The General Data Protection Regulation and its effect on Transatlantic Businesses

I. Intro

As a Robert Bosch Foundation Fellow in Berlin, Germany I worked with various companies to better understand how the forthcoming European General Data Protection Regulations will affect their business operations. I spoke with leaders ranging from small startups to multinational organizations to understand their thoughts on data protection and privacy and to determine what, if anything, they were doing to prepare for GDPR compliance. What I found was an interesting but not wholly unexpected range of answers from "we will be fully GDPR compliant by May 25, 2018" to "what is the GDPR." As one would probably guess it was typically the larger, multinational organizations that fully understood the implications of the GDPR and were working tirelessly to become compliant before 2018. On the other side of the spectrum were the startups which were either oblivious to the forthcoming regulations or it merely wasn't on their radar as they had much more pressing issues, like obtaining enough funding to still be operating when the GDPR comes into force in May 2018. Interestingly on another side of the spectrum, the GDPR may provide ample opportunity for entrepreneurs to found companies to assist other companies in their path to GDPR compliance. This paper will explore the fundamentals of the GDPR as they are currently understood and how it will affect companies of various sizes,with a particular focus on those with transatlantic business operations.

II. What is the GDPR

In May of 2018, the most comprehensive and wide-reaching data privacy law since the dawn of the digital age will take effect. This law, the General Data Protection Regulation, will be the new standard bearer for data protection, setting a new worldwide bar for how companies, multinational organizations, and governments treat data privacy, security, and compliance.

The General Data Protection Regulation (GDPR) is at its very core a law about protecting the privacy rights of individuals, a unique and very European point of view. The GDPR establishes strict global privacy requirements on how companies manage and protect an individual's personal data, regardless of how or where data is sent, processed or stored. This raises the question of what is personal data? The GDPR defines personal data as "any information relating to an identified or identifiable natural person" or in terms that normal people understand it is "information about a living individual who could be

identified from that data, either on its own or when combined with other information."[1] This definition means that information as simple as email addresses or as complex as a marketing profile of a person can be considered personal information if they can be tied back to an individual.

III. Who is affected by the GDPR

The GDPR is universal and extraterritorial. It applies to all personal data about individuals collected or processed in Europe regardless of those individuals' nationality or citizenship. If you do business in Europe, GDPR affects you. The GDPR applies to the data you collect or process about Europeans even if your business is not based in Europe or even if it doesn't have a physical or incorporated presence there.[2] Furthermore, it is not only the companies who collect personal data that are subject to GDPR regulations but also companies that process personal data. The GDPR distinguishes between two types of companies that handle personal data: Data Controllers and Data Processors. Article 4(7) of the GDPR states that controllers are the companies that "alone or jointly with others, determines the purposes and means of the processing of personal data," whereas data processors only "process personal data on behalf of the controller." Therefore, even if a company does not collect personal data from natural persons if it processes that data on behalf of another company it is subject to the GDPR.

IV. Core Provisions of the GDPR

A. Personal Data Defined

The GDPR defines personal data as "any information relating to an identified or natural person," an intentionally broad definition that will include almost any data that a company has about its users, as long as that data can be tied, directly or indirectly, back to a specific person. The Regulation further expands the traditional definition of personal data by including genetic data, biometric data, location data and online identifiers. It is this inclusion of online identifiers that have the largest impact on tech companies and startups. According to one publication, this could include "any information created through interaction with a site app, wearable, or online service which could identify the individual – whether that is an analytics record, a check-in map, a health tracker, or the information exchanged through a social media login."[3] If EU regulators take such a broad view of the definition for online identifiers, it would not be hard to imagine the severe negative impact this could have on Europe's startup ecosystem. Although not a necessity to be considered a startup, the vast majority of startups are technology-based, whether

[1] Deeson. White Paper: *The only GDPR guide you'll enjoy reading*. Page 3. Retrieved at https://www.deeson.co.uk/blog/gdpr-guide-you-wont-hate
[2] Deeson. White Paper: *The only GDPR guide you'll enjoy reading*. Page 5
[3] Deeson. White Paper: *The only GDPR guide you'll enjoy reading*. Page 4

through an app or a website, and either must collect personal data of their users (for logins, etc.) or in some instances their entire business revolves around monetizing data.

Beyond personal data, the GDPR classifies some data as Sensitive Personal Data which requires even stricter security measures and has graver consequences for loss or breach. Currently, data relating to i) racial or ethnic origin, ii) political opinions, iii) religious or philosophical beliefs, iv) trade union membership, v) health data, vi) sex life or sexual orientation, and vii) past criminal conventions are all enumerated as sensitive personal data.

B. Data Processing

What does processing personal data mean? The GDPR is intentionally vague in its' definition of processing which it defines in Article 4(2) as "any operation or set of operations" performed on personal data. Routine business practices such as customer surveys, a recorded conversation with customer service representatives, or even collecting resumes from potential employees all may qualify as processing an individuals' personal data.

The GDPR sets out six guiding principles for processing personal data:

1) it must be processed lawfully, fairly and in a transparent manner. This essentially means that a company must be honest and communicate openly and effectively with individuals about their processing activities.
2) it must be collected for a specified, explicit, and legitimate purpose.
3) it must be relevant and necessary
4) it must be accurate and up-to-date
5) it should not be kept for longer than is necessary, and
6) it must be secure

C. Legal Basis

Under the GDPR there are six legitimate bases for processing an individual's personal data outlined in Article 6. At least one of these bases must be met for the processing of personal data to be legal

Consent

A company may process personal data of an individual if the individual has given consent for the processing. For a company to obtain and rely on consent it must meet the following requirements.

a. Freely given: consent must be clearly distinguishable, intelligible and in clear and plain language. It cannot be enabled by default and must be a positive, affirmative action by the individual, such as checking an opt-in box. Furthermore, individuals must also be able to withdraw consent as easily as they gave consent.
b. Specific: Individuals must be informed of all purposes for processing their personal data at the time they give consent and if another purpose arises the processing company may be required to obtain additional consent for this new purpose;
c. Unbundled: individuals cannot be forced to grant consent for one thing in order to receive another;
d. Informed: individuals should be informed of the processing company's identity, as well as, all third parties who will be receiving their personal data and why they will be receiving it. Furthermore, under Article 12(1) this information should be concise and communicated using understandable language in an easily accessible form with the burden on the processing company to show that an individual was informed prior to consenting. The requirement for information to be clear and concise is relative to the individual who is being informed, meaning that if a company is providing information to a child that information must be written in a way most understandable to children.
e. No imbalance: under the GDPR consent may not be used as a legal basis if there is a clear imbalance between the organization processing personal data and the individual. For example, consent may not be used by governmental authorities as a legal basis, this is because the fundamental imbalance of power between governments and their citizens.
f. Verifiable and documented: processing companies must be able to prove an individual gave their consent, how that consent was given, what information they were given, what they agreed to, when they consented, and whether or not the individual withdrew consent.

Performance of a Contract

A company may process personal data if it is necessary to the performance of a contract to which the individual is a party or if the individual requests the processing for the purpose of entering into a contract. This would be the basis that companies selling things to individuals would rely on as the legal basis for the processing of their personal data. For a company to process payment and provide a good or service to an individual it must process the personal data of that individual.

Compliance with a legitimate legal obligation

A company may process personal data in the course of complying with a legitimate legal obligation of the company. This is meant to be interpreted narrowly and only applies to legal

obligations required under European Union and member state laws. Thus, it would not apply to legal obligations of US-based companies.

Protection of vital interests of the individual

This legal basis is intended to be used in emergency situations to ensure an individuals' survival and should be relied on only if no other legal basis can be used.

Necessary for the public interest

A company may process personal data when it is in the public interest, i.e. for policing, tax collection or statistical purposes of the government.

Necessary for the legitimate interests of the company

Companies may think of this as their "safety net" and in the absence of another legal basis may rely on their "legitimate interests" to process personal data. Although this basis may be easier and more realistic than to gain consent from an individual it should be used with caution as it may be overridden by the "interests, rights or freedoms of the individual." When relying on their legitimate interests, the burden is on the company to show that an individual's fundamental rights and freedoms have not been compromised.

D. Individual Rights

The GDPR enumerates eight "rights" that individuals have regarding the personal data organizations collect about them. These are the i) right to be informed, ii) the right to access, iii) the right to rectification, iv) the right to erasure, v) the right to restrict processing, vi) the right to portability, vii) the right to object to processing, and viii) the right against profiling. Below I will review four of the most significant rights.

Right to Access

One of the most important rights of individuals under the GDPR is enshrined in Article 15, the right to access, individuals have the right to know what data a business collects about them. Through a Subject Access Request, an individual can request a copy of all information a company collects about them. The GDPR further stipulates the strict timelines within which companies must respond to these requests and does not permit companies to charge a fee for this information, except in certain circumstances where it may charge a reasonable administrative fee. However, this right is not absolute as there are some restrictions on an individual's right to access. For instance, an individual's right to access must be weighed against the need to protect other individuals' rights and freedoms. So, if the personal data of an individual reveals personal

data of another individual or contains other confidential information it may be exempt from disclosure under this right. This will make compliance with the GDPR very tricky for companies as they cannot merely release information they have on an individual to that individual but must instead weigh the rights and freedoms of how that information may affect other individuals.

In addition to the information actually collected about individuals, the GDPR allows individuals to request additional information about how their personal data is being processed. This includes confirmation that processing of an individual's data is taking place, where the data is located, the retention periods for that data, and if any third parties are receiving their personal data. Furthermore, companies processing personal data must let individuals know if they are using any automated profiling or decision making (AI) software and what these are being used for.

Right to Rectification

The GDPR states that an individual has the right to have a company that processes their personal data rectify any incorrect data without undue delay, usually within a month of the request unless there are extenuating circumstances. To have their data corrected in a company's system they may have to submit a supplementary statement which the company will review and decide whether or not to update their records. If a company decides not to correct their records they must promptly inform the individual about their decision and the reason therefore. If a company denies an individual's request for rectification, then that person may file a complaint with the supervisory authority in their member state.

Right to Erasure

The right to erasure, also known as the "right to be forgotten" is outlined in Article 17 of the GDPR and is one of the most controversial parts of the GDPR. This right allows, under certain circumstances, for individuals to request that a data processor delete their personal data and stop processing it. However, even if an individual shows that there is a legitimate reason for their data to be deleted an organization may retain and continue processing their data if they have another legal basis for processing that data. Erasure may be requested by an individual if one of the following are met:

1. If the personal data is obsolete or no longer necessary for the reason it was collected;
2. If the processing is based on consent and that consent is withdrawn;
3. If the processing was based on a company's "legitimate interests" and the company cannot prove that their legitimate interest overrides the individual's rights and freedoms;
4. If the processing is illegal;

5. If the data must be erased under EU law; or
6. If consent was given by a Child it may be withdrawn at any point, even after the child is of legal age.

Right to Portability

The right to portability is an interesting right that to some extent already existed before the GDPR but will now apply to all personal data collected about an individual. According to the Article 29 Working Party this "right allows the data subject to obtain and reuse "their" data for their own purposes and across different services." This will empower consumers and prevent companies from keeping individuals' data in proprietary systems, holding it ransom to hinder a person from moving to another service. If a person requests a copy of their data, an organization must provide it in a structured, machine-readable, open file format and it must be provided free of charge. This right to data portability applies when three conditions are met. First, the personal data must have been collected and processed under the legal basis of consent or under the performance of a contract, as explained above. Second, the personal data must have been provided by the individual and not derived from other sources. Third, providing the individual their personal data must not negatively affect the rights and freedoms of others.

E. Privacy Notices

Privacy information notices replace the privacy policies that already exist on your websites and apps. They also replace the days of privacy statements being drafted by lawyers, for lawyers. The language must be simple and plain in a way that anyone can understand.[4] A privacy notice should describe to individuals how the company collects, uses, retains and discloses their personal data.

F. Data Breaches

At a talk once I heard a presenter say, "there are two types of companies, ones that have been breached and ones that do not know they have been breached." This sentence brings into view a new reality in the digital age, we as consumers have entrusted companies, non-profits, governments and other organizations with vast amounts of our personal data and when these organizations lose this data we are all at risk. Because the risk of a data breach is so high and the consequences severe, the GDPR has very strict requirements for how companies must handle data breaches. Article 4(12) of the GDPR broadly 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

[4] Deeson. White Paper: *The only GDPR guide you'll enjoy reading*. Page 9

processed" and according to Article 33, if a breach "is likely to result in a risk to the rights and freedoms of individuals" then an organization must report it to their national data protection authority within 72 hours of when they know, or should have known, about it. Furthermore, if an organization has a "high-risk breach," one affecting vast numbers of individuals or one that includes sensitive personal data, they must not only report the breach to their data protection authority they must also immediately notify the affected individuals.

Consequences of non-compliance

Article 58 of the GDPR provides the supervisory authority with the power to impose administrative fines under Article 83 based on a variety of factors, including:

- The nature, gravity, and duration of the infringement (e.g., how many people were affected and how much damage was suffered by them)
- Whether the infringement was intentional or negligent
- Whether the controller or processor took any steps to mitigate the damage
- Technical and organizational measures that had been implemented by the controller or processor
- Prior infringements by the controller or processor
- The degree of cooperation with the regulator
- The types of personal data involved
- The way the regulator found out about the infringement[5]

Based on the infringement and taking into account the factors above the regulation has a two tiered system for imposing fines on companies in violation of the GDPR. Article 83(4) allows for fines "up to €10M, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher," "[i]f it is determined that non-compliance was related to technical measures such as impact assessments, breach notifications and certifications, then the fine may be up to an amount that is the GREATER of €10 million or 2% of global annual turnover (revenue) from the prior year".6 While Article 83(5) allows for fines "up to €20M, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher," "[i]n the case of non-compliance with key provisions of the GDPR, regulators have the authority to levy a fine in an amount that is up to the GREATER of €20 million or 4% of global annual turnover in the prior year. Examples that fall into this category are non-adherence to the core principles of processing personal data,

[5] O'Neill, Cheryl. (2017 March 17). *GDPR Series, Part 4: The Penalties for Non-Compliance*. Retrieved from https://www.imperva.com/blog/2017/03/gdpr-series-part-4-penalties-non-compliance/
[6] O'Neill, Cheryl. (2017 March 17). *GDPR Series, Part 4: The Penalties for Non-Compliance*.

infringement of the rights of data subjects and the transfer of personal data to third countries or international organizations that do not ensure an adequate level of data protection".

However, according to one publication "When fines are imposed – and they rarely are – they must be "effective, proportionate and dissuasive" to the matter. Fines only tend to be imposed when the company in question refuses to cooperate, repeats their mistake, or commits a privacy violation so offensive that a fine is the only option possible."[7]

G. Data Protection

The GDPR requires companies to have data protection regimes and programs in place. According to section 24(1) "taking into account the nature, scope context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary". This lays out a foundation for a risk-based analysis to data protection while also requiring that companies continuously review and update their policies and technical capabilities.

Article 25 lays out the two fundamental building blocks of privacy under the GDPR, Privacy by Design and Privacy by Default which are discussed further below.

Privacy by Design

Data Protection by design "is about anticipating, managing and preventing privacy issues before a single line of code is written"[8] it starts prior to a company processing a single byte of data by incorporating privacy and data protection ideas into the initial planning of software or a business plan. "The best way to mitigate privacy risks, according to the Privacy by Design philosophy, is not to create them in the first place."[9] According to Dr. Ann Cavoukian, the Privacy Commissioner of Ontario, Canada from 1997-2014 who created the Privacy by Design framework

> "*The Privacy by Design framework prevents privacy-invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred; it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after."*

This Framework laid out seven foundational principles of Privacy by Design:

---

[7] Deeson. White Paper: *The only GDPR guide you'll enjoy reading*. Page 20
[8] Burns, Heather. (2017, July 27). *How To Protect Your Users With The Privacy By Design Framework*. Retrieved from www.smashingmagazin.com/2017/07/privacy-by-design-framework/
[9] Burns, Heather. (2017, July 27). *How To Protect Your Users With The Privacy By Design Framework*.

1. **Proactive** not **Reactive**; **Preventative** not **Remedial**, it should anticipate privacy issues before they reach the user.
2. Privacy as the **Default**. The user should not have to take actions to secure their privacy, and consent for data sharing should not be assumed.
3. Privacy **Embedded** into Design, It should be a core function of the product or service, not an add-on.
4. **Full** functionality. Positive-Sum not Zero-Sum.
5. **End-to-end Security** - Lifecycle Protection of user data. Engaging in proper data minimization, retention, and deletion processes.
6. **Visibility** and **Transparency**. Privacy standards should be visible, transparent, open, documented and independently verifiable.
7. **Respect** for User Privacy. Privacy should be user-centric. This means giving users granular privacy options, maximized privacy defaults, detailed privacy information notices, user-friendly options and clear notification of changes.[10]

The GDPR mentions data minimization (Article 5(1)c and pseudonymisation (Article 6(4)e as necessary tools for protecting individuals privacy specifically in the design phase. In fact, it is impossible to be GDPR-compliant without implementing data minimization rules and processes at every step in the data lifecycle. This means that companies must limit personal data collection, storage, and usage of data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed.[11] Organizations will need to carefully review their data processing operations to consider whether they process any personal data that are not strictly necessary in relation to the relevant purposes.[12]

Privacy by Default

"Privacy by default requires that controllers implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed."[13] In practice, this means that when a product or service gives users multiple options for their privacy settings, the most restrictive should be set as the default. "The bottom line is that,

---

[10] Dr. Cavoukian, Ann Ph.D. *Privacy by Design: The 7 Foundational Principles.* Retrieved at https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[11] https://www.dataguise.com/gdpr-compliance-data-minimization-use-purpose/

[12] Dr. Gabel, Detlev. (2016, July 22) *Chapter 6. Data Protection Principles – Unlocking the EU General Data Protection Regulation.* Retrieved at https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection

[13] Mahmood, Sabba. (2016, January 5) *Getting to know the General Data Protection Regulation, Part 6 – Designing for Compliance*. Retrieved at http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/

by default, businesses should only process personal data to the extent necessary for their intended purposes and should not store it for longer than is necessary for these purposes."[14]

V. How the GDPR will affect companies

a. European Companies

The GDPR will severely affect how European based companies collect, process, and retain the personal data of not only European Citizens but of all individuals. However, the GDPR will greatly reduce uncertainty in transferring personal data between EU Member Countries and will ensure the free flow of information between member states.

b. Multinational Companies

Under the GDPR personal data cannot be transferred outside the European Union to third-party countries unless those countries can guarantee that they have materially equal and adequate data protection regulations. As the GDPR is a cutting-edge data privacy regulation, in practice very few countries will be able to pass this bar. Furthermore, these cross-border restrictions also apply to "onward transfers", from one third-country to another outside of the EU.

The GDPR lays out three avenues by which companies can safely transfer data outside of EU Member States. First, Adequacy Decisions are determinations by the European Commission that a third-party country's laws achieve the same level of protection as the GDPR. This is the best avenue for a company to transfer data outside of the EU, but because it requires governmental action it may not, and currently is not, available to the majority of companies. The Second avenue for a company to transfer data outside the EU are "appropriate safeguards" which are legal tools designed to ensure that companies who receive personal data outside of the EU are bound to protect that data to European-like standards. This mechanism comes in the form of binding corporate rules, standard contractual clauses (Model Clauses), ad hoc contractual clauses or reliance on international agreements. Lastly, and by far the riskiest avenue a company may use to transfer data outside of the EU are "derogations" or exemptions, which should only be used as a last resort.

For an organization in the United States doing business in Europe or European organizations sending their data to the US for processing the US Privacy Shield regime has been determined by the European Commission to meet the standards required by the GDPR. The US Privacy Shield is a self-certification scheme that has organizations commit to EU data protection standards. "To Join Privacy Shield, an

[14] Mahmood, Sabba. (2016, January 5) *Getting to know the General Data Protection Regulation, Part 6 – Designing for Compliance*.

eligible company must self-certify to the U.S. Department of Commerce that it complies with a set of principles and related requirements that have been deemed by the European Commission as providing adequate privacy protection [and] Companies are required to re-certify every year to retain their status as current members[.]"[15] Additionally, [f]alse claims of participation in Privacy Shield are subject to enforcement actions by the FTC as deceptive acts or practices under Section 5 of the FTC Act."[16]

VI. Conclusion

The GDPR will come into effect on May 25th, 2018 at which time all European Companies and international companies doing business in Europe must be compliant with the regulations laid out in this paper. With new obligations on such matters as data subject consent, data anonymization, breach notification, trans-border data transfers, and appointment of data protection officers, to name a few, the GDPR requires companies handling EU citizens' data to undertake major operational reform.[17] The GDPR is about knowing what you have, knowing what you are doing with it, knowing where it is stored, knowing who has access to it, and knowing how you are safeguarding it.[18] Through my conversations with large multinational companies like Microsoft and Google I came to understand that these companies are taking the GDPR very seriously and are investing millions in strategies to not only comply with the regulation but to provide solutions for other companies to be in compliance as well. It is however the smaller companies and in particular startups that, through my observations, are not ready for the GDPR and who may be adversely affected by it the most.

Overall, data protection is a positive opportunity, a cultural shift, and a mechanism to do right by your users and customers. It is not a weapon or a threat, or a thing to fear. Compliance must start from a position of positive trust, not resentment.[19]

---

[15] Luib, Gregory. (2017 September) *Federal Trade Commission Reaffirms Commitment to Enforce EU-US Privacy Shield*. Retrieved from https://info.dechert.com/10/9279/september-2017/federal-trade-commission-reaffirms-commitment-to-enforce-eu-us-privacy-shield(2).asp#

[16] Luib, Gregory. (2017 September) *Federal Trade Commission Reaffirms Commitment to Enforce EU-US Privacy Shield*.

[17] Myers, Anna (2016, January 19) *Top 10 Operational Impacts of the GDPR: Part 4 – Cross-border data Transfers*. Retrieved at https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/

[18] Deeson. White Paper: *The only GDPR guide you'll enjoy reading*. Page 8

[19] Deeson. White Paper: *The only GDPR guide you'll enjoy reading*. Page 20