CLIENT ALERT:

UNDERSTANDING THE GDPR

2550 M Street, NW,
Suite 300
Washington, DC 20037
www.lmiadvisors.com

The European Union ("EU") will shortly implement changes to its data protection policies. Its revised data protection regime – the General Data Protection Regulation ("GDPR") – harmonizes data protection law across the EU without the need for national implementation (although it does permit individual EU Member States to enact national legislation addressing specific situations). In general, the GDPR covers organizations with headquarters, operations, or affiliates in the EU, or that offer goods or services to individuals in the EU or monitor their behavior (including tracking activities online), regardless of where the organization is located or where the data processing takes place. Many organizations that are not subject to existing EU data protection law will be subject to the GDPR, including satellite service providers, so understanding the GDPR is important.

ESSENTIAL ELEMENTS OF THE GDPR

GDPR Principles. The GDPR provides that personal data shall be: (i) processed lawfully, fairly, and in a transparent manner; (ii) collected for specified, legitimate purposes and not further processed in a manner that is incompatible with those purposes; (iii) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed; (iv) accurate and updated, where necessary; (v) kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed; and (vi) processed in a manner that ensures appropriate security of the personal data to maintain integrity and confidentiality. The GDPR also provides that organizations collecting and processing personal data shall be accountable for compliance with the foregoing principles.

The GDPR Applies to Personal Data and Sensitive Personal Data of Natural Persons. Personal Data is information relating to identified or identifiable individuals, including name, identification number, location, online identifier, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity. Sensitive Personal Data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life and sexual orientation, and genetic data or biometric data information. These are subject to additional protections and organizations need even stronger grounds to collect and process this data.

Lawful Bases for Processing Personal Data. Processing of personal data is lawful only if:

- the individual consents to data processing for one or more specific purposes;
- processing is necessary for entering into, or performing, a contract with the individual;
- processing is necessary to comply with a legal obligation under EU or Member State law (*e.g.*, compliance with employment, social security, or social protection laws);
- processing is necessary to protect the life of a person who is incapable of giving consent;
- processing is necessary to perform tasks carried out by a public authority or private organization acting in the public interest; or
- processing is necessary for an organization's legitimate interests or the legitimate interests of a third party.

Data Processors and Controllers. The GDPR applies to data Controllers and Processors. A Controller determines the purposes and means of collecting/processing/storing personal data. A Processor is responsible for processing personal data for or on behalf of a Controller and does not decide how the personal data will be used. All organizations are likely to process at least some personal data as Controllers, even if only in relation to their own employees.

Controllers are responsible for complying with all of the regulations in the GDPR in regard to the personal data that is processed on their behalf. This includes observing the principles of the GDPR, maintaining a lawful basis for processing personal data, ensuring that all the rights of the data subjects are protected, and establishing procedures for reporting breaches.

Processors must: (i) identify the data processing activities for which they are Processors; (ii) maintain a written record of processing activities carried out on behalf of each Controller; and (iii) ensure that they have appropriate processes and templates in place for identifying, reviewing, and promptly reporting data breaches to the relevant Controller.

Satellite-based broadband providers are not subject to the GDPR when processing non-personal data of businesses or entities. However, the provision of broadband data and Internet access services directly to individual consumers will likely be subject to all the obligations of a Controller (*e.g.*, to obtain the consent of users, to inform them of their rights, to ensure the accuracy of their data, etc.). In addition, third-party data processing agreements that facilitate the provision of multi-country, satellite-based services are likely to become more complex as Processors become more careful about agreement terms and the scope of the Controller's contract rights.

Data Subjects' Rights. The GDPR establishes rights of data subjects, which include:

- Right to Access: Controllers must provide data subjects with access to their data.
- Right of Rectification: If requested, Controllers must rectify any errors in personal data.
- Right to Erasure (the "right to be forgotten"): If requested, Controllers must delete data subjects' personal data if the continued processing of those data is not justified.
- Right to Restrict Processing: If requested, Controllers must limit the purposes for which they process data (*e.g.*, exercising legal claims, protecting rights of others, purposes that serve a substantial public interest, or such other purposes as the data subject consents).
- The Right to be Informed: Individuals have a right to be provided information on the identity of the Controller, the Controller's reasons for processing their personal data, the recipients with whom the data may be shared, etc.
- Right to Object to Processing for Scientific, Historical, or Statistical Purposes: Personal data may be processed for scientific, historical, or statistical purposes in the public interest, but individuals have a right to object to such processing.
- Right to Object Generally: Controllers must inform individuals of their right to object.
- Right not to be Evaluated on the Basis of Automated Processing: Individuals have the right not to be evaluated solely on the basis of automated processing of personal data.
- Right to Object to Processing for the Purposes of Direct Marketing: Individuals have the right to object to the processing of their personal data for direct marketing.
- Right of Data Portability: Individuals have the right to transfer data between Controllers.

PREPARING FOR COMPLIANCE

GDPR will be enforced beginning May 25, 2018. Satellite service providers should understand how the GDPR will affect their organizations and identify areas that could cause compliance problems. Companies should ensure that employees who process personal data are appropriately trained, so that they can quickly recognize, and appropriately respond to, GDPR compliance risks, including requests from data subjects to exercise their rights. The organization's compliance processes should also cover the personal data of its employees in EU Member States, which, like that of customers who are natural persons, is also subject to the GDPR.

GDPR Compliance Measures. To the extent not taken already, satellite service providers and other organizations subject to the GDPR should consider steps aimed at compliance, including:

- Document the Collection and Handling of Personal Data. An information audit will identify where/how personal data is collected, processed, stored, and shared. Such an audit will also aid in the completion of a GDPR compliance risk assessment and establishment of effective policies and procedures to mitigate these risks.
- Determine the Lawful Basis for Collecting, Processing, and Retaining Personal Data. Each of the lawful bases for processing data (noted above) are associated with certain obligations imposed by the GDPR, which should be understood by the organization.
- Obtain Appropriate Consent. When the lawful basis for data processing is consent, an organization should ensure that the consent is freely given, specific, informed, unambiguous, properly documented, and easily withdrawn. Consent cannot be inferred from silence, pre-ticked boxes, or inactivity; or tied to other terms and conditions. Individuals generally have more rights where consent is the basis to process their data.
- Provide Information to Data Subjects. The GDPR requires organizations to provide certain information to a data subject, whether the data are obtained directly from an individual or from a third party. The information must be provided in concise and clear language.[1]
- Implement Mechanisms to Access, Correct, Delete, and Update Personal Data. Subject organizations should: (i) review the length of time personal data is kept, considering the purposes for which information is held in deciding whether and for how long to retain it; (ii) securely delete information that is no longer needed for these purposes; and (iii) take reasonable steps to ensure the accuracy of any collected personal data.
- Implement Mechanisms to Respond to Requests. Organizations will have one month to comply with requests from data subjects to exercise their rights to data access, data correction, data erasure, or data porting.[2]

---

[1] The information to be provided includes: (i) the identity and contact details of the data controller, and of the data protection officer, where applicable; (ii) the intended purposes and legal basis for the processing; (iii) the recipients or categories of recipients of the personal data; (iv) where applicable, the fact that the personal data will be transferred to a third country or international organization and the legal basis for doing so; (v) the period for which the personal data will be stored; and (vi) the data subjects' rights in regard to their data.

[2] The right to data portability is new and only applies: (i) to personal data an individual has provided to a Controller; (ii) where the processing is based on the individual's consent or for the performance of a contract; and (iii) when processing is carried out by automated means. Personal data provided to an

Data Breaches Under the GDPR. Organizations implement procedures to effectively detect, report, and investigate a personal data breach. Organizations should assess the types of personal data held and document where they would be required to notify the national data protection supervisory authority or affected individuals if a breach occurred.

The GDPR introduces a duty on all organizations to report certain types of data breach to the applicable supervisory authority, and also to individuals, if the breach is likely to result in a risk to their rights and freedoms (*e.g.*, if it could result in unlawful discrimination, damage to reputation, financial loss, loss of confidentiality, etc.). Failure to report a breach when required to do so could result in a fine in addition to a fine for the breach itself.

Data Transfers to Third Countries. The GDPR authorizes the transfer of personal data to third countries if: (i) an "adequacy decision" has been made by the Commission for the destination country; or (ii) the transfers are subject to "appropriate safeguards," which includes a requirement that the transfers are made in accordance with binding corporate rules approved by a competent national supervisory authority. Otherwise, transfers to third countries may take place only if the transfer meets one of the following conditions:

- the individual has explicitly consented to the proposed transfer, after having been informed of the possible risks involved in such transfers;
- the transfer is necessary for the performance of a contract between the individual and the Controller or implementation of pre-contractual measures taken at the individual's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the Controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise, or defense of legal claims;
- the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
- the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person with a legitimate interest, but only if the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

individual or ported to a different Controller must be structured in a commonly used and machine-readable format free of charge.

Sanctions for Non-Compliance. The consequences for non-compliance with the GDPR are significant. The national supervisory authority and each EU member State is required to impose sanctions and administrative fines in a manner that is effective, proportionate and dissuades non-compliance. Fines for serious infringements may be imposed up to a maximum of €20 million or four percent of worldwide turnover for the preceding financial year.[3]

Useful Links. The following links provide additional guidance regarding the GDPR:

GDPR portal:
https://www.gdpr-portal.com/resources/#links

Complete version of the regulation:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Guide from the UK data protection regulator:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Questions and Concerns. If you have any question and/or concern about the application of the GDPR to your specific circumstances, please feel free to contact LMI Advisors:

Dennis Burnett: dburnett@lmiadvisors.com

Richard Cameron: rcameron@lmiadvisors.com

Lucie Rivière: lriviere@lmiadvisors.com

[3] Factors affecting sanctions include: (i) the nature, gravity and duration of the infringement; (ii) the number of data subjects affected and the level of harm suffered; (iii) the intentional or negligent character of the infringement; (iv) any action taken by the Controller or Processor to mitigate the harm; (v) any relevant previous infringements; (vi) the degree of cooperation with the relevant supervisory authority; (vii) whether the infringement was self-reported by the Controller or Processor; and (viii) any other aggravating or mitigating factors.