G.D.P.R. and how it affects U.S.

A review of GDPR outside of Europe and US Privacy Shield framework

Wes Bearden, Attorney

BEARDEN INVESTIGATIVE AGENCY, INC.
Dallas, Texas
&
New Orleans, Louisiana

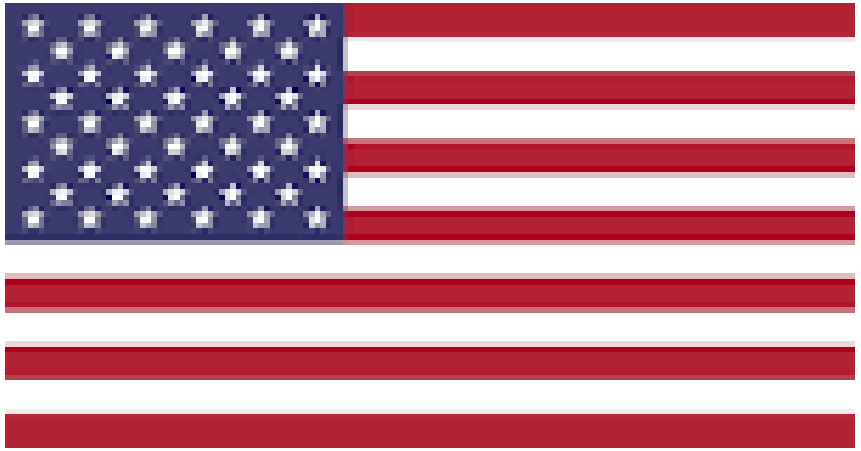
Comparison of US v. European

Federal and State Laws

- No single law in the US regulating the collection and use of personal data. Sectoral law.
- Both federal and state laws regulate the use and protection of personal information. Carve out law and exceptions.

GDPR is binding on all EU member states

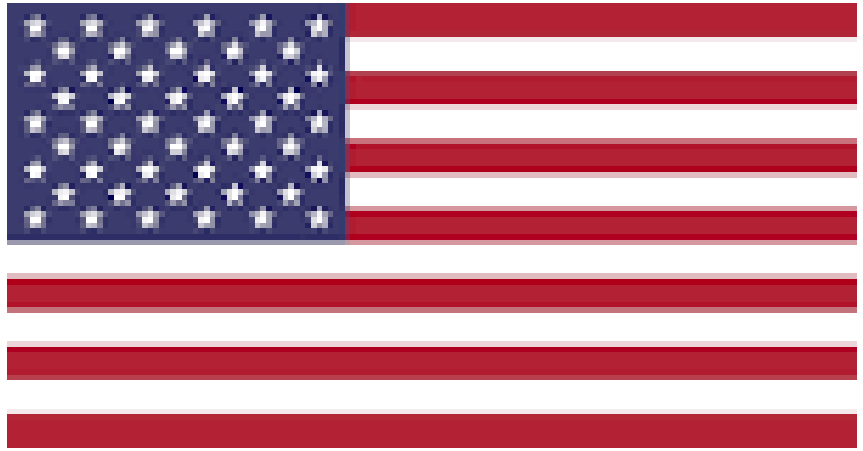
- Overarching law across all industry sectors.
- Parts of GDPR require implementation by EU member state national law. National law supplements GDPR. One stop shop for privacy.



The U.S. Alphabet Soup Laws

- **ECPA** – Electronic Communications Privacy Act
- **FCRA** – Fair Credit Reporting Act
- **SCA** – Stored Communications Act
- **GLBA** – Gram Leach Bliley Act
- **DPPA** – Driver's Privacy Laws
- **CLOUD** – Clarifying Lawful Overseas Use of Data Act
- **FERPA** – Federal Educational Rights and Privacy Act
- **HIPPA** – Health Insurance Portability and Accountability Act

What is Confidential?



Federal and State Laws

There is not single accepted definition of personal, confidential or protected data. Each law carves out the interest they are protecting. Some definitions are more specific than others.

GDPR's Broad Definition

"…any information relating to an identified or identifiable *natural* person." Very broad definition that may include ip addresses, employee numbers, identifiers, trackers????

G.D.P.R – Couple Quick Exceptions, Always Read!!!

- Remember, GDPR doesn't apply to :
  - Deceased Person – *See* Recital 27, but member states can regulate more. So, know you country's law.
  - Legal entities – Subject of your investigation is a corporation or fictitious entity. But be careful of the officers.
  - Country Assessments.

Differing Consent Variations?

Federal and State Laws

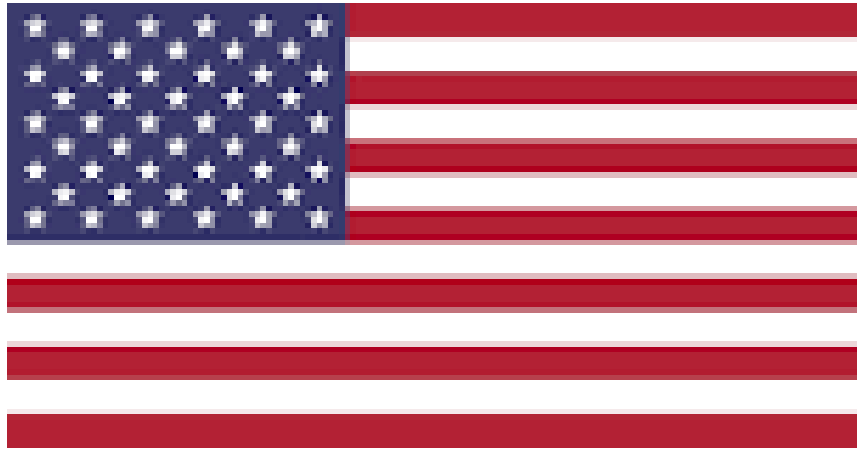
Consent is always available for privacy and easy to meet. Implicitly and Explicitly.

Think Background Authorization

Employee Wrongdoing

GDPR's Consent

Must now be extraordinarily specific and explicit. Must be able to revoke as easily as given. Require much more paperwork to get consent to transfer and process data.



Right to be Forgotten

- This idea of a right to be forgotten pushes large companies to “purge” data. It allows for spoliation of evidence and runs counter to the idea that a witness being able to testify to what they know.
- For many crimes, wrongdoings or civil suits, the day of reckoning comes years after the act. Think Paul Manafort.
- This idea also runs counter to transparency and freedom of speech. *See* Google Case;
- Transparency and the right to know have outweighed this in the U.S.
- This is not the same as right to privacy. We are forgetting not protecting.

Penalties and Deterrents

- US Penalties: Criminal violations and fines are common. But, practically speaking, the damages are left to be proved by the victim. Private lawsuit proving the damages that have occurred is the norm. Compensatory, punitive, exclusion and other damages are tailored to the case and decided by the jury not the government.
- European Penalties: Up to € 20 million plus decided amongst 10 factors which will not weigh favorably to a private investigator and decided by the DPA.

How does the DPA calculate the fine?

- **Nature of infringement**: number of people affected, damaged they suffered, duration of infringement, and purpose of processing
- **Intention**: whether the infringement is intentional or negligent
- **Mitigation**: actions taken to mitigate damage to data subjects
- **Preventative measures**: how much technical and organizational preparation the firm had previously implemented to prevent non-compliance
- **History**: (83.2e) past relevant infringements, which may be interpreted to include infringements under the Data Protection Directive and not just the GDPR, and (83.2i) past administrative corrective actions under the GDPR, from warnings to bans on processing and fines
- **Cooperation**: how cooperative the firm has been with the supervisory authority to remedy the infringement
- **Data type**: what types of data the infringement impacts; see special categories of personal data
- **Notification**: whether the infringement was proactively reported to the supervisory authority by the firm itself or a third party
- **Certification**: whether the firm had qualified under approved certifications or adhered to approved codes of conduct
- **Other**: other aggravating or mitigating factors may include financial impact on the firm from the infringement

Down Stream Control

EU - Controller and Processors under the DPA are an attempt to manage down stream protection of data. The reason is that

US – The government, at least, doesn't place controls on this data. The rights and responsibilities lie with the aggrieved party. Maddow v. Trump.

G.D.P.R – Territorial Scope.

Territorial Scope – GPDR applies to the processing of data in the union when a controller or processor is not in the union and the processing includes “the monitoring of their behavior as far as their behavior takes place within the Union.” Article 3.2.b.

The GDPR's extraterritorial reach comes into play even for corporations established outside the EU. In the context of investigation, multinationals will often need to comply with the GDPR if there is any connection to EU data, even if the data being reviewed is (legally) stored outside the EU, eg, on email servers in the US.

Or, even if your Subject (even a US citizen) travels to Europe, it is covered.

Bearden
INVESTIGATIVE AGENCY

G.D.P.R. – Extra regulation on top of G.D.P.R.

The GDPR establishes only a floor of employee data privacy protection. Each member state is allowed to set higher standards. national laws will apply – for example, employment laws, labor laws, blocking statutes, secrecy of correspondence laws, criminal laws and in some cases, laws governing where data may be stored. In other words, employers cannot take the "one stop shop" idea literally when conducting internal investigations involving data of EU personnel.

Bearden
INVESTIGATIVE AGENCY

U.S Privacy Shield

- What is it?? The EU-U.S. Framework was designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

Bearden
INVESTIGATIVE AGENCY

What do I have to do? Part I

Informing individuals about data processing:

-Commit to DOC and the public by way of statement.

-Get or link to a complaint submission form for individuals to file on you.

-Inform individuals of their rights to access their personal data.

Provide free and accessible dispute resolution:

-Respond to a complaint from an individual within 45 days.

-Provide independent way to investigate their complaint.

-If they complain on you with DPA in EU, DOC gets to investigate you.

-If Complaint, you must Cooperate with the DOC.

-If dispute, you agree to binding arbitration.

Bearden
INVESTIGATIVE AGENCY

What do I have to do? – Part II

You can only use it for limited purposes:

-Must limit personal information to relevant information.

-Must comply with the new data retention principles.

Requirements for data transferred to third parties

-Must Comply with the Notice and Choice Principles.

-Must enter into a contract with the third-party controller.

-Must take responsibility for your down stream parties.

-Provide your contract to the DOC with third parties.

Continuing Responsibilities:

-Must tell everyone if you screw up in a FTC report.

-Must annually “re-certify” to be in the program.

Bearden
INVESTIGATIVE AGENCY

FTC Cases

- *ReadyTech Corp.*, FTC Docket No. 1823100, (JULY 2, 2018).
- *IDmission LLC*, FTC Docket No. 182310 (Sep. 27, 2018).
- *Tru Communication, Inc., dba TCPrinting.net,* FTC Docket No. 1723171 Sep. 8, 2017)

Two Big Take Aways:

- **The FTC remains committed to challenging false promises about Privacy Shield participation.**

- **Avoid a framework false start –** You have to finish the setup completely, and you have to renew. Voluntary.

Will Privacy Shield Be Here Forever?

- Probably not. This is the second challenged program.

Why not?

US passed the Judicial Redress Act In 2015 which was an attempt to provide non-US citizens rights under the Privacy Act. However, FISA remains a really valid concern for EU Citizens.

Will Privacy Shield Be Here Forever?

A number of reasons for asking the Commission to suspend the Privacy Shield pending US compliance, including the recent reauthorization and amendment of Section 702 of the Foreign Intelligence Surveillance Act (“FISA”) which allows US intelligence agencies to collect information on non-US persons located outside of the US and the March 2018 Clarifying Overseas Use of Data (“CLOUD”) Act, which allows US law enforcement agencies to access personal data stored abroad.

Remember, the prior safe harbor system was struck down by the European Court.

Remember, What is Privacy Shield.

Privacy Shield is a determination that adequate safeguards exist. The EU can make determinations of third countries that are adequate. Adequacy decisions are based essentially on:

a. The Rule of Law in that country. (Again, completely different path).
b. The Existence of a Supervisory Authority. (FTC or DOC).
c. And, International Commitments. (Privacy Shield for now).

So, then what?

Article 46 and 47 must then be used to essentially contract the data rights in the receiving country by the controller (“the EU Investigator”) by safeguards to protect the data subject by :.

- Contracting clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or
- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. (Binding Corporate Rules).

Well, what if they won’t agree…

- In absence of a countries binding corporate rules or adequate safeguards, specific transfers may be accomplished if:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order 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;

If you can satisfy above then,

You can fall back on legitimate interest but, you have to notify the data subject and tell them what you are doing.

So, read Chapter 5 carefully and move through Articles 44 – Article 50!!!!!

Find your out.

Facebook gets $1.6 Billion fine!!!