PROGRAM MATERIALS
Program #2968
April 18, 2019

11 Months In - What You Need to Know About GDPR Scope and Enforcement Actions

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Extraterritorial Scope of GDPR and Enforcement Take-Aways

Odia Kagan
Partner and Chair of GDPR Compliance and International Privacy
Fox Rothschild, LLP
okagan@foxrothschild.com
https://www.linkedin.com/in/odiakagan/

EDPB Territorial Guidelines

The Big Bad GDPR

- EU General Data Protection Regulation (GDPR)
- Overhauls EU data protection legislation
- One law directly applies to all 28 states
- Effective date: May 25, 2018

Does GDPR apply to me?

Broad extraterritorial application

GDPR applies to US companies if they

- Have an establishment in the EU (broad)
- set out to provide services to individuals residing in the EU

OR

- Track / monitor EU individuals (cookies)

AND

and those services /activities

- involve processing identifiable personal information

Door No. 1:
Establishment in the EU

- Do you have an “establishment”?
  - Branch or subsidiary in EU member state
  - Any real and effective activity, even a minimal one (even one employee)
  - Just having a website accessible from Europe is not enough
- Is there an inextricable link between the activities of an EU establishment and the processing of data carried out by you?
- Processing in or out of the EU

Example 1: A car manufacturing company with headquarters in the US has a fully-owned branch and office located in Brussels overseeing all its operations in Europe, including marketing and advertisement.

The Belgian branch can be considered to be a stable arrangement, which exercises real and effective activities in light of the nature of the economic activity carried out by the car manufacturing company. As such, the Belgian branch could therefore be considered as an establishment in the Union, within the meaning of the GDPR.

EDPB Guidelines p. 5

- I’m a Non-EU controller with an EU-Processor?

  - GDPR doesn’t necessarily apply)

- I’m an EU based controller use a Non-EU processor - ensure by contract that the processor processes data in accordance with the GDPR

Example 4: A French company has developed a car-sharing application exclusively addressed to customers in Morocco, Algeria and Tunisia. The service is only available in those three countries but all personal data processing activities are carried out by the data controller in France.

While the collection of personal data takes place in non-EU countries, the subsequent processing of personal data in this case is carried out in the context of the activities of an establishment of a data controller in the Union. Therefore, even though processing relates to personal data of data subjects who are not in the Union, the provisions of the GDPR will apply to the processing carried out by the French company, as per Article 3(1).

EDPB Guidelines p. 8

Example 5: A pharmaceutical company with headquarters in Stockholm has located all its personal data processing activities with regards to its clinical trial data in its branch based in Singapore. According to the company structure, the branch is not a legally distinct entity and the Stockholm headquarter determines the purpose and means of the data processing carried out on its behalf by its branch based in Singapore.

In this case, while the processing activities are taking place in Singapore, that processing is carried out in the context of the activities of the pharmaceutical company in Stockholm i.e. of a data controller established in the Union. The provisions of the GDPR therefore apply to such processing, as per Article 3(1).

EDPB Guidelines p. 8

Door No. 2:
Offering Products or Services

“In the EU”

- Physically located in the EU at the time of the offering of goods or services (or the monitoring of behavior, see below).
- Not citizenship.
- Not residence

Example 8: A start-up established in the USA, without any business presence or establishment in the EU, provides a city-mapping application for tourists. The application processes personal data concerning the location of customers using the app (the data subjects) once they start using the application in the city they visit, in order to offer targeted advertisement for places to visits, restaurant, bars and hotels. The application is available for tourists while they visit New York, San Francisco, Toronto, London, Paris and Rome.

The US start-up, via its city mapping application, is offering services to individuals in the Union (specifically in London, Paris and Rome). The processing of the EU-located data subjects' personal data in connection with the offering of the service falls within the scope of the GDPR as per Article 3(2).

EDPB Guidelines p. 13

“Offering”

- marketing and advertisement campaigns directed at an EU country audience
- mentioning dedicated addresses or phone numbers to be reached from an EU country
- using an EU or member state top-level domain name
- mentioning customers domiciled in various EU member states, including client testimonials
- using an EU language or a currency
- offering the delivery of goods in EU member states.

“Offering” (ctd)

- Need some targeting
- List of factors from competition case law
- Consideration not needed
- Website not enough
- What about existing customers?

Example 12: A website, based and managed in Turkey, offers services for the creation, edition, printing and shipping of personalised family photo albums. The website is available in English, French, Dutch and German and payments can be made in Euros or Sterling. The website indicates that photo albums can only be delivered by post mail in the UK, France, Benelux countries and Germany.

In this case, it is clear that the creation, editing and printing of personalised family photo albums constitute a service within the meaning of EU law. The fact that the website is available in four languages of the EU and that photo albums can be delivered by post in six EU Member States demonstrates that there is an intention on the part of the Turkish website to offer its services to individuals in the Union.

As a consequence, it is clear that the processing carried out by the Turkish website, as a data controller, relates to the offering of a service to data subjects in the Union and is therefore subject to the obligations and provisions of the GDPR, as per its Article 3(2)(a).

In accordance with Article 27, the data controller will have to designate a representative in the Union.

EDPB Guidelines p. 16

Door No. 3:
Monitoring or tracking

Monitoring or tracking

- No intent necessary
- Online or other forms of technology
- Behavioral advertising
- Geo-localization activities, in particular for marketing
- Online tracking (cookies, fingerprinting)
- Market surveys and other behavioral studies based on individual profiles

Monitoring or tracking (ctd)

- behavioral advertising
- geo-localization 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

Local representative

- Required
- For enforcement
- Like “service of process agent” but fully liable…

The regulators speak, we listen

ICO on RTBF in Backups

- Put data immediately beyond use
- Retain for an appropriate amount of time
- Delete as soon as possible after (next deletion/destruction cycle)

Germany: Don’t store passwords in cleartext (Knuddels.de)

- contact your DPA directly and quickly
- inform users immediately and comprehensively
- cooperate with your DPA
- improve your IT security even if at great monetary expense

Germany: Don’t forget the Data Processing Agreement

- Germany based controller fined €5,000 for a single missing data processing addendum between it and a processor
- Due to a customer complaint

Germany: Right of Access in the employment context

- Company must provide the data subject with a copy of the personal data which are the subject of processing
- employers must provide their employees with comprehensive information and copies of their performance and behavioral data upon request.
- employees have the right to inspect their employer's whistleblower system

Denmark: Data minimization

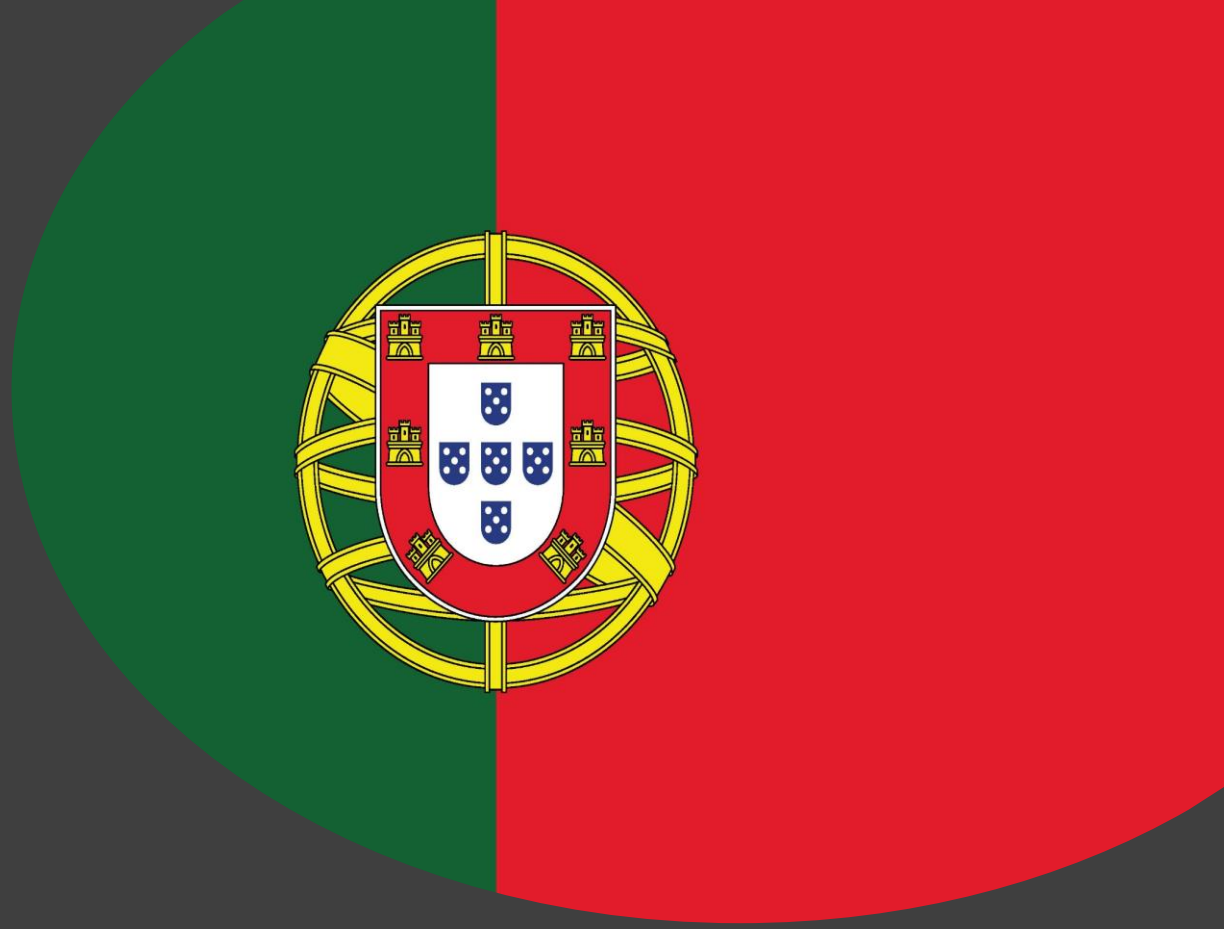
- The removal of a name does not constitute anonymization
- You cannot set a deletion deadline, three years longer than necessary, simply because your database or system makes it difficult to comply with the rules.

- You must adequately document your procedures for data deletion including: follow-up on the deletion of the systems correctly; handling reloading of previously deleted personal data when putting in backup; and logging deletions in the systems

Poland: Right to Information

- the person whose data has been scraped must be informed who has their data; the types of data obtained; what is going to be done with; and the legal basis for the processing
- You need to act in an active matter - that means providing information to a data subject without them having to participate in enabling their own notification
- Compliance is required even if there is a high cost attached (EUR 8M)

Portugal: Information security hygiene in hospital (Barreiro Montijo)



Two violations:

- the existence of user profiles with, unnecessary unlimited access to patient information,
- the existence of user profiles that did not belong to doctors actively employed by the hospital.

UK: Legal Basis (AggregateIQ)

(i) processed personal data:
  (i) in a way that data subjects were not aware of;
  (ii) for purposes they would not have expected and
  (iii) without a lawful basis for the processing.

(ii) failed to provide disclosure of its practices as required by GDPR.

France: Geolocation and SDK Technology (Singlespot)

- inform individuals when downloading the applications that:
  - an "SDK" collects their location data
  - that the data is collected for the purpose of targeted advertising, and
- acquire the user's consent prior to the collection of the information.
- define an adequate retention period, and ensure the security of the data.

France: Disclosure and Consent (Google)

- Privacy notices are just that. Notices.
- Disclose all the pertinent aspects of the processing - why you process their information, how long you keep it and the categories of it.
- Use clear specific language. Vague statements such as “any of the following purposes may apply” will not suffice.
- Try to put all relevant information in one place. (especially if processing is complex, uses information from different sources or involves sensitive information.)

France: Disclosure and Consent (Google)

- Make sure information you provide users is easily accessible.
- Refrain from requiring multiple actions to access the necessary information.
- Consent needs to be specific and unambiguous.
- Use separate call-outs. Statements such as: “I accept that my information is used as described above” may not suffice.
- Get consent for each processing/purpose separately, not in bulk.
- Require action by the user to signify consent (no pre-checked checkboxes).

France: Consent in OBA and Adtech (Vectaury)

- provide all the information people need to understand what they agreed to.
- avoid confusing language that may imply that failing to agree will result in more intrusive ads
- tell users with whom you share their information;
- make sure that the language of the permissions displayed on the user's phone (both iOS and Android) are sufficiently specific (location used for profiling);

France: Consent in OBA and Adtech (Vectaury) (ctd)

- ensure that your "customize preference" option leads to unchecked boxes;
- don't put the "customize" button after a long scroll down.
- a contractual provision guaranteeing consent has been received is not sufficient to meet the consent requirement. you must be able to demonstrate consent had been received.

UK & Austria: Cookie Consent

- Equivalent alternative?
- True Consent?
- Unintended Consequences?

Netherlands: Art. 30 sweep

- Data Processing Ledger
- 30 randomly selected large companies (more than 250 employees) in 10 different sectors: industry, water supply, construction, retail, hospitality, travel, communications, finance, business services, and health care across the Netherlands

Netherlands: Cookie wall ban

- cookie walls that demand a website visitor agrees to their internet browsing being tracked for ad-targeting as the “price” of entry to the site are not compliant with European data protection law
- internet visitors must be asked for permission in advance for any tracking software to be placed — such as third-party tracking cookies; tracking pixels; and browser fingerprinting tech
- and that that permission must be freely obtained. Ergo, a free choice must be offered.

Right of Access (NOYB v. streaming services)

- Controllers that receive a request from an individual asking for access to their data must disclose all data they hold and which could render the individual identifiable, including cookies, online identifiers, tracking technologies, beacons, IP addresses, pixel tags or device identifiers.
- Controllers must provide the information in a manner clearly readable by the average consumer. If you provide the data in machine-readable format, you need to also provide an explanation, software or other means to make the data readable and understandable.

Right of Access (NOYB v. streaming services)

They must disclose:

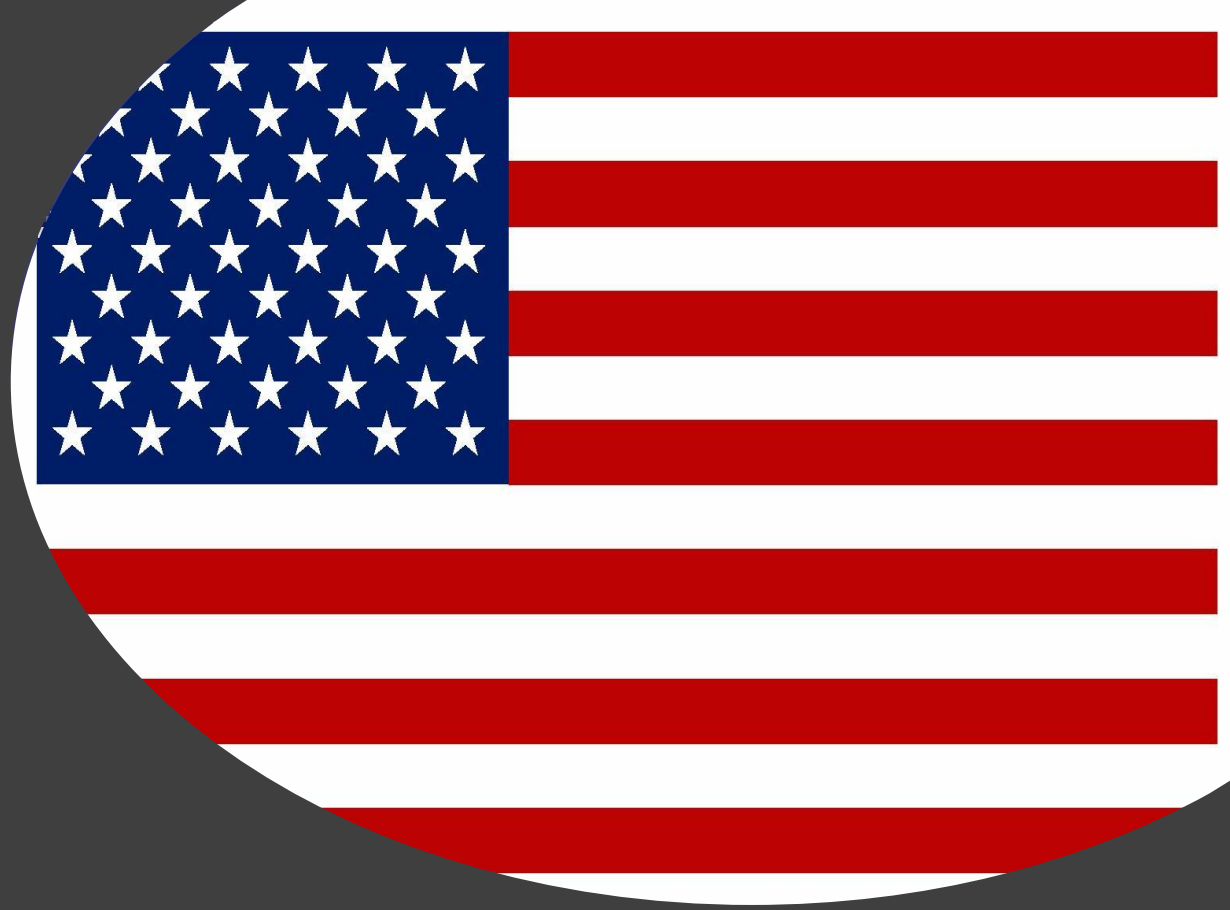
- purpose
- categories
- recipients
- retention
- sources (if not the individual)
- transfers outside the EU
- the individual's right to right to request rectification, restriction of or objection to processing
- the individual's right to lodge a complaint
- the existence of automated processing/profiling

And on this side of the pond…

FTC enforcing “GDPR compliant” statements

“If a company claims that it is compliant with EU law, it better be right, because the FTC will be looking for companies that are non-compliant but say otherwise”

Increased enforcement under Privacy Shield



- Quarterly “false claims reviews” to identify organizations that have started but not finished an initial or re-certification or that did not submit their annual recertification.
- Random web searches for false claims of participation
- 100 organizations Invesigated
- Individuals following media searching for Privacy Shield violations.
- Regular checks for broken links to the privacy policy on the Privacy Shield list.
- Civil Investigation Demands (CIDs) proactively to monitor compliance with the Privacy Shield principles.

Odia Kagan

Partner, Chair of GDPR Compliance and International Privacy

Fox Rothschild LLP

okagan@foxrothschild.com

215-444-7313

https://www.linkedin.com/in/odiakagan/