An Approach for US Companies to the GDPR

A. Do you process the personal data of EU subjects?

"Personal data" means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

"Processing" means any operation(s) performed on personal data, or sets of personal data whether or not automated.

As is apparent from these definitions, practically anyone with a business relationship, or who may explore a business relationship which involves even the slightest exchange of identifiable data, likely processes personal data. If you do these things, then you are within the "material scope" of the GDPR.

If you process personal data of EU subjects, you do so in one—or both—of two statuses under the GDPR—either as a "Controller" or as a "Processor". "'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." "'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller of Subject Data."

B. Are you within the territorial reach of the GDPR?

In Article 3, the GDPR expressly expands the territorial reach of its asserted jurisdiction beyond the prior data protection Directive. The Directive focused, generally, on entities with a legal establishment in an EU member country as broadly interpreted by the Court of Justice of the European Union. Article 3 states three bases for assertion of the regulations territorial reach.

(1) Article 3.1 repeats the establishment language of the former Directive as the first basis for territorial jurisdiction.
(2) Article 3.2 provides the new, "offering goods and services", and "monitoring behaviour" language.
(3) Finally, Article 3.3, provides for coverage where the controller is not "established" in the Union but is otherwise subject to Member state law.

This expansion, through case law under Article 3.1, and the new language in Article 3.2, has properly generated a significant amount of attention and concern because of the consequences of coverage.

Art. 3.1 states:

> "This Regulation applies to the processing of personal data in the context of the activities of an *establishment* of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

The concept of establishment is, thus, broad, capturing all processing by an "establishment" in the EU, whether or not the processing occurs in the EU. The concept of "establishment" rests on effective, practical business activity, without regard to the technical legal relationships between the participants. The "in the context of the activities of" language creates this breadth. The applicable comment states: "Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

Reading this literally, a participant of a regular, substantial business relationship could be found to be part of an establishment in the EU, even where the participant is outside the EU and the entities are legally unconnected. By operating in the "context of the activities of an establishment of a controller or processor" in the union, jurisdiction may be asserted under the regulation.

As stated, the concept of what constitutes an establishment has been broadened considerably by decisions of the Court of Justice of the European Union (CJEU). Two cases which have addressed this issue under the language of the former Data Protection Directive are the *Google Spain* and *Weltimmo* cases.

In *Google Spain*, Google Spain was found to be processing data in the context of the activities of Google, Inc., the U.S. parent, even though the processing at issue was not performed by Google Spain. Under an economic linkage theory, the context of the activities of Google Spain included Google Inc., and contributed to the profits of Google Inc. The *Weltimmo* case affirmed *Google Spain* in a case which sorted which EU Member State's regulators might proceed with enforcement. On this point, the Court observed that the "concept of establishment" captures any real and effective business activity, even if it is minimal, so long as it is exercised through "stable arrangements".

Under Article 3.1 U.S. companies must look not just to their direct and subsidiary's activities in the EU, but also their stable contractual affiliates and partners to ascertain whether they act

“in the context of the activities of an establishment of a controller or a processor in the Union”. Very minimal activities and/or presence may be sufficient to meet the concept of establishment.

Article 3.2 will be pertinent to many US entities, with neither an establishment in the EU (Article 3.1 GDPR) nor otherwise subject to EU Member State Law (Article 3.3 GDPR). It states:

> “This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
> a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
> b) the monitoring of their behaviour as far as their behaviour takes place within the Union.”

Jurisdiction turns, thus, on the requirements that the “processing activities” be “related to” the circumstances described in paragraphs (a) or (b).

Under (a) what does it mean for “processing activities” to be related to “the offering of goods or services… to such data subjects in the Union”? Recital 23 to Article 3.2 (.a)-(b) GDPR, offers a starting point for answering this question by using the word target—as in marketing—as a measure :

> "Applicable to processors not established in the Union if data subjects within the Union are targeted*
> ……..
> In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.
>
> Whereas the mere accessibility of the controller’s, processor’s or an intermediary’s website in the Union, of an email address, or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.”

Although the comment begins with the term “target”, it turns to the word “envisage” in the body of the recital. Numerous commentators have formulated statements interpreting Article 3.2. There is not clarity under this section.

Wiley Rein states: "Article 3(2) appears to adopt a sliding scale approach as opposed to a bright-line rule, and there is little guidance so far on how to interpret this provision." (emphasis added) (May 2017).

A helpful guide, is, however, an EU trade case (*Pammer v. Schluter* (C-585/08). *Pammer* considered the question whether or not a trader's activities were directed at EU Member State citizens in the context of internet marketing of international travel (carriage on a freighter). In this respect, direction of marketing is a proxy for the GDPR words, "offering", "targeting", or "envisaging".

Indeed, it appears the *Pammer* analysis was lifted from the case into Article 3.2, and in part, Recital 23. Under Pammer, the following factors would indicate marketing *directed to* an EU subject, potentially satisfying Article 3.2.a—use of member state language or currency, use of a Member state top level domain, marketing content referencing Member State customers, or marketing specifically targeting Member State customers.

While these factors are helpful in the context of internet marketing, much room remains to argue both sides of the issue. At present, a company not clearly beyond or within the regulation's territorial reach will have serious decisions to make about how to behave under the regulation because of this section. A careful examination of a company's activities which result in receipt of EU subject personal data will be crucial to this decision.

C. <u>If you are within the GDPR what does it require?</u>

As Controller and Processor, you must implement Data security by design

Article 32 requires Controllers and Processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, such as: pseudonymisation and encryption of personal data, the ability to ensure the confidentiality of the processing system, the ability to restore timely access to lost data due to a physical or technical incident, a process for testing and evaluating the effectiveness of the processing security systems. The risk of accidental or unlawful destruction, loss, alteration unauthorized disclosure of data must be considered in assessing the proper security level to be applied. Under Art. 32.4, the controllers and processers are responsible for ensuring persons acting under their authority do not process data in an unauthorized way.

Verify Lawful Processing

Controllers and Processors must purposefully consider the lawfulness of their data processing. Recital 40, states:

> "In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation..."
> Put simply, if the purpose of the contemplated processing is not permitted, then it is not lawful.

Article 6.1.a-f states the conditions of lawful processing, and requires that at least one of numerous conditions apply before the processing is allowed. A summary of the primary conditions for lawful processing are:

> a) the data subject has given consent to the processing of his or her personal data;
>
> b) processing is necessary for the performance of a contract to which the data subject is party;
>
> c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;"
>
> e) processing is necessary for the performance of a task carried out in the public;
>
> e) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party...

Where consent and/or the performance of a contract is the basis of the processing, additional considerations affecting the processing come into play. Specific conditions of consent are provided in Article 7. In short, the burden of proof is on the Controller to demonstrate consent by the subject for the data processing. Some data is sensitive, and subject to further requirements. Under Article 8, data subjects must be of a minimum age to give valid consent for processing of their data, or consent is required from the "holder of parental responsibility over the child". Processing involving some sensitive data, e.g., health data, union membership, political opinions, racial or ethnic origin, etc., is prohibited by Art. 9.1, absent an enumerated exception allowing such processing. Examples of the exceptions include "explicit consent" by the subject, the subject has "manifestly" made the information public, and/or for public health reasons. Processing of data involving criminal convictions and offences may only occur "under the control of official authority." Article 10.

Adopt the Required Approach to data subjects (Article 12)

Businesses must adopt a very specific approach to data subjects in their dealings with them. These requirements are provided, principally, in Article 12.

Article 12.1 requires the Controller to take measures to provide information concerning the processing of the data subject's data and a breach of data, to the data subject. These duties compel development and implementation of distinct form making, record keeping and business processes, and communications capability. It also requires the information provided data subjects be clear and plain. The information must be in written form, or if requested by the data subject may be supplied orally.

Article 12.2 requires the Controller to facilitate the exercise by the data subject of all rights conferred under Articles 15 to 22.

Under Article 12.3, the Controller is required to respond to requests under Articles 15-22 "without undue delay," and within one month of receipt of the request, at the most. Extensions are available but at further administrative cost.

Under Article 12.4, should the Controller not take action on a data subject's request, the Controller must inform the data subject "without delay," and no later than a month of the request why no action is occurring on the request and the data subject's option to lodge a complaint with the "supervisory authority" and to seek a "judicial remedy."

Article 12.5 requires, with limited exception, that responses under Articles 13-22 must be provided "free of charge."

Article 12.7-8 authorizes presentation of requested processing information concerning data subjects to them in standard ways, depending on where the information concerning the data subject was obtained. Different, but similar notices to data subjects are provided under Article 13 (where the personal data was collected from the data subject) and Article 14 (where the personal data was not obtained from the data subject).

Provide Notices to Data Subjects

The GDPR requires very specific notices be given by the Controller to data subjects. The precise content of the notices is differentiated by the source of the personal data being processed, that is, whether the data is supplied by the subject or is obtained elsewhere by the controller. In total, Articles 13 and 14 provide almost two dozen different specific notices which must be provided to data subjects, and requirements for when the notices must be provided.

Establish GDPR-Conforming Response Capabilities

Article 15-22 list and describe the rights of data subjects and the corresponding duties of a Controller arising from the data subject's rights.

Article 15 provides the data subject the right of access to the data. In addition to the right to demand the information required to be noticed to the subject under Articles 13 and 14, the Controller is required

to supply the data subject with a "copy of the personal data undergoing processing. If the information is requested electronically the information "shall be provided in a commonly used electronic form."

Article 16 provides the data subject the right to "rectification." This requires the Controller to provide, "without undue delay" the rectification of "inaccurate personal data concerning him or her. This includes the right to have "incomplete personal data completed," and a means for supplying a "supplementary statement." Controllers making corrections must pass corrections down the line, to subsequent receivers, so that where practicable everyone in a chain is advised of the correction. Art. 19.

Article 17 sets out the data subject's right to be "forgotten." Article 17.1 allows the subject to demand and obtain from the Controller "erasure" of the personal data concerning the person. Erasure must occur "without undue delay." With limited exceptions, the Controller is further obliged to erase personal data without undue delay under additional circumstances, including where the data are no longer necessary for the purposes for which collected or processed, the subject withdraws consent and no other grounds allow processing, unlawful processing has occurred, or Member State law required erasure.

Pursuant to Article 18, a data subject may restrict processing of his/her personal data under certain circumstances. Circumstances allowing a subject to restrict processing include when the accuracy of the data is contested (to allow correction/verification of the data), the processing is unlawful, when the Controller's need for the data is ended but the data subject needs the personal data for legal purposes, and when the data subject has properly objected to the processing (to allow assessment of the legitimacy of the objection). Once restricted, personal data processing may only be performed with subsequent consent of the subject, or in connecting with other legal needs or public interests.

Article 19 requires the Controller to communicate any rectification, erasure or restriction of processing undertaken under Articles 16-18 as to every recipient to whom the data have been disclosed. This is not required if impossible or if it would involve disproportionate effort. If the data subject asks, the Controller must identify recipients of the data to the data subject.

Under Article 20, if the data processing is based on consent or a contract, and the processing occurs by automated means, data subjects have the right to receive the personal data about them in a structured, commonly used and machine readable format. Data subjects may transmit those data to another Controller and may require the Controller to transmit the data directly to another Controller when technically feasible.

Demonstrate "Compelling Grounds" for Certain Processing

Under Article 21 data subjects have the right to object to processing of their personal data when it relies on certain public interest grounds or under "official authority" of the Controller, or other legitimate interests of a Controller (Art. 6.1. e, f). After an objection is made it is the Controller's burden to demonstrate "compelling legitimate grounds" for further processing. Where the purpose of the processing is direct marketing the subject may object at any time. In such cases the processing must stop.

Under Article 22, data subjects have the right not to be subject to a decision based solely on "automated processing, including profiling, which decision produces "legal effects" or similarly "significantly affects" the data subject. Controller's may apply automated processing where it applies to a contract between the data subject and the Controller, conforms to the Member State's terms for such processing, and is based on the data subject's "explicit consent" to the automated processing. Controllers must, however, provide for human "intervention" in the processing to allow data subjects to express their point of view and to "contest the decision." Automated processing decisions with legal or other significant affects may not be made under this article based on "special categories" of personal data identified in Article 9 absent explicit consent of the subject, or in the public interest.

Where a high risk data breach occurs, Article 33 requires detailed reporting by the Controller to the pertinent Supervisory Authority. Article 34 supplies detailed requirements concerning alerting subjects of the data breach, including providing the identity of the Controller or Processor's data protection officer, the likely consequences of the breach and mitigating measures underway.

Appoint an EU representative

Controllers and processers not "established in the Union" but nevertheless subject to GDPR extraterritorial jurisdiction must "designate in writing" a representative in the Union. Art. 27. The representative must be located in one of the member states where the data subjects are located. The representative must be "mandated" by the Processor/Controller to be "addressed" instead of, or in addition to, the Controller/Processer by pertinent supervisory authorities and data subjects so far as issues under the GDPR. There are exceptions for some Processors, but all Processors processing special personal data should verify whether they qualify for one of the exceptions.

Possibly Prepare a Data Processing Impact Statement

Under Article 35 when processing, in particular using new technologies, is likely to result in high risk to subjects, it must be preceded by an assessment by the Controller of the "impact" of the planned processing on the protection of personal data. This assessment may be performed by the Controller's Data Protection Officer. The regulation provides detailed contents for the impact assessment. Once in place, Controllers must review processes to determine if processing is occurring in accordance with the data impact assessment, at least so often as there is a change of the risk presented by the processing operations. This is a significant business planning issue since it is required be performed ahead of actual processing.

Possibly Appoint a Data Protection Officer

Article 37 requires designation of a "data protection officer" (DPO) where:

(a) the processing is carried out by a public authority (not Courts, however);

(b) the "core activities" of the Controller or Processor consist of operations which require "regular and systematic" monitoring of data subjects on a "large scale", or

(c) the core activities of the Controller or Processor consist of processing, on a "large scale", sensitive "special categories" of data or data relating to criminal convictions.
Under Arg. 37.5, the DPO must be designated based on professional expert knowledge of data protection law and practices and ability to perform the tasks under Art. 39.

The DPO may be a staff member of the Controller or Processor, or be hired under a service contract. The DPO's contact details be provided to the supervisory authority. According to Recital 97, the job of the DPO is to "assist the Controller or Processor to monitor internal compliance with the" GDPR. The recital states the DPO "should be in a position to perform their duties and tasks in an independent manner."

Ensure Compliant Relations between Controllers and Processors

Article 28 addresses the relationship between Controllers and Processers, and in doing so sets out requirements on Processers where both are subject to the GDPR. Controllers may use only Processers providing "sufficient guarantees" to implement appropriate technical and organizational measures complying with the GDPR. Processing by a processer must be governed by a contract or other legal "act" subject to Member State law binding "on the Processer with regard to the Controller." Art. 28.3. Note, however, certain indirect exceptions to these requirements exist to facilitate transfer of personal data to countries with neither adequacy approval by the EU, or other data protection safeguards.

The required contract contents are set out in Article 28.3. a- h. These include requirements that processing may only occur under documented instructions of the Controller, by persons "committed" to confidentiality or statutory obligation of confidentiality, the processer take all required security steps, the processer delete or return data at the end of the processing and where applicable, delete copies, and that the processer demonstrate compliance Article 28's requirements. The Processor must allow and contribute to audits for compliance by the Controller or his hired auditor.

Under Article 28.9, the contract must be in writing. If a processer "infringes" the GDPR by determining the purposes and means of processing, it will be considered a Controller as to the infringing processing.

The model contract language provided by the EU under its predecessor Directive for use between Controller's and Processer's is noteworthy for its flow of obligations and indemnity from the Processor to the Controller. For non-EU Processors, submission to EU jurisdiction for purposes of enforcement of data subject rights and discipline by the EU Supervisory Authority is required.

Keep Records of your Processing

Article 30 provides requirements of Controllers and Processers concerning record keeping about processing performed under their responsibility. This requires installation of a compliant processing oversight and recording function. Article 30.1.a-g provides the detailed content of the documentation the Controller must create concerning its processing. Article 30.2.a-d provides the detailed content of the record Processers must create as to all processing activities carried out for a Controller. All records of processing must be in writing. The records must be available for delivery to the "Supervisory

Authority" on request. Exceptions to this record keeping requirement apply, such as for smaller companies, however any Processor processing special or criminal personal data must examine the exceptions carefully to determine their applicability.

Establish a Self- Reporting System for Breaches

Article 33 requires the Controller to report to the Supervisory Authority without undue delay and within 72 hours of becoming aware of it any personal data breach likely to result in a risk to the rights and freedoms of natural persons. If not made within 72 hours, an explanation of the delay must be provided.

Under Article 33.1, Processors must notify the Controller without undue delay after learning of a personal data breach. The notification must describe the nature of the data breached, categories and number of subjects and records breached, state the name of the data protection officer with full details, describe the likely consequences of the breach and describe the measures taken or planned by the Controller to manage and mitigate the effects of the breach. Art. 33.3.a-d. This required reporting may occur in phases if not all available at the same time, without undue further delay. Art. 33.4. The Controller is required to document breaches including the facts of the breach, its effects and remedial action taken.

Where the breach is likely to result in high risk to data subjects, Article 34 requires the Controller to report the breach without undue delay to the subject. The report must contain the information set out in Article 33.3.b-d. Some exceptions apply which should be investigated, including where the Controller's technical/organizational measures applied to the data render the data unintelligible (e.g., due to encryption), the Controller's subsequent measures ensure the risks to the subjects rights and freedom are not likely to occur, and where notification would involve disproportionate effort, in which case a public announcement may suffice.

D. <u>What if I do not Comply with the GDPR?</u>

There are several significant exposures for covered businesses which fail to comply with the regulation. The regulation provides two levels of penalty exposure, one as high as EUR 10m, or 2% of worldwide sales. Generally, these involve violations which appear more technical or of lesser potential for harm. The second level of penalties include fines as high as EUR 20m or 4% of worldwide sales. These are reserved for violation of basic processing principles, conditions of consent, basic data subject rights, or improper transfer of data outside the EU, or disobeying a Supervisory Authority, all of which are viewed as foundational aspects of the data protection objective.

Civil enforcement under GDPR of alleged violations by data subjects is also available. Under Articles 79 and 82 data subjects are entitled to material and non-material damages cause by non-compliant processing. This means recoverable damages are not limited to demonstrable economic loss. Where more than one Controller or Processor is involved, then any liability is joint and several. For the immediate future, the likelihood of actual U.S. prosecution of violations and/or immediate dramatic prosecutions and penalties within the EU is probably low, especially for businesses making a good faith

and demonstrable effort to comply with the regulation. This will, of course, change as EU Member State Supervising Authorities come on line with the regulation, experience under the regulation grows, and conflicts with US companies develop.

There is also a substantial business risk of non-compliance. US business which process EU Subject data will lose business if they refuse to comply, or incompletely comply, or refuse the offered contracts of their EU business partners. The best policy for covered U.S. businesses is to comply and be able to demonstrate compliance, as well as arrange to accommodate the demands and responsibilities imposed by contracts with EU business partners concerning EU personal data processing.

Summary

Once GDPR applicability is determined a host of significant responsibilities apply to US Controllers and Processors of EU subject personal data. The duties extend to the data subject, the EU and its supervising authority, and between Controllers and Processors. Significant adjustments may be required on both the security and informational side of Controller and Processor technology to comply with the notice and subject response obligations imposed on Controllers and Processors. The security by design concepts of the regulation will expose many gaps in current processing capacity. GDPR compliance management will become an administrative function in covered businesses whether or not they operate at a level requiring data processing assessments or designation of a DPO. Companies that resist compliance risk not just enforcement but loss of business relationships with customers obliged to comply.

Michael H. Gladstone

May 14, 2018