GDPR – external briefing

TABLE OF CONTENTS

What is GDPR?

The General Data Protection Regulation (or GDPR) is a piece of legislation that was passed in the European Union (EU) in May 2016. It was passed with a 2 year lead in period, and came into full effect on 25 May 2018.

GDPR updates and replaces the European Data Protection directive of 1995 and the related Data Protection laws passed in individual EU territories. It is designed to reflect technological and social changes in the intervening period and strengthen the rights of individuals using social media, online financial services and so on, in the face of new techniques such as biometrics and profiling. Because it's a regulation rather than a directive, it automatically applies across all 28 (then 27) countries of the EU, and supersedes local laws (though individual member states are allowed to pass complementary local laws to further strengthen certain aspects of the regulation).

What about the UK?

The UK officially left the EU on 31 January 2020. Under the provisions of the Withdrawal Agreement, current rules on trade, travel and business for the UK and the EU continue to apply for the duration of the transition period, due to end on 31 December 2020. New rules will take effect from 1 January 2021.

The EU Withdrawal Agreement Act of 2020 effectively converted EU law, including the GDPR, as it stood at the moment of exit into domestic law, so at present UK privacy law remains entirely aligned with the GDPR. Nevertheless, the EU privacy commission will need to recognize the UK as a "safe third country" for data transfers from the EU; if this is not achieved as part of the negotiations during the transition period, there could be restrictions or requirements for additional protections on personal data transfers from the EU to the UK. Mediaocean has addressed this by ensuring that we have Standard Contractual Clauses signed to cover any personal data transfers to the UK office or to UK data centers and service providers.

What are the main requirements of GDPR?

First of all, please note that unlike the old Data Protection rules it replaces, GDPR explicitly applies to companies outside the EU who handle EU citizens' data. GDPR also introduces tighter rules about breach notifications in the event that personal data is compromised, and higher fines for companies breaching GDPR principles or failing to adequately protect personal data.

The principles of GDPR are that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit, legitimate purposes (purpose limitation).
- Adequate, relevant and limited to what is necessary (data minimization).
- Retained no longer than necessary (storage limitation).
- Protected using appropriate technical or organizational measures (integrity & confidentiality).

Individuals in the EU have the following rights over their personal data:

- Right to be Forgotten – i.e. request their data to be erased – UNLESS there is another legal requirement which means the data has to be retained (for example, as part of a company's financial records, or as part of a bank's anti-fraud reporting).
- Right to Rectification – i.e. request inaccuracies to be corrected.

- Right to Data Portability – i.e. request their data be moved to a different platform or provider e.g. bank or social media site.
- Right to Object/Restrict – i.e. to ask the data controller to cease processing & destroy their personal data, or stop using it while legal proceedings are going on.

What personal data does Mediaocean process?

The definition of "personal data" under GDPR is very broad. Any information relating to an individual resident in the EU that can identify the individual counts as personal data, including business contact information. GDPR also includes new data elements in the definition – for example location data & online identifiers such as IP addresses, mobile phone identifying numbers, Google IDs, geolocation data and so on.

Under this definition, there are two categories of personal data that Mediaocean processes:

1. Data we process in Aura, Prisma, Spectra DS & Lumina for our clients in the EU – business contact information, user credentials, audit trail information, expense claims & payment information for agency staff etc.
   Please note: in the case of all information that Mediaocean processes in these systems, we will act solely on the instruction of our clients. If you are a user at a client company, and you have queries or concerns about the information held about you in these systems, please refer to your company HR policies on data protection in the first place.
2. Data we collect about our EU users in our internal contact databases, so that we can provide support, updates and training about our systems, in accordance with service agreements with our clients- business contact information, issue tickets, voice recordings of phone calls, training records, stats about users of our support services and so on.

Please refer to our privacy policy for more details about how & where we process this data.

Mediaocean's GDPR program

Mediaocean's privacy program ensures compliance with the requirements of GDPR and includes the following:

- Regular review of the privacy policy and associated privacy notices.
- Maintenance and regular review of a register of personal data processing.
- Data Protection Impact Assessments and Legitimate Interest Assessments.
- Privacy and security awareness training for all new hires with annual refreshers as part of a certification program for all staff.
- Vendor management procedures, to ensure that contracts are in place to govern relationships with vendors who process personal data for Mediaocean, and that the performance of these vendors is monitored for compliance with the defined requirements.
- Procedures to ensure that cross-border transfers of data are adequately safeguarded, for example through the use of the Privacy Shield scheme and/or the EU's Standard Contractual Clauses.
- Privacy Incident response and escalation procedures.
- Regular privacy audits.

What if I have a query or a complaint?

As we state in our privacy policy, we commit to resolve complaints about privacy and our collection or use of personal data. If you have inquiries or complaints regarding the handling of personal information, please first contact your support team in the usual way. If the complaint is not resolved to your satisfaction then please email Infosec&Compliance@mediaocean.com.