated the privacy notice because we will include a revision date, shown below.

For questions regarding this notice or DLP in general, please contact dataprivacy@rgare.com.

Last updated: August 2019