reputation.com®

reputation.com®

WHITE PAPER

Preparing for the GDPR

March 1, 2018

CONTENTS:

DISCLAIMER: This White Paper is for informational purposes only. It is not intended, nor should it be relied upon as legal opinion or legal advice. This White Paper is not a substitute for obtaining professional legal advice from a qualified lawyer. We encourage you to consult with your legal counsel to discuss how the GDPR may apply to your organization and how to ensure compliance.

INTRODUCTION

Reputation.com, Inc., based in Silicon Valley, is the leading provider of Online Reputation Management services for the enterprise market in the United States and internationally. Reputation.com offers a best in class SaaS platform for review management, surveys, social media management, directory services, and business listings, along with a variety of related analytics, reporting and managed services. To learn more about our products and services please visit our website www.reputation.com.

Reputation.com is committed to protecting our customers' data and to helping our customers comply with data protection requirements. Reputation.com welcomes the GDPR as an opportunity to enhance data protection and improve transparency about its data practices and privacy. We believe that strong data protection is a critical enabler for consumer confidence, which translates into enhanced service offerings and the growth of digital commerce.

This White Paper describes the key requirements of the GDPR, how the GDPR may impact your organization, and what Reputation.com is doing to prepare for the GDPR. This paper does not prescribe policies or procedures to bring you into compliance with the GDPR. Instead, it highlights important considerations for you to weigh when you process personal data in the European Union (EU) or personal data originating from individuals in the EU. It informs you about aspects of the GDPR relevant to our business relationship. Due to the unique nature of your business you may be subject to other requirements and considerations, including requirements that apply to your particular industry and privacy laws in other jurisdictions where you collect, use, store, or transfer personal data.

THE GDPR

GDPR stands for General Data Protection Regulation. It is a new EU data protection law set to replace the existing Data Protection Directive 95/46/EC and designed to harmonize data protection and privacy laws for companies doing business in Europe. The GDPR was adopted on April 27, 2016 and goes into full force May 25, 2018 with transparency, choice and accountability at its core.

The GDPR applies to any company established in the EU as well as to those outside the EU if they "process" personal data through the provision of goods or services to EU data subjects (i.e., the individuals to whom the data relates) or monitoring their behavior (including through online tracking technologies), even if the data is stored outside the EU.

As with the current framework, the GDPR classifies companies as "data controllers" and "data processors". Data controllers collect and process personal data for their own purposes and determine the purpose and/or means of processing personal data. Data processors process personal data solely on behalf of, and as directed by, a data controller.

Reputation.com is a data processor when acting as a service provider to our customers. Our customers are data controllers for the data they submit through our services. Reputation.com is a data controller of our employees' personal data that we process as part of our human resources operations. Similarly, we are a data controller of data provided by customers to Reputation.com in connection with the purchase, sign-up, or use of our services, such as billing information and email addresses.

Both data controllers and data processors are liable for violations, which can result in steep fines of up to €20 million or 4% of global annual revenues, whichever is higher.

The full text of the GDPR can be found here. For more information, please visit the EU Commission's GDPR website at this link.

WHAT ARE THE KEY OBLIGATIONS?

The GDPR builds upon the current legal framework and retains many of its basic concepts and principles. However, it is more prescriptive in areas such as content of privacy policies, data processing agreements and consent. It also demands more from businesses in terms of accountability for their use of personal data and enhances the existing rights of individuals.

Key obligations include:

- **Transparency**: The GDPR requires data controllers to provide data subjects with detailed information about their processing operations at the time when personal data is collected, including explaining the legal bases for processing the data, third parties with whom the data may be shared, data retention periods, transfer of data outside the EU, individuals' rights.

- **Legal Basis for Processing**: As with the current framework, the GDPR requires that data controllers have a "legal basis" to process personal data. Examples include consent, necessity to perform a contract, or "legitimate interest."

- **Individuals' Rights**: Enhanced rights include strengthened rights to erasure ("right to be forgotten"), to restrict "automated decision-making" and profiling (e.g., using personal data to evaluate or predict a person's health, economic condition, interests), to "data portability" (the right to receive personal data in a way that makes it easy for individuals to move the data elsewhere).

- **Data Processing Agreements**. The GDPR is prescriptive about the clauses to be included in data processing agreements. Required terms include detailed instructions regarding the permitted processing, cooperation with fulfillment of the data controller's GDPR obligations, prior permission for engaging sub-processors.

- **Data Security**: Data controllers and processor are required to take security measures "appropriate" to the risks inherent in the processing, such as encryption.

- **Breach Notification**: Data controllers are required to notify data protection authorities of certain personal data breaches within 72 hours after having become aware of the breach. They must also notify affected individuals if the breach is likely to result in a "high risk" to their rights and freedoms. Data processors must notify data controllers without undue delay after becoming aware of a breach.

- **Privacy Impact Assessment**: The GDPR requires data controllers to conduct a Privacy Impact Assessment prior to data processing that is inherently "high risk" to the right and freedoms of individuals. In some cases, prior consultation of data protection authorities is required.

- **Record-keeping**: The GDPR requires data controllers and processors to keep detailed records of data processing, including purposes of the processing, categories of data processed, data transfers.

- **Data Protection Officer**: Data controllers and processors must appoint a Data Protection Officer in specified circumstances (e.g., large-scale, regular and systematic monitoring of individuals, or large-scale processing of sensitive data).

- **Data transfers**: GDPR carries forward the current framework's requirement to implement approved transfer mechanisms prior to transferring the data to certain non-"adequate" jurisdictions, like the United States. These include certification to the Privacy Shield framework, or implementation of standard contractual clauses approved by the EU Commission.

WHAT CAN YOU DO TO COMPLY WITH THE GDPR?

You may be already well on your way to GDPR readiness. If you are still considering the requirements or would like to ensure you have covered the keys to GDPR compliance, the following can be used as a reference:

1. Make sure that decision makers and key people in your company are aware that the current EU legal framework is changing to the GDPR and appreciate the impact on your business.

2. Conduct an inventory of and mapping all data holdings across your company or within particular business areas, and record the findings.

3. Review your public-facing privacy policies, marketing materials or other notices and update them to satisfy the GDPR's transparency requirements, including the requirement to describe the categories of service providers, like Reputation.com, with whom you share personal data.

4. Map your vendors and service providers that process personal data on your behalf and put in place GDPR-compliant data processing contractual provisions. As your service provider, Reputation.com offers a data processing addendum updated for GDPR (refer also to section "What is Reputation.com doing to prepare for the GDPR?" below).

5. Review your policies and procedures, and update them as warranted to ensure appropriate procedures are in place for responding to data subject requests.

6. Identify the lawful basis for processing activities, document it and update privacy policies to explain it.

7. Assess the risks to the personal data you hold and choose appropriate security measures.

8. Ensure appropriate processes are in place to detect, investigate, report and document data breaches.

9. Consider whether you are required to designate a Data Protection Officer and, if not required, consider whether voluntary designation is appropriate for your business.

10. Be familiar with the data that is transferred from the EU in connection with your use of our services (see section "What is Reputation.com doing to prepare for the GDPR?" below for information on how we ensure compliance with EU data transfer requirements). Ensure your data transfer mechanisms will suffice after May 25, 2018.

WHAT IS REPUTATION.COM DOING TO PREPARE FOR THE GDPR?

In a regime where customers are accountable for the data practices of their service providers, our GDPR compliance is a critical element of our business. To that end, Reputation.com integrates GDPR compliant privacy protections into our products and services, service agreements and record keeping practices to help us and our customers meet compliance GDPR obligations.

We have a robust set of security policies and procedures that are available upon request, but some of the key information includes the following:

1. **Contracts Updated for GDPR**. We have updated our service agreement to meet the requirements of the GDPR and reflect our respective roles and responsibilities with respect to data protection requirements. A copy of our updated Reputation.com (UK) Ltd. Standard Service Agreement with our GDPR Data Processing Addendum may be found at this link.

2. **We are Certified to Privacy Shield**. We are certified to the EU-U.S. Privacy Shield framework, which ensures that we can transfer personal data outside the EU in compliance with the GDPR's data transfer requirements and helps customers legitimize transfers of personal data. You can see our certification on the U.S. Department of Commerce's Privacy Shield website at this link.

3. **Use of Customer Personal Data**. We only process customer Personal Data as a Processor on behalf of and in accordance with our customer's' prior written instructions and as necessary to provide our services in accordance with our service agreement.

4. **Data Portability**. The GDPR includes certain requirements on data controllers for the portability of personal data. The data that our customers provide or that we otherwise receive in connection with our Services provide belongs to our customers. We provide for portability and are continually working to enhance the robustness of our data export capabilities.

5. **Deletion of Customer Personal Data**. The Company will permanently and securely delete (or, at the election of the Customer, return, in such format as Company may reasonably elect and subject to the Customer paying all of Company's

fees at prevailing rates, and all expenses, for transferring the Customer Personal Data to such format) all Customer Personal Data in the possession or control of Company or any of its sub-Processors, within 90 days after Company ceases to provide the Services, unless the applicable law of the EU or of an EU Member State requires otherwise. Company will procure that its sub-Processors do likewise.

6. **Confidentiality**. We require all employees and contractors with access to personal data to sign confidentiality agreements. We also require all employees to go through a background check and a reference check before they are hired.

7. **Appointment of Sub-Processors**. We engage sub-processors to help processing personal data only in accordance with our service agreement and GDPR Data Processing Addendum.

8. **Security Measures**. The GDPR requires processors to implement appropriate technical and organisational measures to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to customer personal data. Data security has been and will continue to be a high priority for us.

   Some of the key security measures that we employ include:

   a. **Platform and Storage is Secure**. Our SaaS reputation Management platform and all customer data is stored on secure servers at Amazon Web Services. The AWS cloud infrastructure has been designed and is managed in alignment with key security and best practices, including, but not limited to: ISO 27001, SOC 1/SSAE 16/ISAE 3402(formerly SAS70); SOC 2, SOC 3, PCI DSS Level 1, FedRAMP(SM), DIACAP, FISMA, ITAR, FIPS 140-2, CSA, and MPAA. *Note: A copy of the AWS certification under ISO 27001 is available upon request.*

   b. **Personal Data is Encrypted at Rest**. Personal Identifying Information is encrypted in the Reputation Management Platform and in related databases using Advanced Encryptions Standard (AES) algorithms.

   c. **Data in Transit is encrypted**. Data in transit to and from the platform is strongly encrypted using proven, standard protocols and algorithms.

   d. **Password Security**. We securely encrypt your passwords. Passwords are one-way encrypted using the bcrypt algorithm, with a random salt for each password. This means that only the original creator of the password knows its value. When passwords must be retrieved, public/private key encryption is used, with a key length of 4096 or greater. Access and retention of passwords are strongly controlled and logged.

   e. **Regular Penetration Testing**. The Reputation.com website and platform undergo quarterly penetration by an independent third party security consultant.

   f. **Credit Card Information**. Reputation.com does not store credit card numbers and security information. In the event that an enterprise uses a credit card to purchase a service, the credit card number is immediately encrypted and turned into a secure token by our credit card processing company. We only store the secure token on our systems.

   g. **No Sensitive Information Collected or Stored**. We do not collect or store sensitive information such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. We also do not collect or store personal financial data, Social Security Numbers, National Insurance numbers, government-issued ID numbers.

   h. **Security Breach Reporting**. We have processes in place to quickly notify you of any security incidents involving personal data. We will provide you with reasonable assistance necessary to help you meet GDPR obligations.

For more information on Reputation.com's security policies and procedures, please ask your sales representative or customer success manager.