What is the GDPR?

The General Data Protection Regulation

The General Data Protection Regulation, or simply GDPR, will be the European Union's primary privacy regulation.

Led by the European Parliament, the Council of the European Union, and the European Commission, the GDPR is set to go live in May 2018.

Does the GDPR Apply to Me?

Yes, if you do any of the following:

- Data Transfer
- Analytics
- Behavioral Advertising
- Geo-Location Monitoring
- Cloud Storage

By: Joel Thayer and Alex Cooke
Illustrations by: Eric Gagnier

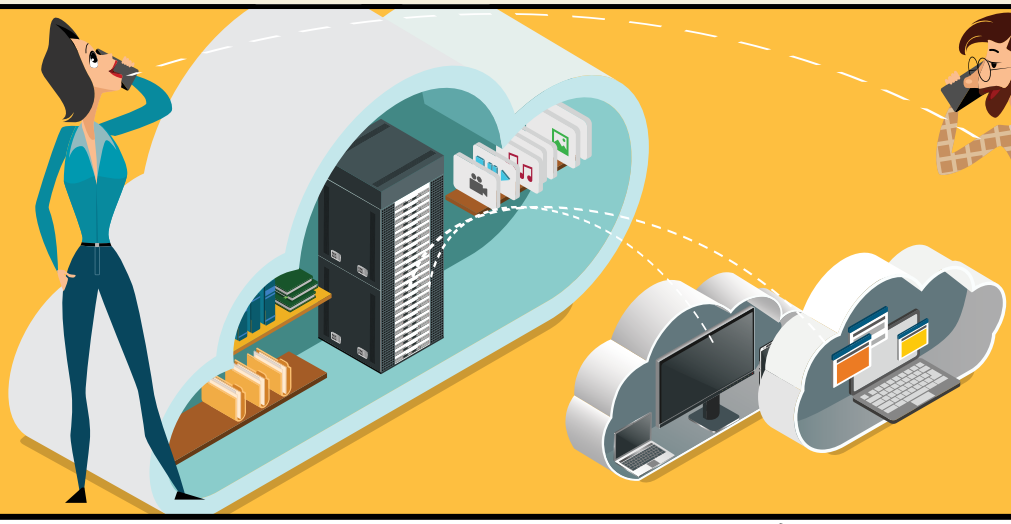
TABLE OF CONTENTS

Are You a Controller? Processor?...Both?

CARRIE "Controller"

Controller - The natural or legal person, public authority, agency, or other body that determines the purpose and means of the processing of personal data. When the purposes and means of data processing are determined by the European Union or member state law, they may also provide the specific criteria for its nomination.

Carrie runs a business that relies on the collection of her customers' data, the use of which she solely controls. The GDPR considers Carrie a "Controller", because she collects and determines the use of her customers' data.



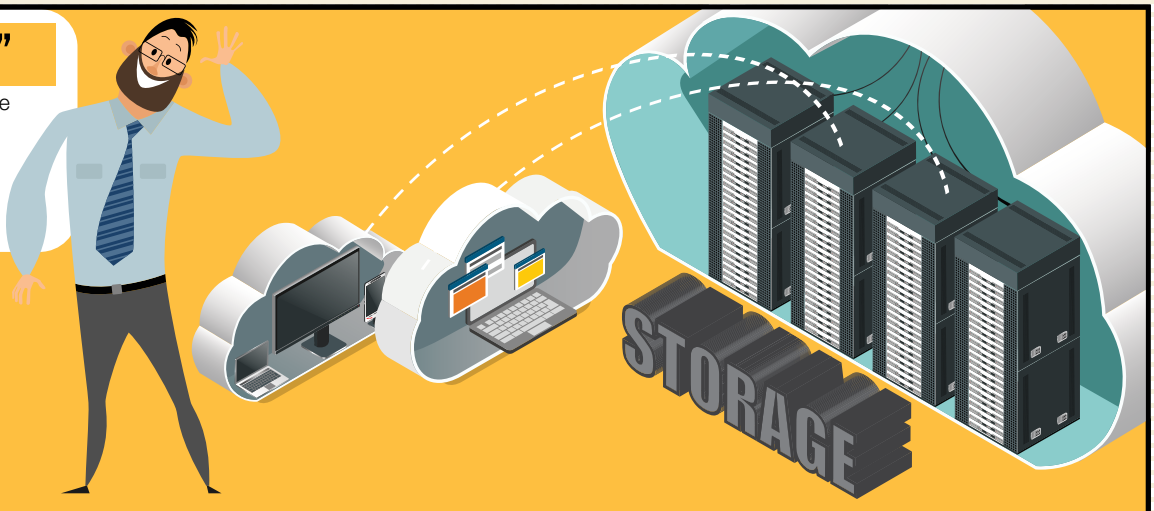
PIERRE "Processor"

Processor - A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

Pierre is a subcontractor of Carrie and runs a cloud service. He helps Carrie move and store the data she controls. The GDPR considers Pierre a "Processor", because he processes data on behalf of Carrie, but does not control how the data is used.

ANDY "Analytics"

Under the GDPR, it is possible for the EU government to consider you a "Co-Controller".



Andy is customer of Carrie. Andy purchases Carrie's data to analyze and sell to third parties for various purposes. Though Andy uses data collected by Carrie, he determines a use for the data that is completely independent of Carrie. The GDPR would categorize Andy a "Co-Controller" with Carrie.

Whom Does the GDPR Impact?

Does the GDPR Apply to Me?

Unless you never, ever, ever deal with the personal information of an EU subject, the GDPR applies to you.

It does not matter whether your business is physically located in the EU. The GDPR is not based on the location of your company, but whether your company manages, transfers, or stores any personal information of an EU subject.

Am I Collecting EU Citizens' Personal Data?

Article 4 of the GDPR defines personal data as "any information related to a natural person [within the EU]" used to "directly or indirectly" identify the person. According to the GDPR, this information can include "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." This definition is broad and can easily apply to any app developer who maintains, stores, collects, or distributes this data. For example, companies that collect analytics concerning an EU subject's personally identifiable information (PII) are beholden to the GDPR rules as data collectors.

Do I Need to Have a Physical Presence Across the Pond?

If you consistently hold or process data on an EU subject, the GDPR will require your company to have a physical presence, or appoint a representative, in the EU. The regulation's Article 27 requires any processor or controller that is not based in the EU, but continues to process or maintain an EU subject's PII to "designate in writing a representative in the [EU]."

However, Article 27 does not apply if the frequency with which your company processes the EU subject's data is "occasional," and the data does not include any of the "special categories" of personal information, like a person's racial or ethnic origin, or political orientation. Unfortunately, the EU has not defined the term "occasional." We have reason to believe the EU may consider the frequency of a company's constant geo-location activities to be more than an "occasional" interaction. Regardless, ahead of the introduction of the GDPR, you should be aware of how and how frequently your company collects the PII of an EU subject.

How Do I Prepare?

You Must Seek Consent

The GDPR has strict rules regarding consent. The regulation requires consent be given in "an intelligible and easily accessible form with the purpose for data processing attached to that consent." The GDPR requires companies to ensure that information concerning terms of service and the treatment of an EU subject's data is written in clear, plain English and is distinguishable from other matters. The company must also provide easy mechanisms for EU subjects to withdraw their consent, instead of forcing them to go through unnecessary hoops.

Under GDPR, the Age of Consent Can Be as Low as 13

Article 8 of the GDPR requires parental consent to process the personal data of children under the age of 16. EU member countries have the autonomy to lower the age for which parental consent must be given but not below 13 years of age. App companies and tech innovators who provide apps for children should pay close attention to this threshold age.

You Must Protect the Data "by Design and by Default"

There are serious outstanding questions as to how and when the EU will hold a controller or processor liable for the data they handle. For example, GDPR's "Data Protection by Design and by Default" requirement under Article 25 mandates controllers to safeguard consumer data by "appropriate" technical means. The term "appropriate" includes "state of the art" methodologies, however, the EU has not defined the term "appropriate" or the responsibility it bestows on app developers.

CONSENT IS KEY

Article 9 of the GDPR requires a controller or processor to obtain explicit consent from the EU subject when processing any information that falls into any of the special categories personal data. This means an app company must receive an explicit opt-in from the EU subject before the company can process this type of data.

The (Contractual) Relationship Between Controllers and Processors

Under the GDPR, controllers of data and processors of data should have a contractual relationship. Controllers should always request an indemnification clause and receive written assurance of "sufficient guarantees" of GDPR compliance before selecting a processor. Processors should always play the game of Mother, May I with controllers' data.

Art. 28 requires that a controller only contract with processors that can provide "sufficient guarantees" of GDPR compliance. If the controller receives these guarantees, and there is a breach that results from the processor's doing, the GDPR could potentially hold the processor directly liable. In addition, a processor cannot hire a sub-processor without the controller's prior consent and written contract.

Art. 32 requires that a processor take "appropriate" measures to ensure a level of security for controllers' data. In addition, a processor cannot hire a sub-processor without the controller's prior consent and a written contract to that effect.

Yo, Do I Need a DPO?

The bar is high for this requirement and ultimately depends on the type of data and how it's used. A data protection officer, commonly known as a "DPO," refers to a company employee who reports directly to the board of directors, possesses "expert knowledge of [EU] data protection laws and practices," and can educate and train the company's employees on the GDPR's requirements. For more information, please visit the appendix dedicated to DPO requirements.

You Suffered a Data Breach in the EU; Now What?

Article 4 of the GDPR defines a "personal data breach" as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." A company's next steps in the face of a data breach in the EU depend on whether it is classified as a controller or a processor under the GDPR.

Article 33 outlines the distinct responsibilities of both a controller and processor:

If a controller's system determines a breach in the system, then it must notify the supervisory authority "without undue delay," no later than 72 hours "after becoming aware of the breach." However, a notification is not required if the breach is "unlikely to result in a risk to the rights and freedoms of [an EU subject]."

A processor must notify the controller without "undue delay" once it "becomes aware of a data breach." Processors do not have the 72-hour backstop to the notification requirement.

What Happens if I Infringe a GDPR Provision?

The GDPR also provides a tiered structure for fines, depending on the severity of the offense. For example, under Article 28, a supervisory authority can impose a 2 percent fine on a company for not conducting an impact assessment or failing to maintain records needed to notify the supervisory authority.

The GDPR has a maximum penalty of 4 percent of a company's annual global revenue or €20 million (whichever is higher) for violating any provision of the GDPR.

What You Should Do

Whether you're an app developer, innovator, small business, or somewhere in between, we strongly encourage you to undertake the following fundamental actions to ensure you are compliant with the GDPR.

1. Build privacy and security measures into your products from the start because the GDPR requires "data protection by design and default." You should undertake Data Protection Impact Assessments as needed, and document your work.
2. Determine whether you process or control any personal data on EU subjects, or if you plan to in the future.
3. Ensure that your staff and leadership are aware of the GDPR and understand specific responsibilities to meet the regulation's requirements.
4. Document all the types of data held and processed by you and your contractors to identify personal data.
5. Audit your processes according to every right provided to an EU subject under the GDPR, even if you are certified and compliant under the U.S.-EU Privacy Shield. If you identify a right that your processes cannot address, revise accordingly.
6. Audit your data processing practices according to laws identified in the GDPR. If you cannot identify a lawful basis for the processing activity within the GDPR, ask critical questions about why the activity is being undertaken.
7. Provide EU subjects access to their data that you hold, and be mindful of the GDPR's related requirements regarding data. Clearly craft your privacy policies to disclose how your company uses the data it collects and the lawful basis for its processing.
8. Make sure your methods of obtaining consent are consistent with the GDPR. Remember, consent must be freely given by informed subjects, and requests for consent must be clearly and prominently featured. Under the GDPR, consent must be opt-in.

    a. If you hold or process children's data, ensure that you take the additional steps needed to attain parental consent before processing.
9. Keep detailed records – not just of the personal data and the processes performed, but also of efforts to improve internal processes to align with the GDPR's requirements.
10. Ensure that you have a reliable system to prevent, detect, and mitigate data breaches. In the event of a breach, make sure you are aware of what supervisory authority you must report to within a 72-hour window, and how to notify at-risk individuals.
11. Hold all contractors to account for GDPR responsibilities, clearly and in writing, before conducting business with them.
12. Designate a qualified person to fill the role of DPO if your company processes personal information. Even if your company is not required to appoint a DPO, it doesn't hurt to have an informed expert with a physical presence in the EU.
13. If you are not based in the EU but collect or process EU subjects' data and personal information, identify your lead data protection authority to ensure you meet the presence requirements within a specific jurisdiction.

Key Things To Know

New Rights of EU Data Subjects That Every App Developer Should Know

We encourage you to familiarize yourself with the new rights and features introduced with the GDPR:

Right to Access

As outlined by the GDPR, the expanded rights of data subjects include the right for EU subjects to be informed when, where, and why their personal identifiable data is being processed. Further, the controller must take a few additional steps to provide a free copy of the personal data in a readable electronic format.

Right to Data Erasure

Also known as a "right to be forgotten," the right to erasure allows EU subjects to request the data controller to erase his/her personal data, cease further dissemination of the data, and have third parties halt further processing of the data. The GDPR imposes enumerated duties on the controller or processor under compliance with this right.

For example, the right requires a company to erase an EU subject's PII when the company is no longer using the information, or it is irrelevant to original purposes for processing. In addition, when an EU subject requests data, the controllers must consider the subject's rights to "the public interest in the availability of the data."

Data Portability

GDPR introduces data portability, the right for a data subject to receive their personal identiable data in a "commonly used and machine-readable format." The GDPR also grants the data subject with the "right to have the personal data transmitted directly from one controller to another, where technically feasible." The controller or processor must adhere to any request subject to this right as long as it "does not adversely affect the rights and freedoms of others."

Right Against Automated Decision-Making aka The Right Against Profiling

The GDPR provides EU subjects with the right to "not be the subject to a decision based solely on automated processing" that could legally affect him or her. For example, this has clear implications for developers engaging in machine learning. However, it is unclear how EU authorities will apply this right in that context, and we will have to wait for further guidance. To ensure the integrity of these rights, the GDPR requires data controllers to "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."

Government Access to Data Under the GDPR

The GDPR's Article 48 loosely defines when and how non-EU member governments can access an EU subject's data. The article states that a GDPR-compliant company can only comply with a judgement, such as a warrant, "requiring a controller or processor to transfer or disclose personal data" of an EU subject if the judgment is "based on an international agreement," like a mutual legal assistance treaty (MLAT), "in force" between the EU and the "requesting third country." The United States and the EU have an existing MLAT agreement. As a result, compliance with any U.S. law enforcement-issued warrant or process seeking personal data, in a manner that is not based on the MLAT, could trigger liability under Article 48.

Additional Information

EU Glossary of Relevant Terms

Binding Corporate Rules (BCRs) - a set of binding rules established to allow multinational companies and organizations to transfer personal data from within the European Union to organization affiliates outside the EU.

Biometric Data - personal data relating to the physical, physiological, or behavioral characteristics of an individual which enables their unique identification.

Consent - the act of freely providing specific, informed, and explicit agreement via statement or action which signals agreement to the processing of their personal data.

Controller - the natural or legal person, public authority, agency, or other body that determines the purpose and means of the processing of personal data. When the purposes and means of data processing are determined by the European Union or member state law, they may also provide the specific criteria for its nomination.

Data Concerning Health - any personal data related to the physical or mental health of an individual or the health services provided to him or her.

Data Controller - the entity that determines the purposes, conditions, and means of the processing of personal data.

Data Erasure - also known as the Right to be Forgotten, entitles the data subject to mandate the data controller to erase his or her personal data, cease further dissemination of the data, or have third parties cease processing of the data.

Data Portability - the requirement that controllers provide data subjects with a copy of his or her data in a format that allows for easy use and portability among other controllers. "More information here."

Data Processor - the entity that processes data on behalf of the data controller.

Data Protection Authority - national authorities tasked with the data privacy and protection. The authority also monitors and enforces data protection regulations within the European Union.

Data Protection Officer - an independent data privacy expert who works with companies to ensure they are adhering to the policies and procedures set forth in the GDPR. "More information here."

Data Subject - a natural person whose personal data is processed by a controller or processor.

Delegated Acts - non-legislative actions implemented to supplement or provide clarity to existing legislation.

Derogation - an exemption from a law.

EU Glossary of Relevant Terms

Directive - a policy goal all European Union member countries must meet through their own national laws.

Encrypted Data - data protected through technological measures to ensure the data is only accessible to entities with specified access.

Enterprise - any entity engaged in economic activity, including people, partnerships, associations, etc.

Filing System - any set of personal data that is made accessible via specific criteria or query.

Genetic Data - data regarding the inherited or acquired characteristics of an data subject which provide unique information about his or her health or physiology.

Group of Undertakings - a controlling undertaking and its controlled undertakings.

Main Establishment - the place within the European Union where a company makes the main decisions about data processing. This term refers to actions by the processor.

Personal Data - any information related to a natural person or data subject that can be used to directly or indirectly identify the person.

Personal Data Breach - a breach of security that leads to the accidental or unlawful access to, or destruction or misuse of, personal data.

Privacy by Design - a principle that calls for the inclusion of data protection at the inception of a system's design, rather than as a feature added later.

Privacy Impact Assessment - a tool used to identify and reduce privacy risks by analyzing the personal data being processed alongside the policies in place to protect the data.

Processing - any operation performed on personal data. The term includes automated operations, including the collection, use, and recording of data.

Processor - a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

Profiling - any automated processing of personal data for the purposes of evaluating, analyzing, or predicting the behavior of a data subject.

Pseudonymisation - the processing of personal data to ensure it can no longer be attributed to a single data subject without the use of additional data. The additional data must remain separate to ensure non-attribution.

Recipient - the entity to which personal data is disclosed.

EU Glossary of Relevant Terms

Regulation - a binding legislative act that must be applied in its entirety across the European Union.

Representative - any person in the European Union explicitly designated by the controller to be addressed by the supervisory authorities.

Right to be Forgotten - also known as "data erasure," entitles the data subject to mandate the data controller to erase his or her personal data, cease further dissemination of the data, or have third parties cease processing of the data.

Right to Access - also known as "Subject Access Right," entitles the data subject to access any personal data the controller may have gathered about her or him.

Special Categories of Personal Data - refers to data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. This also includes the processing of genetic data, biometric data for the unique purpose of identifying a natural person, data concerning health, or data related to a person's sex life or sexual orientation.

Subject Access Right - also known as the "Right to Access," entitles the data subject to access any personal data the controller may have gathered about her or him.

Supervisory Authority - a public authority established by an EU member state, in accordance with Article 46.

Trilogues - informal negotiations between the European Commission, the European Parliament, and the Council of the European Union, usually held following the first readings of proposed legislation to expedite agreement on a compromise text.

References

European Union, GDPR Portal (2017), https://www.eugdpr.org/

Alex Fugairon, How the GDPR and Privacy Shield Regulations Relate—and What They Mean for your Business, PivotPoint Security (Jul. 13, 2017), https://www.pivotpointsecurity.com/blog/gdpr-privacy-shield-regulations/

Alex Reynolds, GDPR Matchups: US State Data Breach Laws, iapp (May 10, 2017), https://iapp.org/news/a/gdpr-match-up-u-s-state-data-breach-laws/

European Union, GDPR Portal (2017), https://www.eugdpr.org/

Sean Baird, GDPR Matchup: The Health Insurance Portability and Accountability Acti, iapp (May 17, 2017), https://iapp.org/news/a/gdpr-match-up-the-health-insurance-portability-and-accountability-act/

Tay Nguyen, GDPR Matchup: The Children's Online Privacy Protection Act, iapp (Apr. 17, 2017), https://iapp.org/news/a/gdpr-matchup-the-childrens-online-privacy-protection-act/

Working Party 29, U.S. Privacy Shield Draft Adequacy Decision, Opinion (2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

Appendix A

GDPR and EU-U.S. Privacy Shield: Same, but Very Different

So, back in the day (July 2016 to be exact) the U.S. Department of Commerce and the European Commission approved the EU-U.S. Privacy Shield to support transatlantic digital data flows. The Privacy Shield was designed to help companies comply with EU data protection requirements when transferring personal data from the European Union to the United States. U.S. companies have the choice to self-certify through a process overseen by the Department of Commerce's U.S. International Trade Administration. The Privacy Shield allows American companies, particularly those subject to the jurisdiction of the Federal Trade Commission (FTC) and Department of Transportation (DOT), to voluntarily participate in the program if they import personally identifiable information from the EU. Even though the Privacy Shield deals with similar data flows between the EU and the United States, the GDPR's extraterritorial nature will still likely hold companies liable, even if they self-certified under the Privacy Shield.

It can be dangerous to assume that Privacy Shield certification equates to GDPR compliance; we strong advise against that assumption.

It can be dangerous to assume that Privacy Shield certification equates to GDPR compliance; we strongly advise against that assumption. At this stage, it is difficult to predict how articles within the GDPR relate to EU-U.S. Privacy Shield. Even though the Privacy Shield is intended to facilitate extraterritorial data transfers from the EU to the United States, the GDPR has an extraterritorial provision that extends to EU subjects data even beyond the borders of EU, as outlined in Article 3(1). This seems to imply that the provisions of the GDPR preempt that of EU-U.S. Privacy Shield, but, again, we will need further clarification from the EU to be certain.

Among the many unanswered questions about the GDPR's relationship to the Privacy Shield, two stand out:

Do entities currently certified under the Privacy Shield meet some, or all, of the GDPR's requirements?

The EU Article 29 Working Party (WP29), the EU working party advisory group focused on data protection compliance (and independent of official European Commission policymaking), recently advised that Privacy Shield guidelines did not adequately comply with all aspects of the GDPR. For example, the WP29 argued that the Privacy Shield's guidelines did not align with the GDPR's new notions about the right to data portability or "additional obligations on data controllers, including the need to carry out data protection impact assessments and to comply with the principles of privacy by design and privacy by default…" The WP29 noted that these are GDPR-specific concepts not yet conceived at the time of the Privacy Shield's development and implementation.

How will compliance with the Privacy Shield and GDPR affect FTC and DOT enforcement in the United States?

The role of FTC and DOT is straightforward for those currently certified under the Privacy Shield. If a company makes a false claim about Privacy Shield certification, or is successfully certification but not in compliance with the Privacy Shield's guidelines, then the FTC can take (and has taken) enforcement actions to combat and prevent this deception. It is unclear what effect Privacy Shield certification will have when evaluating how it factors into overall compliance with the GDPR, but we hope the EU provides guidance to that effect. It is clear that these policies are different, so we discourage making absolute claims about compliance with the Privacy Shield or the GDPR.

Appendix B

GDPR's Relationship to U.S. Privacy Law

A. Breach Laws

U.S. Law	GDPR
Breach Notification Process Requirement • The United States currently does not have a federal breach notification requirement. States impose individual notification deadlines with varying length.	**Breach Notification Process Requirement** • The GDPR imposes a uniform breach notification deadline for all EU member countries.
Definition of Breach • The United States does not have a uniform definition of a breach. • States individually define the concept of a breach, which can include the unlawful disclosure or retrieval of Social Security Numbers, government-issued ID numbers, bank account numbers, or other financial material.	**Definition of Breach** • GDPR uniformly defines a "personal data breach" as the unlawful retrieval or disclosure of "any information relating to an identified or identifiable natural person." This includes any information that can identify a person online.
Harm Threshold • Most state laws do not have a "harm" threshold in the event of a breach; instead, they have reporting requirements when a safe harbor does not exist. • States without a "harm" threshold usually link the threshold to the likelihood of financial harm.	**Harm Threshold** • The GDPR has two harm thresholds: 1) for supervisory authority notifications, harm is determined by whether the breach "is unlikely to result in a risk to the rights and freedoms of natural persons;" 2) for consumer notifications, harm is determined by whether the breach is "likely to result in a high risk to the rights and freedoms of natural persons."
Timing Requirements • Most states impose a "no unreasonable delay" standard for notifications. States with hard deadlines can range from 30 to 60 days or from the time of the breach discovery.	**Timing Requirements** • Companies have 72 hours "after they become aware," and without "undue delay," to report the breach to a supervisory authority.
Requirement to Maintain Records • In the event of a personal data breach, the United States does not have a requirement to maintain records to verify legal compliance.	**Requirement to Maintain Records** • In the event of a personal data breach, the GDPR requires the breached entity to maintain and submit records to the supervisory authority to ensure their compliance with Articles 33 and 34, pertaining to notification requirements.
How to Notify Authorities • The United States does not have a presiding format on how to notify regulators. However, most states require some form of written notice.	**How to Notify Authorities** • The GDPR does not define the format by which a company should notify a supervisory authority, but requires them to "notify" the supervisory authority and "communicate" the exchange with the data subject in it.

Appendix B

GDPR's Relationship to U.S. Privacy Law

B. Children's Online Privacy Protection Act (COPPA)

U.S. Law	GDPR
Age of Consent • Under COPPA, the age of consent is 13 years old.	**Age of Consent** • Under the GDPR, the age of consent is 16 years old. Member states have discretion to lower the age of consent as long as it is not below 13 years old.
Parental Consent • COPPA requires companies with content directed at children, and which seek information from children, to "clearly and comprehensively describe how personal information collected online from kids under 13 is handled" within their privacy policy. Before collecting any data, the company must clearly state that it intends to collect personal information, as defined by COPPA, and seek "verifiable" parental consent.	**Parental Consent** • The GDPR does not provide exhaustive guidance regarding parental consent. However, they encourage the controller of data to take reasonable efforts to seek parental verification.
Parental Access • Under COPPA, parents have an explicit right to know how the app developer and others collect and use their child's PII. COPPA equates the child's right to privacy with the parent's right to privacy. • Companies must also prominently post a link to the data collection policy in all places where the app collects said information. • Companies' privacy statements must provide "a list of all operators collecting personal information; a description of the personal information collected and how it's used; and a description of parental rights" in simple, accessible language.	**Parental Access** • The GDPR does not provide insight on the issue of parental access, nor does it provide a standard on the topic.

Appendix B

C. Health Insurance Portability and Accountability Act (HIPAA)

U.S. Law	GDPR
Protected Information • HIPAA protects a patient's "personal health information (PHI)." PHI represents any individually identifiable information related to past or present physical or mental health condition, the healthcare provided, or the payment of healthcare.	**Protected Information** • The GDPR's "data concerning health" (DCH) is similar to HIPAA's "personal health information" (PHI). • DCH refers to "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."
Processing Health Information under GDPR • Under HIPAA, "use" means "the sharing employment, application, utilization, examination, or analysis of such inform mation within an entity that maintains such information." • HIPAA defines "disclose" to mean "release, transfer, provision of access to, or divulging any manner of information outside the entity holding the information."	**Processing Health Information under GDPR** • Under the GDPR, "processing" is an extremely broad concept. It is relatively similar to the HIPAA concept of "use and disclose," because it is an amalgam of the two concepts. • The GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."
Covered Entities • Narrowly defined as any entity that is a healthcare provider that electronically transmits PHI in connection with a HIPAA-recognized healthcare service (e.g., e-billing, a health plan, or a healthcare clearing house).	**Covered Entities** • Any entity collecting related health information, irrespective of the location of the entity.

Appendix C

Data Protection Officers (DPOs): When Do You Need One?

Article 37 of the GDPR requires either a controller or a processor to designate a DPO in one of the three following instances:

- "the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;"
- the company's core activities include "regular and systematic" monitoring of EU data subjects "on a large scale;" or
- the company's core activities include the "regular and systematic" monitoring of special categories of data or criminal convictions and offenses of EU data subjects "on a large scale."

If an app company's data collection procedures include any of these practices, then they must appoint a DPO in their company. The app company must publish the DPO's contact information so as to make that person accessible to any supervisory authority.

Under Article 37 and 39, a DPO must:

- be appointed on the basis of "professional qualities and, in particular, expert knowledge on data protection law and practices;"
- be "a staff member or an external service provider;"
- provide their contact details to the relevant Data Protection Authority;
- cooperate with EU supervisory authorities;
- receive appropriate resources to carry out tasks and maintain expert knowledge;
- "report [directly] to the highest level of management;" and
- not carry out "any other tasks that could results in a conflict of interest."