EU GDPR

A PRIMER IN PLAIN ENGLISH

INSIDE

EU GDPR – A PRIMER

INTENDED AUDIENCE: AMERICAN COMPANIES WITH BUSINESS INSIDE THE EU28

"You know it's coming, but you don't know what it means. You have business in the EU28, or you sell products or services to clients or customers living in the EU28. You have to figure it out, but you don't want to become a legal or compliance expert, or learn French or German. This white paper is for you! " – Laurence Dunne

ABOUT THE AUTHOR

Laurence Dunne has 25 years experience implementing compliance products for financial services and healthcare companies, including United Healthcare, American Express, Blue Cross, Citibank and Apple. Laurence has served as a primary owner of compliance products for Fortune 500 companies for the USA Patriot Act, the CFPB, HIPAA, Dodd-Frank, The CARD act, Sarbanes Oxley, the FFIEC's Authentication in an Internet Banking Environment directives and the Affordable Care Act.

OVERVIEW

WHAT IS GDPR?

The EU General Data Protection Regulation ("GDPR") is a comprehensive data protection law that updates and replaces older EU laws and national laws in different EU member nations to set high, globally-applicable standards for the protection of personal data of EU citizens, regardless of where that data is stored. To overcome the lack of a central enforcement mechanism within the EU, the GDPR will be enforceable by each member state, and each member state is legally obliged to set up a Data Protection Authority for the purpose of enforcing GDPR. The law will come into force on May 25th 2018.

APPLICABILITY

GDPR protects the personal data of EU Citizens for most commercial purposes, even when the business transaction involves a business entity outside the jurisdiction of the EU. An important point to note is that the GDPR only protects the EU citizens data when they are actually in the EU. So, for example, if you run an e-commerce engine and sell digital products such as software, financial services, access to information, entertainment products such as movies or music, or any other digital product, or for any other reason you collect personal data on EU citizens who are *inside* the EU at the time you collect or use their personal data, the law applies. It does not cover the personal data of EU citizens who are *outside* the EU at the time of the transaction.

EXCEPTIONS

There are a few exceptions and exemptions to GDPR. It does not apply to governments when they are acting in a normal governmental capacity, including fighting crime and terrorism, collecting data related to government benefits, the provision of state-run healthcare, transportation and other functions. However, it *does* apply to companies providing those services on behalf of an EU member nation. For example, if a German Police officer stops a speeding motorist and writes him a paper ticket, then uploads the citizens personal information to a police-hosted server, neither the officer nor the police force can be subjected to GDPR remedies. However, if the police software was developed by a commercial entity, they may be considered non-exempt. If a commercial entity hosts the police data on their servers, they are not exempt.

DEFINITIONS

SUMMARY

GDPR is complicated, and this paper lists many acronyms. Rather than explain each in context, a brief primer on the lingo of the GDPR will get you speaking European Legalese before your boss asks you questions you can't answer!

CLEAR AFFIRMATIVE ACTION

This is an import piece of legalese. *Clear affirmative action* means a positive action, such as clicking an "I Agree" button, in a "Clear" manner, and it governs the definition of consent of a data subject.

CONSENT

Consent has a specific meaning under GDPR. It is defined in Article 4 (11) as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*;"

This is one of the most onerous parts of GDPR as it expressly forbids complex legal agreements and privacy policies governing data use of EU Citizens. It demands clear affirmative action in unambiguous language, and it covers a wide range of data uses for all data subjects.

CONTROLLER

A controller is a legal entity responsible for determining the "*purpose and means of processing personal data"* (EU GDPR 4 (7)). The controller is legally accountable to GDPR, and the processor is separately legally accountable. For example, if you use a third-party E-Commerce engine to run your website, store personal data, process payments and shipping, that third party is the *processor*. You are the *controller*.

DATA PROTECTION AUTHORITY (DPA)

Each of the EU28 countries has a Data Protection Authority, responsible for enforcing the GDPR in their country. The GDPR has no central

enforcement mechanism, so enforcement is the responsibility of the DPA in each of the EU28.

DATA PROTECTION OFFICER (DPO)

Article 37 requires all controllers and processors who, in the course of normal business operations, regularly monitor personal data of a *data subject*, to appoint a *Data Protection Officer* (DPO). The DPO does not need to be a full-time employee of the controller or processor, but this person has specific responsibilities outlined later in this document.

DATA SUBJECT

A Data Subject is any person whose personal data is subject to GDPR. All residents of EU28 nations are data subjects while they are residing in those countries.

EU27 AND EU28

These references started popping up after the United Kingdom voted to leave the European Union in 2016. On March 30th 2019, the U.K. will leave the European Union, reducing the number of member nations from 28 to 27. Since there is considerable uncertainty over which EU laws will continue to apply to the United Kingdom, the terms EU28 and EU27 are used to differentiate between laws that currently apply to all 28-member nations or that will continue to apply to the UK after BREXIT, and laws that will apply only to the remaining 27 nations.

PROCESSING / PROCESSOR

Any operation(s) that include the collection, transmission, storage, dissemination, use or destruction and disposal of Personal Data, whether automated or manual. That's right, if your call center staff records EU citizen data on sheets of paper, that's considered *processing*. A legal entity, such as a government entity, corporation, charity or trust, who engages in processing is a *Processor.*

PSEUDONYMISATION

Pseudonymization is the process of removing personally identifiable portions of personal data so that the rest of the data can be used for aggregation, analysis, predictive or other purposes without consent or other GDPR considerations. For instance, if you are collecting healthcare data on EU citizens, you may remove personal references in that data and store the rest of the data for use in analyzing – for instance – the odds of a 50-year-old male contracting cancer. Since no reasonable court would define *50-year-old male* as a data element that would identify a *specific* 50-year-old male, this data can be considered *pseudonymized*. However, there is considerable scope for interpretation, and each of the 28 EU DPA's may interpret the specifics differently. For instance, if you also collect a postal code, profession and marital status, that might limit the number of people enough to allow a data thief to identify a specific individual. Care and due diligence need to be exercised when using this process.

PERSONAL DATA

As stated in GDPR Article 4 (1), 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"*

Think of it as being similar to but stricter than PII in the USA. If you can use the information to identify a person, their location, or activities in which they partook, it's personal data. Personal data includes name, address, Government ID's, email, telephone numbers, IP Address, Geo-Location, biometrics and anything else that can be used to identify a specific individual. As facial recognition takes off, photos, especially photos with geo-location tags, could also be considered personal data.

RECIPIENT

A recipient is a legal entity to whom/which data is disclosed in the course of processing. Public authorities in the EU28 are not considered Recipients when they are acting in their normal roles.

IMPACT

GET TO THE POINT. AM I IMPACTED?

If you collect or use *Personal Data* on a *Data Subject*, you are required to comply with GDPR. This means you are required to comply if you sell (or offer free) services to EU citizens who are in the EU at the time during which you are collecting or using their personal data. You are not required to comply if you take steps to ensure that you only interact with EU citizens when they are not residing in the EU.

SAFE HARBORS

There are several safe-harbors defined in the GDPR.

1. Data collected by an individual is explicitly excluded, even if the person stores or transmits that data through a commercial entity in a context where there is no reasonable expectation that the commercial entity is responsible for monitoring the data. So, for example, there is no requirement for companies running messaging applications to safeguard information passed between two users of the platform.
2. Member states and "competent authorities" are exempted when performing duties in the public interest. So, for example, the US Government does not have to comply with GDPR when collecting traveler data from EU citizens.
3. Pseudonymization is explicitly defined as a safe harbor. Once the data is no longer identifiable to the person, it can be used without regard to the provisions of GDPR.

WHAT DATA IS IMPACTED?

GDPR expands the definition of personal data, and makes it clear that cyber data, such as GPS Location, IP address and biometric data, are included. If a third party could use the data to identify a specific data subject, it is subject to GDPR.

RIGHTS OF DATA SUBJECTS

GDPR in Articles 12-23 defines specific rights for data subjects. These are often referred to as "the rights" and they are as follows:

1. **The right to be forgotten**. The data subject has the right to demand that the controller erase personal data if:
    a. The data is no longer necessary for the purpose of processing
    b. The data subject has previously withdrawn their consent for processing
    c. Erasure is required to comply with other EU directives
2. **The right to access**. The data subject has the right to know if any personal data is being stored for processing. If the answer is *yes*, then the data subject has the right to know:
    a. What data is being stored
    b. The purpose for which it is being stored
    c. The duration for which it will be stored
    d. Origin of the data (if the data did not come from the data subject)
3. **The right to Restriction**. The data subject has the right to demand that their personal data cannot be used for processing purposes if:
    a. The accuracy of the data is in question (such as a disputed item on a credit report)
    b. The processing is unlawful and the data subject has demanded that the data be kept on file for legal purposes
4. **The right to rectification**. The data subject has the right to rectification of inaccurate personal data "*without undue delay*". There is no specific definition of "*undue delay"*
5. **The right to portability**. Data subjects have the right in certain circumstances to have their data made portable "*in a structured, commonly used and machine-readable format*".
6. **The right to be informed.** The data subject has the right to be informed when their data is rectified, erased, restricted or shared.
7. **The right to object.** The data subject has the right to reject their data being processed at any time. This includes the right to object to direct marketing, the right to object to their data being passed to third party entities or used for analytical or scientific purposes. An explicit override is available for data that is "in the public interest"

OBLIGATIONS OF PROCESSORS AND CONTROLLERS

GDPR defined several obligations on *processors* and *controllers*. While the two terms have completely different legal meanings, much of what follows can legally land on either party since one is responsible and the other is accountable. For example, if the *processor* is responsible for maintaining records of processing activities, the *controller* is accountable legally for their choice of processor. Article 28 (1) states "*the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*"

1. The obligation to implement appropriate technical and operational measures (TMO) to comply with this regulation. This requirement does explicitly call out the level of risk and cost as factors in what counts as an appropriate technical and operational measure, so there is leeway here to make the effort proportional to the risk.
2. The obligation to review and update appropriate technical and operational measures, though no specific timeframe is mentioned.
3. Processors must designate, in writing, a representative in the EU.
4. The obligation to implement technologically feasible security measures, including:
    a. Pseudonymization of personal data
    b. Encryption of personal data
    c. Ability to restore access in a timely manner in the event of a technical outage
    d. A process for regularly evaluating the effectiveness of such measures

5. The responsibility to notify: In the event of a personal data breach, the *controller* must notify the appropriate authority **within 72 hours** of when the processor became aware of the breach *unless* the breach is unlikely to result in a risk to the rights and freedoms of a data subject
6. The responsibility to notify the data subject of the breach
7. Responsibility to get consent via a clear affirmative action from the data subject whenever personal data is collected.
8. Responsibility to conduct an impact assessment for new technologies.
9. Responsibility to comply with regulations governing transfer of data to parties outside the EU.

DATA PROTECTION OFFICER

Article 37 of GDPR indicates that all processors and controllers must appoint a ***Data Protection Officer***. The Data Protection Officer is an officer appointed by any organization systematically processing large amounts of personal data on data subjects. The DPO:

1. Educates and trains employees, vendors, clients and other contacts on the data privacy policies and procedures of the company
2. Conducts audits to ensure continued compliance with GDPR and company privacy policies
3. Serves as the point of contact between the company and the Data Protection Authorities in the EU28
4. Maintains records of all data processing
5. Consults with technical leadership on all new technological changes that may impact data storage, transmission, use and risk
6. Ensures that international transfers of data occur within the framework of the GDPR's adequacy and appropriate safeguard provisions

Note that there is no specific requirement for DPO's to have any licensing in any member nation, but they are required to have a deep understanding of GDPR.

RECOMMENDATION: Hire a DPO based on knowledge of US Data privacy regulations, including PCI, HIPAA, Gramm-Leach-Bliley, USA Patriot Act, Dodd Frank and regulations from the FFIEC and CFPB. Keeping a streamlined one-size-fits-all approach to GDPR and US regulations and having those policies roll up to the same compliance officer makes sense to prevent technology divergence.

IMPACT ON COMPANIES WHO DON'T ADVERTIZE SERVICES TO THE IMPACTED COUNTRIES

Are you impacted if, in the course of your normal business, you provide services to American consumers but don't have any specific blocks in place to prevent European Data Subjects from using your services? It depends. There is no simple answer and case law has yet to be tested. However, a good rule of thumb is to look at how you advertise your services. It would be difficult to argue in court that you are not advertising your services to the EU28 if for example:

1. Your website collects address information for credit card purchases and allows for EU28 countries to be selected
2. You perform IP blocks but you don't block EU28 IP Addresses
3. You send or receive text messages from EU28 phone numbers
4. You translate your website into EU28 languages other than English and Spanish
5. Your records, if examined, would indicate a large percentage of your business comes from the EU28
6. You allow EU currencies such as the Euro or British Pound to be used for payment

It would be a lot easier to argue if:

1. You ship physical merchandise and block shipping addresses in the EU28

2. You only offer services unlikely to appeal to EU28 residents (Like US Tax services for instance)
3. Your website is only in English

RECOMMENDATION: Take a conservative approach to determining if you need to comply. There is no need to comply if it would be clear to any reasonable person that you are making no effort to solicit business in the EU28. However, if a reasonable person would conclude that you do have users, clients, customers or other entities covered by GDPR, it's better to be safe than sorry. Maximum fines are EUR 20,000,000 per calendar year.

APPLICABILITY OUTSIDE THE EU

NORWAY

While Norway is not a member of the European Union, much of EU law applies in Norway through their association agreement with the EU, and Norway has confirmed that it will implement GDPR and establish a DPA.

SWITZERLAND

Switzerland is a landlocked nation surrounded by EU nations on all sides. As such, GDPR will have an enormous impact on Swiss business even though the Swiss Government has not implemented GDPR. On September 15th 2017, the Swiss Government instead announced that it would update its 40-year-old data protection act to align with GDPR. However, as of time-of-writing, there is no confirmation that the Swiss parliament will act, so this remains an area of uncertainty.

THE UNITED KINGDOM

On March 30th 2019, the United Kingdom will leave the European Union. It remains unclear what will happen next. The Conservative Party announced in August of 2017 new legislation that broadly aligns with GDPR, but it is not identical and it has not yet been implemented into British law. This means that it is possible that the UK will adopt GDPR in 2018 but then lose alignment with it the following year, creating a quagmire for Non-European companies with operations in the UK. A key area of difference with the British legislation is the right to have childhood data erased on the data subjects 18th birthday, applicable to social media companies. A key area of concern is that in the event of a so-called "hard BREXIT" where the UK exits the EU without a succession agreement, British companies will suddenly be subject to the GDPR's external data transfer requirements.

These include:

1. It is not lawful to transfer data outside the EU in response to a legal requirement from a third country.
2. The EU will have to make a legally binding "adequacy" decision to determine if data can be transferred to a third-party country at all
3. The Adequacy decision will be based in part on whether the privacy regime in the third country prevents data being passed on to additional destinations.
4. Amendments to GDPR tightened the definition of 'adequacy" to basically mean "equivalency". This means that even if the UK aligns with GDPR on day one, any further changes to British law could be detrimental to equivalency.

RECOMMENDATION: Assume that the UK will implement GDPR in 2018, but may also implement additional regulations (which are not barred under GDPR). Monitor BREXIT to see what will happen in March 2019. Specifically monitor for additional legislation under the UK's DPA, and keep abreast of the EU's position on external data transfer to the UK, as well as any reciprocal arrangement the UK may implement with the EU.

For American companies with lines of business in the UK, this represents some risk. Compliance with GDPR doesn't automatically mean compliance with UK law in the event that there is no succession treaty. For American companies with business in the EU27 but no business in the UK, this remains an area of uncertainty and contingency planning won't be possible until the regulatory framework of BREXIT is finalized.

It should be noted that there will be some pressure on both the UK and EU governments to minimize friction, and this creates a likelihood that issues related to GDPR will be resolved. However, the nature of the transition remains uncertain so this remains an area of uncertainty.

ICELAND

As a member of the European Economic Area, Iceland is obliged to implement GDPR.

EU OVERSEAS TERRITORIES

GDPR applies to overseas territories of EU member nations. While most EU nations do not maintain a significant amount of overseas territory, France, the Netherlands and the UK all do. Territories like French Polynesia, Aruba, Curacao, Greenland, the Cayman Islands, and any other territory of an EU nation will have to comply with GDPR.

EU APPLICANTS AND CANDIDATES

The GDPR does not apply to EU candidate countries until they are fully-fledged EU members. However, most EU candidate countries have either implemented aligned regulation (Turkey, Albania, Bosnia, Serbia) or are publicly debating it (Macedonia, Kosovo).

RECOMMENDATION: Assume that Non-EU nations will either implement GDPR or will align closely with it, and apply all GDPR rules across all of your European business. Assume that the data transfer rules will apply to all but the EU27.

COMPLIANCE TO-DO LIST

1. REORGANIZE DATABASES TO RECORD CONSUMER PREFERENCES

GDPR requires you to provide data subjects with the rights outlined earlier. This requires that you start logging what they agreed to and when. Come up with a data structure that allows users to securely:

a. Access their own personal data
b. Update their own personal data and correct any mistakes
c. Understand when you use it and what for
d. Delete their own data, subject to its necessity for reasonable business purposes
e. Allows them to give and withdraw consent for use of personal data for any of the purposes you use it for

This data structure should allow you to store, with a high degree of confidence, the specific text the user agreed to during consent. If your privacy terms change, the data structure should optimize the process for obtaining new consent for the amended terms. Where possible, align all of this with your domestic processes for ease of maintenance.

2. GAIN CONSENT

Implement a process for communicating with all new and existing customers and getting their consent to your data policies. Such consent needs to be "*clear affirmative action*" and devoid of complex legalese. Affirmative action means it cannot be a pre-checked box. The consumer must have to take an action to consent, like checking a box, or clicking an 'I agree' button. Give the user appropriate choices. If you use their information for processing, marketing and analysis, there should be three separate consents. Only mandate the ones that must be mandatory for the purposes of completing the transaction in which the user is presently engaged. Present the message positively. Remind the user that this is for their protection. Tell them you take their privacy seriously. Use this as an opportunity to spin the GDPR into a positive, gaining the users confidence in your platform.

3. HIRE A DATA PROTECTION OFFICER

This may seem like a no-brainer since it's mandatory, but the DPO will be responsible for all aspects of GDPR compliance on an ongoing basis, so get him or her on board as early in the process as possible. Bear in mind that there are no specific qualifications required, nor is it required that the DPO is a full-time employee. However, the DPO will be accountable to EU authorities so this should be a person who is deeply familiar with GDPR and data privacy in general.

4. PERFORM A ONE-TIME ORGANIZATION-WIDE DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The DPO's first job should be to understand the totality of an organizations data and assess the impact GDPR will have on existing data capture, storage, transmission and use. Create a one-time project plan to remediate issues and a delivery plan to implement prior to the May 25th 2018 deadline. This should include a plan to delete data that is no longer needed, encrypt data that is

5. IMPLEMENT ONGOING DATA PROTECTION IMPACT ASSESSMENT

The DPO's next job is to establish a process for ensuring continue compliance with GDPR for new products, technologies and procedures on an ongoing basis.

6. ESTABLISH CONTACT WITH THE DPA'S IN THE EU28

The DPO should establish contact with DPA's in the countries in Europe in which you do business.

Here is a complete list of all DPA's in the EU28:

http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

7. IMPLEMENT THE RIGHT TO BE FORGOTTEN

Establish a process by which a data subject can be forgotten. Remember that cost is a major factor in determining the method used. There is no specific requirement determining how to meet this requirement, so take the opportunity to implement the highest amount of automation possible. Don't keep data longer than necessary. Remove the data once it's no longer needed without the user's explicit instruction where possible. Give users the ability to retrieve notification of when their data was deleted. Pseudonymize data as soon as possible.

RECOMMENDATION: This is one area where divergence with the US might be preferable for many companies. In many instances, US law requires that certain data be kept on file for a period of time. For instance, US REG-E requires that financial activity is maintained on file for seven years.

8. CREATE ORGANIZATIONAL AWARENESS

Establish a training routine to educate organization members on all procedures related to GDPR. Mandate attendance and record employee training to ensure 100% compliance. Include this training in all new onboarding.

9. ESTABLISH CONTRACTUAL COMPLIANCE

Work with the company's legal team to ensure that all vendor and client contracts that have an impact on data collection, use, storage and destruction are modified to reflect their obligations. The legal team will also need to re-draft all consumer privacy agreements as part of step 1 above.

10. ESTABLISH OPERATIONAL COMPLIANCE

Work with the company's operations team to ensure that there are policies and procedures in place to meet each of the following operational obligations:

a. The obligation to notify the appropriate DPA within 72 hours of discovery of a breach
b. The obligation to notify the data subject when their data is breached
c. The obligation to ensure that all new technology has passed a Data Protection Impact assessment prior to implementation.