GDPR - 10 THINGS YOU NEED TO KNOW (US PERSPECTIVE)

1. Privacy and data protection are fundamental rights

Privacy is internationally recognised as a fundamental human right, like the right to free speech and freedom of assembly, including in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (which has been ratified by the US). The right to privacy includes the ability of individuals to determine who holds information about them and how the information is used.

In the European Union, the right to privacy and the right to protection of your personal data are further enshrined as fundamental human rights in the Charter of Fundamental Rights of the EU. This means that the situations when these rights can be interfered with are very limited. An analogous example from the United States would be the Fourth Amendment right to be free from unreasonable search and seizure. The EU Charter has a status similar to that of the U.S. Bill of Rights, in that every EU law must adhere to its requirements.

Data protection rights and obligations were originally enshrined in the EU in the 1995 Data Protection Directive, which was then implemented in Member States through national legislation (e.g. in the UK, the Data Protection Act 1998). The General Data Protection Regulation (GDPR), which comes into effect on 25 May 2018, reforms and replaces data protection law across Europe. GDPR will apply directly in all Member States of the EU and be complemented by national legislation.[1]

GDPR strengthens the rights of individuals with regard to the protection of their data, imposes more stringent obligations on those processing personal data and provides for stronger regulatory enforcement powers. A key change is the introduction of fines of up to €20 million or up to 4% of global annual turnover, whichever is greater. This is a huge increase from previous fines (for example in the UK, the maximum possible fine under current law was £500,000).

[1] The nature of EU legislation itself is somewhat complex. The EU and its member states have a relationship somewhat analogous to that of the U.S. federal government and the U.S. state governments, in that the EU can pass some legislation that requires the EU member states to do certain things. The EU has the ability to pass two different types of legislation - regulations and directives. A regulation is automatically law in all of the member states, meaning that they must follow it exactly as written. A directive requires each member state to include certain requirements in its own national laws -- for instance, to safeguard personal data - but the directive itself is not enforceable in each nation. Each nation's translation of the directive into its national law is called "implementation". Even though GDPR is a regulation, and therefore its provisions will apply directly, it permits member states discretion on certain areas at a national level, which is why further national legislation is needed.

2. GDPR can apply to U.S. companies

GDPR is extraterritorial in its scope, which means that there are circumstances in which GDPR can apply to companies around the world, including the U.S. GDPR applies to all those offering goods and services to individuals in the EU (irrespective of whether the individuals have to pay) and/or monitoring the behaviour of individuals in the EU (this includes online tracking).

Companies that are operating both in and outside of the EU will have to adapt their practices, at least for all data processing that falls under the GDPR. This raises the question as to whether companies are going to raise standards across the bar or implement a dual standard, where for example, U.S. consumers are less protected. Many companies have yet to make their position clear.

Currently, many U.S. companies self-certify their compliance with specified data protection standards under the EU-U.S. "Privacy Shield", which is a framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States.

GDPR is an addition to and trumps obligations under the Privacy Shield.

3. GDPR recognises that individuals have the right to control their data

GDPR is about giving individuals more control over their personal data but this does not equate to personal data as a commodity to be bought and sold or that individuals should have to pay to protect.

Data protection is a fundamental right; it should improve trust and reduce power imbalances. Data subjects have rights over their personal data, regardless of who holds or processes it. GDPR gives individuals control over their data by limiting the way it can be used by others and giving individuals rights, such as the right to know how their data is being used, to access it, to rectify it, delete it and port it. Control means an individual having rights over their data, but this doesn't mean the onus is only on the individual. Rather, as is made clear through the GDPR: there is a role for the legislator in providing strong rights in law; there is a role for industry in designing systems that by default protect our data, to fulfil their obligations and permit individuals to realise their rights; and there is a role for regulators to provide guidance about these rights and to take action when they are violated.

4. GDPR provides comprehensive not sectoral data protection

GDPR is comprehensive data protection legislation in that it will apply to all those processing personal data (with some limited exceptions e.g. there is another piece of legislation for law enforcement). In the EU, this is complemented by additional sectoral legislation, such as rules on privacy in electronic communications. This is in stark contrast to the U.S. where there is no overarching data protection framework, but instead a patchwork of legislation at both the national and state level (e.g. the Privacy Act of 1974, COPPA, HIPAA and state breach reporting).

5. You need a legal basis if you want to process personal data

The GDPR does not prevent the processing of personal data fullstop. Rather, it sets out rules and conditions that must be followed when personal data is processed. As a quick reminder, processing under the GDPR means basically doing anything with data, including collecting, storing, using, altering, generating, disclosing and destroying. If you are doing any of these and more with personal data, one condition of the GDPR is that you have a legal basis to do it.

The GDPR provides for six such legal bases, one of which is consent. If you are going to rely on consent, it must be freely given, specific, informed and unambiguous (no pre-ticked boxes). Individuals must also be able to withdraw consent at any time.

There are other conditions, too, all of which require you to think about the necessity of what you're doing, i.e., could you achieve the same thing in a way that interferes less with the individual's rights? The two most relevant legal bases in a commercial context are likely to be where the processing is necessary for the performance of contract and where the processing is necessary for the purposes of the legitimate interests of the party in control of the data (or even a third party).
An example of where processing is necessary for the performance of a contract is when an individual buys a product online, a company will need to process their address in order to deliver it to them. Processing on the basis of legitimate interest is harder to explain and often less clear, but to rely on it a company must explain how they are going to use your data, specify what their legitimate interest is in using the data in that way and ensure that doing so doesn't cause any prejudice to the fundamental rights of the individual.

If you are dealing with data that reveals sensitive personal information (such as that revealing ethnicity, political opinions, religion, biometrics, health, sex life), then there are even stricter conditions. If you are relying on consent, this consent must be explicit, and you cannot rely on the legitimate interest condition.

6. GDPR requires transparency and accountability.

Most legal instruments covering data protection, both national and international, are based on some key principles. This is the same with GDPR which builds on the principles under the previous EU framework. These principles include that personal data must be processed lawfully and fairly; for specific, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary; accurate; retained only as long as necessary; and kept secure.

Some key additions to these principles in GDPR are the requirements of transparency and accountability. If you are processing personal data, you must do this in a way that is transparent to the individual whose data is being processed.
This means clear, concise and accessible privacy notices.

In terms of accountability, you must be responsible for and be able to demonstrate compliance with all the data protection principles. GDPR places a number of related obligations, including carrying out data protection impact assessments, appointing data protection officers, keeping records of processing operations and having contractual agreements in place when you share data. GDPR also introduces mandatory data breach reporting to the regulator within 72 hours and in high risk cases to individuals.

7. Privacy by design and by default

GDPR requires companies processing personal data to design their systems in a way that minimises the processing of data to what is necessary for a specific purpose and to protect by default personal data from being used for other purposes. The onus is on companies to protect personal data and data protection and privacy must be considered from the very outset. This should encourage innovation and is something that start-ups should consider from the outset, particularly given that privacy protections and the trust they build can be appealing to new users.

8. The definition of personal data is wide under GDPR

It's not a case of tomato, tomato. Even pre-GDPR, the definition of personal data in Europe was originally wider than the scope of Personally Identifiable Information (PII) in the U.S. However, under GDPR, this definition is further strengthened and explicitly includes information from which an individual can be identified both directly or indirectly by reference to an identifier (a piece of information/ data that distinguishes you). This includes location data, online identifiers (such as certain cookies and IP addresses) or other factors specific to a person's physical, physiological, genetic, mental, economic, cultural or social identity. In recent years, the scope of PII has expanded, as recognised by the FTC, to cover data which can be reasonably linked to a particular person, computer or device. In spite of this, the understanding of PII and its scope does not necessarily match that of personal data under GDPR and the two should not be used interchangeably.

9. Under GDPR individuals have rights

A key aspect of GDPR is strengthening individuals' rights in relation to their data:

a. Information

Individuals must be provided information about who is using the data and for what purpose. The information must be concise, transparent, easily accessible, in clear and plain language, be comprehensive, and be given at the time the data is requested or obtained

b. To Access

Individuals have the right to access their personal data on request (within 1 month) free of charge, no matter whether it is collected directly from them or obtained from a third party.

c. Rectify

Individuals have the right to have personal data corrected if it is inaccurate or incomplete; they must be informed about third parties to whom the data has been disclosed; and third parties must be informed of the correction where possible.

d. Erasure

Individuals have the right to request that personal data be deleted or removed where there is no compelling reason for its continued processing. This right is subject to a number of tests and exceptions, importantly the freedom of expression.

e. Restrict

Individuals have the right to 'block' or suppress processing of personal data in particular circumstances. Personal data can then be stored but not further processed until the issue is resolved.

f. Portability

Individuals have the right to obtain and reuse the personal data they've provided for their own purposes across different services. They can move, copy or transfer their personal data from one provider to another in a "commonly used and machine-readable format."

g. Object

Individuals have the right to object to processing, including profiling. This means that such processing must be stopped unless compelling grounds override the interests of the individual. There is an absolute right to object to processing for direct marketing purposes.

h. Automated decision-making

Individuals have the right not to be subject to decisions based on automated processing without any human intervention, if such a decision significantly affects them.

10. GDPR defines and limits profiling

Profiling, using people's data to evaluate certain personal aspects about them, and analyse or predict aspects relating to them, as a defined concept is new in GDPR. Under GDPR, if companies are carrying out profiling activities, they must be clear about how they are using personal data and have a valid legal basis for these activities. As noted above, the restrictions on processing people's sensitive personal data, including people's political and religious beliefs, ethnicity or sexual orientation and health, are especially stringent. This means that there are limits on how people can be profiled, especially when profiling reveals sensitive data and individuals can object to these practices. This means that it is not business as usual for those conducting data driven targeted marketing and the compliance of these practices need to be examined thoroughly.