Clarivate Analytics
GDPR Readiness Programme

On 25th May 2018, the EU General Data Protection Regulation (GDPR) replaces the existing 1995 EU Data Protection Directive (European Directive 95/46/EC). The GDPR will impact the way companies process EU personal data, including Clarivate Analytics (Clarivate) and its customers.

Clarivate is committed to taking the steps necessary to be in compliance with the GDPR. Over the last year, we have implemented a GDPR Readiness Programme to ensure adherence with this new regulation and support our customers' own GDPR compliance.

Below are some answers about what the GDPR means and how we have been preparing for this legislation. If you have any questions about our data privacy and security policies in general, please contact us at: data.privacy@clarivate.com

1. What does the GDPR require?

The GDPR establishes rules for how organizations can process the personal data of data subjects who are in the European Union. While many of these rules already existed under previous EU law, some rules are now stricter. The rules reach beyond the physical borders of the EU and apply to any organisation, regardless of whether it has a physical presence in the EU, if it offers goods or services to people in the EU, or if it tracks the behaviour of those people.

2. How is Clarivate preparing for the GDPR?

Since early 2017, Clarivate has been preparing for the GDPR with a formal compliance project headed by our Chief Compliance Officer. Much of the preparation is happening behind the scenes but a number of initiatives will be visible to our customers. Listed below are some of the steps we have taken:

- **Assessment**: We have carefully reviewed where and how our relevant services collect, use and store personal data and we are updating procedures policies, standards, governance and documentation as needed.

- **Products**: We are evaluating potential new features to add to our various products to assist our customers in meeting various GDPR compliance obligations, such as notice and consent requirements, if necessary.

- **Cross-Border Transfers of EU Personal Data**: Cross-border transfers of personal data will occur in relation to some of our products. In addition to ensuring our contractual commitments meet the GDPR requirements, Clarivate has standard contractual clauses in place where necessary.

- **Employee Training and Awareness**: Our employees will receive training on GDPR-specific content. In addition, Clarivate will conduct ongoing awareness initiatives on a variety of topics, including data protection, security and privacy.

3. What is the difference between a controller and a processor?

If you access personal data, you do so as either a controller or a processor, and there are different requirements and obligations depending on which category you are in. For this reason, it is important to understand whether you are acting as a controller or a processor, and to familiarize yourself with your responsibilities accordingly.

A controller is the organization that determines the purposes and means of processing personal data as well as the specific personal data that is collected from a data subject for processing. A processor, on the other hand, is the organization that processes the data on behalf of the controller. The GDPR has not changed the fundamental definitions of controller and processor, but it has expanded the responsibilities of each party. Controllers will retain primary responsibility for data protection (including, for example, the obligation to report data breaches to data protection authorities); however, the GDPR does place some direct responsibilities on the processor, as well.

4. When does Clarivate act as a processor?

Clarivate is only a processor in relation to certain products and only in limited circumstances. For instance, in the context of our hosted software products, such as ScholarOne and Converis, our customers act as the controllers, and Clarivate acts as the processor. We also occasionally act as processors in relation to non-software services and products, such as when Web of Science Author Connect (WoSAC) customers supply us with a contact list (also known as a suppression file) or when publisher customers provide us with reviewers' personal data for use with Publons. Please contact us if you are in doubt whether or not we are processors in relation to the Clarivate product you subscribe to.

5. How will Clarivate help my company comply with the GDPR?

When acting as processors, we will only process your personal data in accordance with your instructions and we have a duty to inform you if we reasonably believe your instructions infringe upon the GDPR requirements, or other European Union or Member State data protection legislation. However, we will have no responsibility for the accuracy and the quality of the personal data that is supplied to us.

As controllers, our customers have a number of GDPR obligations to data subjects, such as expanded data privacy rights, data breach notification, and more robust consent requirements. We are committed to helping our clients comply with the GDPR and are working to enhance our products and services to support Clarivate's and our clients' GDPR compliance. We will assist as required and when we are best placed to take a particular compliance measure.

6. How will Clarivate assist my company in fulfilling data subject rights?

We will promptly notify a customer if we receive any requests from a data subject to exercise their rights, including, without limitation, rights relating to access, rectification, restriction of processing, objection to processing, data portability (if applicable), and erasure. To the extent reasonably possible and legally permitted, we will assist customers in fulfilling their obligations to respond to a data subject request under applicable data privacy legislation.

7. Who can access personal data that Clarivate processes on behalf of its customers?

We may permit our employees, contractors (including the employees and contractors of our affiliates) and authorised sub-processors to access personal provided that they are bound by confidentiality covenants and only to the extent that they need access to perform services for our clients.

8. How does Clarivate manage sub-processors?

We will obtain general written authorisation from our clients in the relevant data processing agreement before transferring their personal data to a sub-processor. We will inform our clients of any changes in authorised sub-processors. Further, we will bind our sub-processors contractually to provide sufficient guarantees to implement technical and organisational measures in compliance with the GDPR, and we will remain liable for their acts and omissions.

9. Does the GDPR prevent a company from storing data outside of the EU?

The GDPR does not introduce new restrictions on the transfer of EU personal data nor does it prevent transfers of EU personal data outside of the EU as long as the processors adhere to the necessary data protection regulations and safeguards.

10. Which safeguard mechanisms does Clarivate adhere to when transferring data outside of the EU?

Where a client supplies us with EU personal data to one of our entities located outside the EU, or when one of our entities based in the European Union uses an affiliate or a third-party outside the EU as a sub-processor, we use Standard Contractual Clauses (SCCs). The European Commission drafted and approved the SCCs, which contain detailed obligations related to the transfer and protection of personal data.

The SCCs will not, however, apply to every data transfer outside the EU. For instance, in relation to EU-US transfers, SCCs are not required when the sub-processor has adhered to the EU-US Privacy Shield framework. Equally, for countries that the European Commission has ruled to offer an adequate level of protection in relation to personal data, no additional safeguards such as the SCCs are required.

11. How long does Clarivate keep personal data?

At the end of a contract for services, upon a client's request, we will return or securely destroy personal data. This is subject to any limitations described in the relevant data processing agreement between us and our customers as well as any restrictions prescribed by law that prevent us from returning or destroying such personal data. Clients may delete individual or organization-level personal data by using available features in the Clarivate products and/or services, or by contacting us.

12. How does Clarivate ensure the security of Client Personal Data?

At Clarivate, we implement and maintain many processes to ensure that Client Personal Data is kept secure. For instance, some of the measures we take include, but are not limited to:

I. Compliance Programme: Ongoing data protection compliance programme for ensuring adherence with applicable legislation.
II. Security: We have robust security measures in place to ensure the resilience of our networks and we have processes in place to track data and flag data breaches.
III. Restricted Processing: We only use Client Personal Data to provide the services our clients request and subject to confidentiality covenants.
IV. Training: We ensure that personnel who process Client Personal Data have the necessary awareness in data protection and data security through training.
V. Verification: We screen both employees and prospective vendors and we monitor existing vendors to ensure their integrity and compliance with applicable data protection laws and contractual obligations.

13. How does Clarivate handle data breaches?

Clarivate uses industry-standard technologies and processes to monitor the IT systems supporting our products and services against security breaches. Suspected breaches are escalated internally according to established procedures. Clients who are controllers will be notified in the most expedient time possible, consistent with steps to investigate, verify, and establish the scope of the breach. Pursuant to the terms of the relevant data processing agreement, Clarivate will cooperate with such clients to notify regulators and data subjects as required by applicable law.

14. How will the GDPR impact Clarivate's marketing activities?

Clarivate has updated its marketing practices and procedures by implementing a new marketing policy in line with GDPR requirements. This new policy, which incorporates key data privacy principles, sets out clear and strict rules about how personal information should be collected/acquired and used for marketing purposes. As well as ensuring that our workforce receive appropriate training on our new policy, we will continue to promote and monitor their adherence with these new rules.

15. Does Brexit have any immediate effect on how companies in the UK must or need not be GDPR-compliant?

Once Brexit is final, the GDPR will not have any immediate authority in the UK. However, the Information Commissioner's Office (ICO), the British data protection authority, is working on legislation referencing the GDPR. At this point, it seems likely that companies within the UK will still be under this legislation or a very similar one.