GDPR ANALYSIS

I. ARE STANDARD CONTRACTUAL CLAUSES NECESSARY?

The GDPR provides broad obligations on controllers and processors of personal data that apply to entities subject to the GDPR's territorial scope.

If both entities are independently subject to the territorial scope of the GDPR, the entities may export the personal data outside the EU for processing without the need for the Standard Contractual Clauses. The GDPR provides substantial protections for the personal data and since **both** entities are subject to the GDPR, the Standard Contractual Clauses are unnecessary.

If, however, only one of the entities is subject to the territorial scope of the GDPR, that entity must require the non-EU entity to execute Standard Contractual Clauses to ensure the non-EU entity adequately safeguards the personal data.

Consequently, when engaging a vendor to process personal data on behalf of UD, both UD and the vendor must be examined, as well as the nature of the processing activities, to determine whether each is independently subject to the GDPR or whether Standard Contractual Clauses may be required.

II. ARE THE ENTITIES INVOLVED SUBJECT TO THE TERRITORIAL SCOPE OF THE GDPR?

There are two ways an entity can become subject to GDPR: (i) through an establishment in the EU, or (ii) through targeting on individuals within the EU.

A. ESTABLISHMENT IN THE EU – Article 3(1): Do you have a physical presence within the EU regardless of whether you actually process the personal data there?

Recital 22 implies that to be established in the EU, the entity (i) engages in effective and real exercise of activities (ii) through a stable environment in the EU. Both elements must be considered in light of the "specific nature of the economic activities and the provision of services concerned."

Note: This analysis is especially important for when an entity offers services exclusively over the Internet. Just because a non-EU entity's website is accessible in the EU does not mean it is established in the EU for purposes of this analysis.

1. Stable Arrangement – The legal form of the arrangement (e.g., subsidiary, branch, etc.) is not the determining factor.

    a. This is a low bar when the controller's activities consist largely of providing services online so even if a single employee is located within the EU and conducts activities associated with providing those services, it may be enough to qualify as being "stable."

    b. However, if an employee based in the EU conducts activities relating to the controller's activities outside the EU, the mere presence of the employee in the EU would not satisfy the stability requirement.

Questions to consider: (i) What are the main activities of the entity (e.g., education, research, etc.); (ii) Is there a physical presence within the EU; (iii) Regardless of whether there is a physical presence, does the processing activity by a person located in the EU relate to the economic activity of the entity?

2. Effective and Real Exercise of Activities – Regardless of whether the processing is conducted at a physical presence (i.e., establishment) within the EU, does the processing relate to the activities being conducted within the EU?

Note: This is a case-by-case determination based on relevant case law. It cannot be interpreted restrictively, but presence alone is also not sufficient. Some commercial activity carried out by a non-EU entity within the EU may be so far removed from the processing of personal data by this entity that the existence of the commercial activity in the EU would not be sufficient to bring the data processing by the non-EU entity within the scope of the GDPR.

   a. Relationship between a data controller or processor outside the EU and its local establishment within the EU - Are the processing activities conducted outside the EU inextricably linked to the activities of an establishment within the EU? If so, even if the processing is being conducted outside the EU, the GDPR applies.

   b. Revenue raising in the EU – Does the EU establishment raise revenue in the EU? This may be sufficient to find the GDPR applies to the non-EU entity assuming the activities are inextricable linked to the processing of personal data outside the EU and individuals in the EU

B. APPLICATION OF TARGETING CRITERION – Article 3(2): Are you offering goods or services to individuals in the EU or monitoring behavior of individuals located in the EU?

1. The fact that goods and services are available to individuals in the EU or that you are monitoring behavior of individuals located in the EU is by itself not enough to put you within the scope of the GDPR. You must be purposefully "targeting" those activities to people in the EU. This determination is made at the moment when the relevant trigger activity takes place, i.e., at the moment of offering of goods or services or the moment when the behavior is being monitored, regardless of the duration of the offer made or the monitoring undertaken.

Note: An entity not established in the EU may be subject to the GDPR in relation to some processing activities but not subject to the GDPR with respect to other processing activities so you should define the processing activities in question very specifically.

Note: Just because a person is in the EU does not trigger the GDPR alone. The additional element of targeting of individuals in the EU, either by offering goods or services to them or by monitoring their behavior must always be present.

2. Offering of goods or services (regardless of whether payment of the data subject is required) to data subjects in the EU must intentionally target them and not be inadvertent of incidental.

Note: if the processing relates to a service that is only offered to individuals outside of the EU but the service is not withdrawn when such individuals enter the EU, the related processing will not be subject to the GDPR. In this case, the processing is not related to the intentional targeting of individuals in the EU but related to the targeting of individuals outside the EU which continue whether they remain outside the EU or whether they visit the EU.

a. Is the activity a "Society service," which is any service normally provided for remuneration, at a distance, by electronic means and at the individual request for services"?

b. Are the goods or services intentionally being offered to individuals in the EU? Is it apparent that the non-EU entity envisions offering services to data subjects in the EU?

(i) The mere accessibility of the non-EU entity's or an intermediary's website in the EU, 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.

(ii) Factors such as the use of a language or a currency generally used in one or more Member States of the EU with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the EU, may make it apparent that the controller envisions offering goods or services to data subjects in the EU.

(iii) To "direct activity" means that the controller must have manifested its intention to establish commercial relations with EU consumers.

(iv) Consider the following factors **collectively** to determine whether the non-EU entity is offering goods or services targeted to individuals in the EU:

- The EU or at least one Member State is designated by name with reference to the good or service offered;
- The controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the EU; or the controller or processor has launched marketing and advertisement campaigns directed at the EU audience;
- The international nature of the activity at issue, such as certain tourist activities;
- The mention of dedicated addresses or phone numbers to be reached from an EU country;
- The use of a top-level domain name other than that of the third-country in which the controller or processor is established, for example ".de", or the use of neutral top-level domain names such as ".eu";

- The description of travel instructions from one or more other EU Member State to the place where the service is provided;
- The mention of international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers;
- The use of a language or currency other than that generally used in the trader's country, especially a language. R currency of one or more EU Member States;
- The data controller offers the delivery of goods in EU Member States.

Note: Recital 23 confirms that the mere accessibility of the controller's, processor's, or an intermediary's website in the Union, the mention on the website of its email or geographical address, or of its telephone number without an international code does not, of itself, provide sufficient evidence to demonstrate the controller or processor's intention to offer goods or services to a data subject located in the Union. In this context, goods or services are inadvertently or incidentally provided to a person in the EU and the related processing of personal data would not fall within the territorial scope of the GDPR.

3. Monitoring of data subjects' behavior – the behavior monitored must (i) relate to a data subject in the EU and (ii) the monitored behavior must take place within the territory of the EU.

   Questions to Consider: (i) Are natural personal tracked on the internet including subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting his or her personal preferences, behaviors, and attitudes? (ii) Are other types of network or technology involving personal data processing used for tracking purposes (e.g., wearable technology and other smart devices)? (iii) Does the controller have a specific purpose in mind for collecting and subsequently reusing the relevant data about an individual's behavior within the EU? (iv) What is the purpose for the processing and any subsequent behavioral analysis or profiling techniques involving that data.

   a. Monitoring activities can include:

      - Behavioral advertisement;
      - Geolocation activities, in particular for marketing purposes;
      - Online tracking through the use of cookies or other tracking techniques such as fingerprinting;
      - Personalized diet and health analytics services online;
      - CCTV;
      - Market surveys and other behavioral studies based on individual profiles;
      - Monitoring or regular reporting on an individual's health status.

   b. Processing activities "related" to targeting activities also fall within the territorial scope of the GDPR even if the processor is not located in the EU.

C. MEMBER STATE LAW MAY ALSO APPLY – If it is more stringent than the GDPR

D. REPRESENTATIVE OF CONTROLLERS OR PROCESSORS NOT ESTABLISHED IN THE UNION

1. These designations must be made in writing.

2. Article 27(2) provides two requirements to be exempt from the designation obligation.

    a. Processing is "occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offenses referred to in Article 10"

        (i) Processing is occasional if it is not carried out regularly and occurs outside the regular course of business or activity of the controller or processor

        (ii) Factors to consider when determining whether processing is carried out on a large scale include:

            - The number of data subjects concerned, either as a specific number or as a proportion of the relevant population
            - The volume of data and/or the range of different data items being processed
            - The duration, or permanence, of the data processing activity
            - The geographical extent of the processing activity

    b. Processing "is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope, and purposes of the processing."

        (i) This requirement is not limited to processing unlikely to result in high risk to the rights and freedoms of data subjects.

        (ii) When assessing the risk to the rights and freedom of data subjects, consider both the likelihood and severity of the risk.