GDPR

a practical guide for the small business

Law Office Of S. Grynwajc
Transatlantic Legal Services

INTRODUCTION

Because we specialize in helping startups and small businesses comply with the GDPR, we wanted to design a GDPR Glossary of terms that speaks to small businesses, not large multinational companies with an army of lawyers able to decipher the GDPR for them. We wanted to avoid what too many GDPR glossaries already do by simply reproducing the definition in the text of the GDPR (which anybody can do, and often isn't very helpful) and, instead, take a different and, we hope, more disruptive approach, and explain some of the most commonly found GDPR terms in non legalese, plain English, and in the context in which they are most relevant.

We are European lawyers practicing in the U.S. As such, we are used to having to explain in plain language EU legal concepts to U.S.-based companies that aren't familiar with the laws of the EU. Some of the terms used in the GDPR are very complex, and also not very well defined as it is under the Regulation. We hope that our Glossary will help eliminate some of that complexity. Enjoy the reading !

WHAT IS THE GDPR?

GDPR, which stands for the General Data Protection Regulation, is a European legislation which came into effect on May 25, 2018, replacing the EU Privacy Directive (95/46/EC) of 1995. This regulation imposes strict new rules for any organization or business coming in contact with the personal data of EU residents, regardless of where the organization is located.

WHAT IS A REGULATION V. A DIRECTIVE?

Regulations and directives are two instruments used to pass legislation at the EU level. A directive is a legislative act that expresses a goal but permits each individual member state of the EU to determine the means of how they will achieve that goal, thereby leading to as many sets of rules as there are member states in the EU. On the other hand, a regulation is automatically applicable to all EU member states and becomes the law of the land across the EU. The GDPR is unique in that, although it is a regulation, it is an incomplete regulation, and provides, in more than 50 areas, the right for member states to adopt revisions or supplemental rules to those of the GDPR. These national exceptions are commonly referred to as national derogations.

WHEN DOES THE GDPR APPLY?

The GDPR applies to organizations located within the EU or organizations located outside the EU that process personal data of EU residents when offering them goods or services, or that monitor the behavior of EU residents.

HOW DO I BECOME COMPLIANT WITH THE GDPR?

To comply with the GDPR, companies processing the personal data of EU residents must not only comply with GDPR, but also with any applicable national derogations. If they use cookies or use the personal data of EU residents for marketing purposes they also need to comply with another EU legislation, the E-Privacy Directive of 2002, as well as all applicable national privacy legislations implementing that directive into national law.

HOW TO USE THIS GLOSSARY ?

This glossary of GDPR terms is alphabetical. Within each definition, terms in red refer to terms separately defined within the glossary. In the right column, for ease of reference, we have included the associated article of the GDPR. We hope that the structure as a table will facilitate the reading and understand the interaction between the various key provisions of the EU regulation.

Term	Definition	Article
Adequacy finding	An Adequacy finding is a decision by the EU that the privacy law of a particular country outside the European Union is substantially equivalent and protective of **personal data** as EU law to permit the free transfer of data from the EU to that country without the need to comply with any additional requirements. Adequacy findings are reviewed every 4 years. 13 countries have so far been approved under an Adequacy finding, the latest being the UK.	
Binding Corporate Rules (BCR)	Internal rules for multinational groups which, when implemented, guarantee data transfers within the group are GDPR compliant. To have approved BCR's, an organization must apply for authorization from one of the EU's **Data Protection Authorities ("DPA")**. BCRs do not guarantee compliant data transfers outside of the group. BCRs are one of the three main methods for validly transferring EU data outside the European Economic Area, the other main ones being an **Adequacy finding** by the **EU Commission and the EU Standard Contractual Clauses**, aka the "**Model Clauses**". The **EU-U.S. Privacy Shield Framework** belonged in that category in respect of transfers to the U.S., but is no longer approved as a valid mechanism for transferring EU personal data after its invalidation by the Court of Justice of the EU in July 2020."	**Art. 47**
Biometric Data	This is one of the new categories of personal data that is now expressly stated as one of the **"Special Categories of Data"** under the GDPR. Biometric Data refers to identifiable data related to physical, physiological, or behavioral traits. This includes facial scans, fingerprints, and retinal scans.	**Art. 4 §14 Art. 9**

Term	Definition	Article
Consent	One of the 6 legal bases for processing personal data under the GDPR. To be deemed valid, consent must be freely given, be specific, affirmative, and informed. For example, if you are requesting to store and use someone's personal data, they might need to opt-in to such collection through clear and separate opt-ins for each instance of data collection. Please note that consent is not always required. Processing may be lawful without consent if it falls under one of the other Article 6 categories of lawful processing.	**Art. 4 §11 Art. 7**
Controller **or Data Controller**	Whoever decides what data is collected, the way it is collected, and how it is used. This can include individuals or "legal persons" such as companies or organizations. As a general rule, any organization that operates a website through which the personal data of EU residents is collected is deemed a data controller. Controllers have an obligation to make sure that their service providers who have access to the personal data of EU residents (aka "**data processors**" or "**processors**") also comply with the GDPR.	**Art. 4 §7 Art. 24**
Data Protection Authority ("DPA")	AKA "Supervisory Authority" Each European country ("Member State") has their own authority responsible for enforcing the GDPR.	**Art. 4 §21 Art. 51**

Term	Definition	Article
Data Protection Officer (“DPO”)	Person formally appointed to be responsible for compliant data processing practices within a company or organization. Under the GDPR, you must appoint a DPO if: - you are a public authority or body (except for courts acting in their judicial capacity) - your core activities require **large scale, regular and systematic monitoring of individuals** - your core activities consist of **large scale processing of special categories of data** or data relating to criminal convictions and	**Art. 37 Subject to National Derogations**
Data Processing Impact Assessment	AKA “DPIA” Prior to processing personal data, Controllers are required to assess the privacy risks of their processing methods when their processing is likely to result in a high risk to the rights and freedoms of the data subjects. DPIA’s are required where the processing involves: - **profiling** data subjects - **large scale processing** - **regular and systematic monitoring of publicly accessible areas on a large scale** DPIA’s should include: - A description of processing operations - The purpose of processing - An assessment of the balance between the purpose and the necessity and proportionality of processing - An assessment of the risks to the rights and freedoms of data subjects - Steps to address the risks, including security mechanisms and safeguards	**Art. 35 Subject to National Derogations**

Term	Definition	Article
Data Subject	A person within the EU whose information is being processed. Data subjects covered by the GDPR physically reside in a European member state while their personal data is being processed.	**Art. 4 §1**
EU Representative	Companies or organizations that are not based in or do not have a physical presence in the EU must appoint a representative physically in the EU. The representative acts as the point of contact for DPA's and data subjects. Exceptions to appointing a representative include: - Personal data is only processed occasionally - Processing doesn't include **large scale processing** of **special categories of data** - Processing doesn't include personal data related to criminal convictions - Processing won't result in risk to the rights and freedoms of data subjects	**Art. 27**
European Economic Area	The European Economic Area consists of all 28 Member States in addition to Lichtenstein, Iceland, and Norway.	

Term	Definition	Article
E-Privacy Directive	AKA “the cookies directive” The 2002 E-Privacy Directive. This directive, currently the subject of a draft Regulation aimed at replacing it, focuses on protecting internet users’ privacy by requiring websites to obtain user **consent** and provide users with control over when and why they are being tracked by **cookies**.	
Extra-territorial Effect	Before the GDPR, companies with no employees, offices or processing facilities, e.g., servers located in the EU would generally not be subject to the EU Privacy Directive. The GDPR goes further and covers any organization, anywhere in the world, that either (1) offers “goods or services” to EU users or (2) “monitors the behavior” of EU data subjects.	
General Data Protection Regulation	AKA “GDPR” European legislation which came into effect on May 25, 2018, replacing the **EU Privacy Directive (95/46/EC) of 1995** which imposes strict new rules for any organization or business coming in contact with the personal data of EU residents, regardless of where the organization is located.	
Genetic Data	Another new category of data that is now expressly stated as one of the “**Special Categories of Data**” under the GDPR. Genetic Data refers to identifiable data concerning data subjects’ gene sequences.	**Art. 4 §13**

Term	Definition	Article
Large Scale Processing	Large scale processing is not defined by the GDPR. Considerations in determining whether processing meets this standard include: - Number of data subjects - Volume of data / range of personal data types processed - Duration or permanence of processing activity - Geographical extent of processing activity Examples of large scale processing include: - Travel data of individuals using public transportation systems - Geo-locations of customers in multiple locations of an organization - Customer data in regular course of business for insurance companies or banks - Personal data for behavioral advertising - Patient data in a hospital When an organization processes data on a large scale they are required to designate a **DPO**.	**Art. 37 Subject to National Derogations**
Member States	Members states are subject to the GDPR and include the following 27 countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden. As a result of the UK decision by referendum to leave the EU (aka "Brexit"), the United Kingdom is no longer a Member State	

Term	Definition	Article
Legitimate Interest	Legitimate interest is one of the 6 lawful bases for processing personal data under the GDPR. This standard is very flexible but also unclear for controllers. A 3-part test must be used to determine if your processing qualifies as a legitimate interest: **Purpose**: Is there a legitimate purpose for the processing? **Necessity**: Is this type of processing necessary to accomplish that legitimate purpose? **Balance**: Is this legitimate interest strong enough to override the **data subjects' rights** ? Examples of legitimate interests include fraud prevention, ensuring security, or identifying criminal or public security threats. Other processing like direct marketing and employee data transfers might be legitimate based on why and how it's being done.	**Art. 6 §1 Subject to National Derogations**
National Derogations	Certain provisions of the GDPR allow member states to add or modify the terms of the Regulation as they are applied to residents of their country. More than 50 provisions of the Regulation grant the member states the right to provide their own rules. Companies with data subjects in multiple member states should be familiar with the derogations of those member states before processing data of those residents	**Art. 23**

Term	Definition	Article
Personal Data	Any information that can be used to directly or indirectly (i.e., alone or in combination with other information) identify an individual, including: Full name Home address Email address, including a business email address National identification number Passport number Vehicle registration plate number Driver's license number Face, fingerprints, or handwriting Credit card numbers Date of birth Birthplace Genetic information Telephone number Login, screen name, nickname, or handle IP-address Device IDs, User ID, and Cookie ID Pseudonymous data This is distinguishable from 'Personally Identifiable Information' which has a narrower definition in the US.	**Art. 4 §1**

Term	Definition	Article
Privacy Shield	The EU-U.S. Privacy Shield was a self-certification mechanism designed in 2016 as an approved means for transferring personal data from the EU to the U.S. Until its invalidation by the Court of Justice of the EU on July 16, 2020, it was one of three main methods for validly transferring EU data outside the European Economic Area, the others being **BCRs** and the **Standard Contractual Clauses**, **aka the "EU Model Clauses"**. Please note that registering as a self-certified organization under the Privacy Shield did not mean you were GDPR compliant. The Privacy Shield only addressed the validity of the transfer of the personal data of EU residents from the EU to the U.S., which is only one of the requirements of the GDPR	
Processing	Anything done to personal data, including: collecting, storing, modifying, structuring, sending, using, accessing, and deleting. Processing of personal data is lawful if it falls into one or more of the following six categories: - The data subject gives explicit consent - The processing is necessary to perform a contract with the data subject (e.g., supply requested goods or services) - The controller is legally required to process the data - The processing is required to protect the vital interests of the data subject or another person - The processing is necessary to perform a task in the public interest (e.g., processing done by schools, hospitals, or the police) - Controller has a **legitimate interest** in processing the data There are additional requirements depending on the quantity and quality of processing.	**Art 4. §2**

Term	Definition	Article
Processor or Data Processor	Whoever holds or processes data on behalf of a controller, but is not responsible for making decisions regarding such data. For example, an organization, as controller, may outsource the processing of personal data to a third party for email marketing and engagement tracking, making the outsourced company the processor.	**Art. 4 §8 Art. 28 Subject to National Derogations**
Profiling	Automated processing of personal data used to classify, or make decisions or predictions about data subjects. This can include simple classifications based on age, sex, or numerical categories (e.g. credit score) regardless of if it is used for predictions. Under Article 22 exceptions, controllers may only use automated processing where: - The data subject has given their explicit consent - Necessary to enter into or perform a contract between the controller and the data subject - Authorized by Union or Member State law	**Art. 22**
Regular & Systematic Monitoring of Data Subjects	An organization that participates in regular and systematic monitoring of data subjects must designate a **DPO**. This includes when organizations track and **profile** data subjects in a recurring and organized method. Examples of regular and systematic monitoring include: **Profiling** and scoring for risk assessment Operating telecommunications networks Mobile app location tracking Behavioral advertising Fitness devices that track health data	**Art. 37 Subject to National Derogations**

Term	Definition	Article
Record of Data Processing Activities	Data controllers and data processors must maintain processing records. Controllers have more stringent requirements than processors. Controllers must keep records of the following information: T- he name and contact information for the controller, EU representative, and **DPO**. - The purpose of processing - The categories of data subjects - The categories of personal data - The categories of recipients the personal data is shared with - Any third countries personal data is transferred to - Any time limits for erasure per category of data - A description of data security measures Processors must keep records of the following information: - The name and contact information for the processor, the controller they are acting on behalf of, the EU representative, and the DPO. - The categories of processing - Any third countries the personal data is shared with - A description of data security measures Organizations with less than 250 employees are not required to keep such records unless: - The processing is likely to result in a risk to the rights and freedoms of data subjects - The processing is not occasional - The processing includes **special categories of data**	**Art. 30**

Term	Definition	Article
Right to Access	Data subjects have the right to know what data is processed about them. This information includes access to: - The purpose of processing - The categories of data collected - The third parties that data is shared with - The time period during which the data will be stored - The procedures that are available to rectify, request, or erase data - The right to lodge complaints with a **supervisory authority** - The sources that provided their data, if the data subject did not directly provide the data Information regarding potential profiling and the purpose	**Art. 15**
Right to Data Portability	One of the new rights of data subjects under the GDPR. Data subjects have the right to request, receive, and share any personal data collected on them in an accessible, readable format.	**Art. 20**

Term	Definition	Article
Right to Erasure	AKA “Right to be Forgotten”. One of the new rights of data subjects under the GDPR. Data subjects have the right to request that data collected about them be erased. Controllers must also take reasonable steps to make sure that third parties with whom they shared the data erase it as well. Data subjects may not exercise this right, and controllers are not required to erase such data, where processing is necessary to: - Exercise the right of freedom of expression and information - Comply with a controller’s legal obligation to Union or Member State law - Public interest in the area of public health - For research and archiving for public interest, scientific, or historical purposes - Establish or defend legal claims	**Art. 15**

Term	Definition	Article
Security of Processing	Controllers and processors should implement appropriate technical and organizational security measures around the personal data they process. These measures may include: - The pseudonymization and encryption of personal data - The ability to guarantee that processing systems will be confidential, available, and resilient - The ability to restore personal data in a timely manner in the event of an incident - A process to regularly test, assess, and evaluate the security measures **Pseudonymization:** A data security measure where processed data is separated and cannot be connected to an identifiable person without additional information. Pseudonymized data is still considered personal data, subject to GDPR, since there is a chance of it being linked to a data subject. **Encryption**: A data security measure where data is translated into code that may only be accessed with a key. Encryption is considered one of the most secure data protection methods.	**Art. 32 Subject to National Derogations**

Term	Definition	Article
Sensitive Personal Data	AKA “Special Categories of Personal Data” Sensitive personal data includes the following categories of data: - racial or ethnic origin - political opinions - religious or philosophical beliefs - trade union membership **- genetic data** **- biometric data** - data concerning health - data concerning a natural person’s sex life or sexual orientation Processing of sensitive data is not prohibited if it falls under one of the Article 9 exceptions, which include: - Data Subject gives explicit **consent** - Controller is legally required under employment / social security law - Necessary to protect “vital interests” of the data subject or another person where the data subject can’t consent - Legitimate activities of a non-profit political, philosophical, religious, or trade union organization processes - Data subject manifestly made the personal data public - Necessary to establish or defend legal claims or where a court is acting in judicial capacity Substantial public interest (based on Union or State law) - Necessary for health, medical, or social diagnosis, services, or treatment (based on Union or Member State law) - Necessary to archive research and statistics in the public interest	**Art. 9 Subject to National Derogations**

Term	Definition	Article
Standard Contractual Clauses	AKA “EU Model Clauses” Approved language incorporated into contracts involving international data transfers to provide adequate safeguards of the data and data subjects. It is one of three main methods for validly transferring EU personal data outside the European Economic Area, the others being **BCRs** and an **Adequacy finding** Standard Contractual Clauses are the most favored mechanism for validly transferring within a small business.	

This glossary does not constitute legal advice and does not establish an attorney-client relationship. You should always seek professional advice on the GDPR and other EU privacy laws from a lawyer admitted to practice in the EU and who is specialized in those areas.

FOLLOW US !

Law Office of S. Grynwajc

sglawnyc

@sglawNYC

Law Office of S Grynwajc

Law Office Of S.Grynwajc

CONTACT US

stephan.grynwajc

www.transatlantic-lawyer.com

stephan@transatlantic-lawyer.com

+1 (347) 543-3035