Research Brief on the General Data Protection Regulation Framework

- By Rohan Bhasin

Contents

Introduction

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to:

- Harmonize data privacy laws across Europe,
- Protect and empower all EU citizens data privacy
- Reshape the way organizations across the region approach data privacy.

GDPR reshapes the way in which sectors manage data, as well as redefines the roles for key leaders in businesses, from CIOs to CMOs. CIOs must ensure that they have watertight consent management processes in place, whilst CMOs require effective data rights management systems to ensure they don't lose their most valuable asset – data.**The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.** The regulation will fundamentally

reshape the way in which data is handled across every sector, from healthcare to banking and beyond.

Subject Matter and Objectives :-

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Timeline

1. 25 January 2012: The proposal for the GDPR was released.
2. 21 October 2013: The European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) had its orientation vote.
3. 15 December 2015: Negotiations between the European Parliament, Council and Commission (Formal Trilogue meeting) resulted in a joint proposal.
4. 17 December 2015: The European Parliament LIBE Committee voted for the negotiations between the three parties.
5. 8 April 2016: Adoption by the Council of the European Union. The only member state voting against was Austria, which argued that the level of data protection in some respects falls short compared to the 1995 directive.
6. 14 April 2016: Adoption by the European Parliament.
7. 24 May 2016: The regulation entered into force, 20 days after its publication in the *Official Journal of the European Union*.
8. 25 May 2018: Its provisions became directly applicable in all member states, two years after the regulations enter into force.

9. 20 July 2018: the GDPR became valid in the EEA countries (Iceland, Liechtenstein, and Norway) after the EEA Joint Committee and the three countries agreed to follow the regulation.

Brief History

The EU's data protection laws have long been regarded as a gold standard all over the world. Over the last 25 years, technology has transformed our lives in ways nobody could have imagined so a review of the rules was needed.

In 2016, the EU adopted the General Data Protection Regulation (GDPR), one of its greatest achievements in recent years. It replaces the 1995 Data Protection Directive which was adopted at a time when the internet was in its infancy.

The GDPR is now recognised as law across the EU. Member States have two years to ensure that it is fully implementable in their countries by May 2018.

General Impact

GDPR affects every company, but the hardest hit will be those that hold and process large amounts of consumer data: technology firms, marketers, and the data brokers who connect them.

Even complying with the basic requirements for data access and deletion presents a large burden for some companies, which may not previously have had tools for collating all the data they hold on an individual.

But the largest impact will be on firms whose business models rely on acquiring and exploiting consumer data at scale. If companies rely on consent to process data, that consent now has to be explicit and informed – and renewed if the use changes.

The layman has the power to hold companies to account as never before. If individuals begin to take advantage of GDPR in large numbers, by withholding consent for certain uses of data, requesting access to their personal information from data brokers, or deleting their information from sites altogether, it could have a seismic effect on the data industry.

Even without user pressure, the new powers given to information commissioners across the EU should result in data processors being more cautious about using old data for radically new purposes.

Counterintuitively, though, it could also serve to entrench the dominant players. A new startup may find it hard to persuade users to consent to wide-ranging data harvesting, but if a company such as Facebook offers a take-it-or-leave-it deal, it could rapidly gain consent from millions of users.

Footprint on Banks

This new data protection regulation puts the consumer in the driver's seat, and the task of complying with this regulation falls upon businesses and organizations. Otherwise, you're failing to comply.

What falls under GDPR compliance?

Well, GDPR applies to all businesses and organizations established in the EU, regardless of whether the data processing takes place in the EU or not. Even non-EU established organizations will be subject to GDPR. If your business offers goods and/or services to citizens in the EU, then it's subject to GDPR.

All organizations and companies that work with personal data should appoint a data protection officer or data controller who is in charge of GDPR compliance.

There are tough penalties for those companies and organizations who don't comply with GDPR fines of up to **4% of annual global revenue** or **20 million Euros**, whichever is greater.

Many people might think that the GDPR is just an IT issue, but that is the furthest from the truth. It has broad-sweeping implications for the whole company, including the way companies handle marketing and sales activities.

Compliance for Corporations

Preparations for GDPR-compliance

A key component of the GDPR legislation is privacy by design.

Privacy by design requires that all departments in a company look closely at their data and how they handle it. There are many things a company has to do in order to be compliant with GDPR. If you have yet to to take the next step towards compliance, here are just a few ways to help you get started.

1. Map your company's data

Map where all of the personal data in your entire business comes from and document what you do with the data. Identify where the data resides, who can access it and if there are any risks to the data. This is not only important for GDPR, but will help improve Customer Relationship Management.

2. Determine what data you need to keep

Don't keep more information than necessary and remove any data that you aren't using. If your business has collected a lot of data without any real benefit, now is the time to consider which data is important to your business. GDPR encourages a more disciplined treatment of personal data.

In the clean-up process, ask yourself:

- Why exactly are we archiving this data instead of just erasing it?
- Why are we saving all this data?
- What are we trying to achieve by collecting all these categories of personal information?
- Is the financial gain of deleting this information greater than encrypting it?

3. Put security measures in place

Develop and implement safeguards throughout your infrastructure to help contain any data breaches. This means putting security measures in place to guard against data breaches, and taking quick action to notify individuals and authorities in the event a breach does occur.

Worryingly, law firm EMW found that data breach complaints have increased by 160% since the GDPR came into effect.

Make sure to check with your suppliers also. Outsourcing doesn't exempt you from being liable and you need to make sure that they have the right security measures in place. For example, the recent data breach for companies using third party survey provider, Typeform.

4. Review your documentation

Under GDPR, individuals have to explicitly consent to the acquisition and processing of their data. Pre-checked boxes and implied consent will not be acceptable anymore. You will have to review all of your privacy statements and disclosures and adjust them where needed.

5. Establish procedures for handling personal data

As we mentioned earlier, individuals have 8 basic rights under GDPR.

You now need to establish policies and procedures for how you will handle each of these situations.

Example:

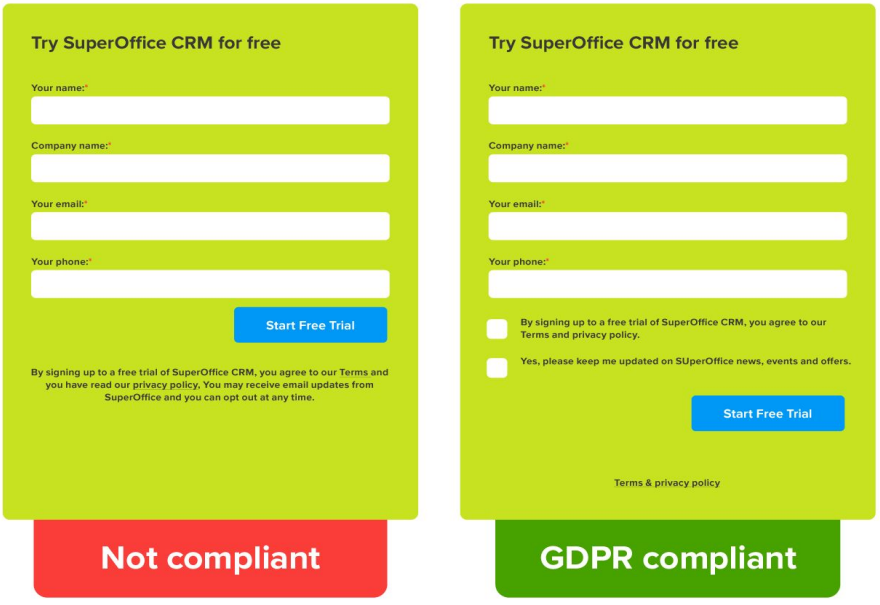
1. How can individuals give consent in a legal manner?
2. What is the process if an individual wants his data to be deleted?
3. How will you ensure that it is done across all platforms and that it really is deleted?
4. If an individual wants his data to be transferred, how will you do it?
5. How will you confirm that the person who requested to have his data transferred is the person he says he is?
6. What is the communication plan in case of a data breach?

Customer Engagement

The conditions for obtaining consent are stricter under GDPR requirements as the individual must have the right to withdraw consent at any time and there is a presumption that consent will not be valid unless separate consents are obtained for different processing activities.

This means you have to be able to prove that the individual agreed to a certain action, to receive a newsletter for instance. It is not allowed to assume or add a disclaimer, and providing an opt-out option is not enough.

GDPR has changed a lot of things for companies such as the way your sales teams prospector the way that marketing activities are managed. Companies have had to review business processes, applications and forms to be compliant with double opt-in rules and email marketing best practices. In order to sign up for communication, prospects will have to fill out a form or tick a box and then confirm it was their actions in a further email.



Organizations must prove that consent was given in a case where an individual objects to receiving the communication. This means that any data held, must have an audit trail that is time stamped and reporting information that details what the contact opted into and how.

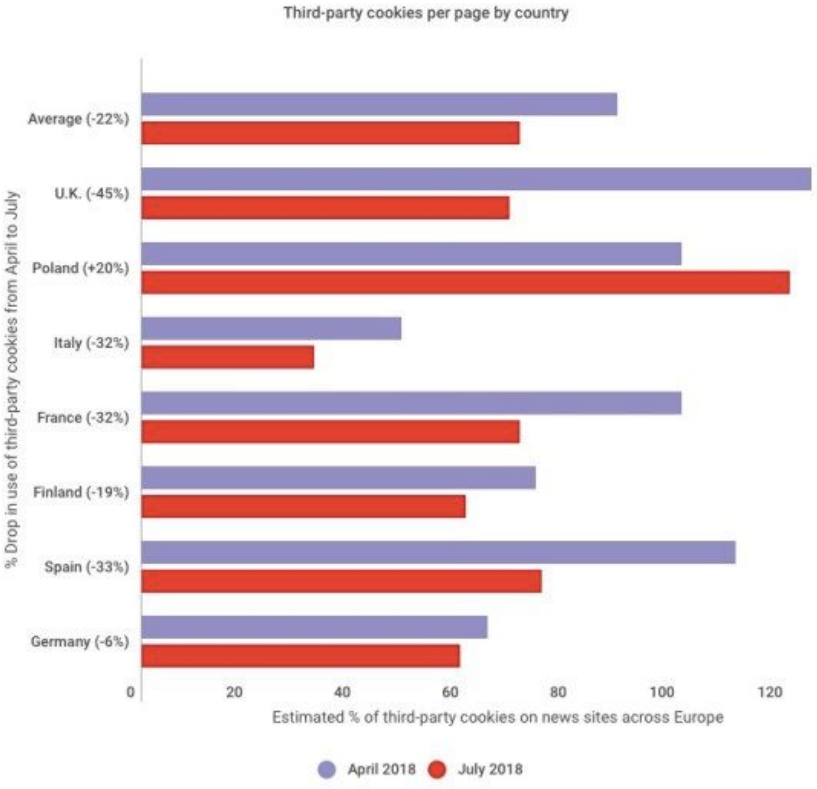
If you purchase marketing lists, you are still responsible for getting the proper consent information, even if a vendor or outsourced partner was responsible for gathering the data.

In the B2B world, sales people meet potential customers at a trade show, they exchange business cards, and when they come back to the office, they add the contacts to the company's mailing list. In 2018, this is not possible anymore.

Companies will have to look at new ways of collecting customer information.

Plummeting for Third Party Cookies

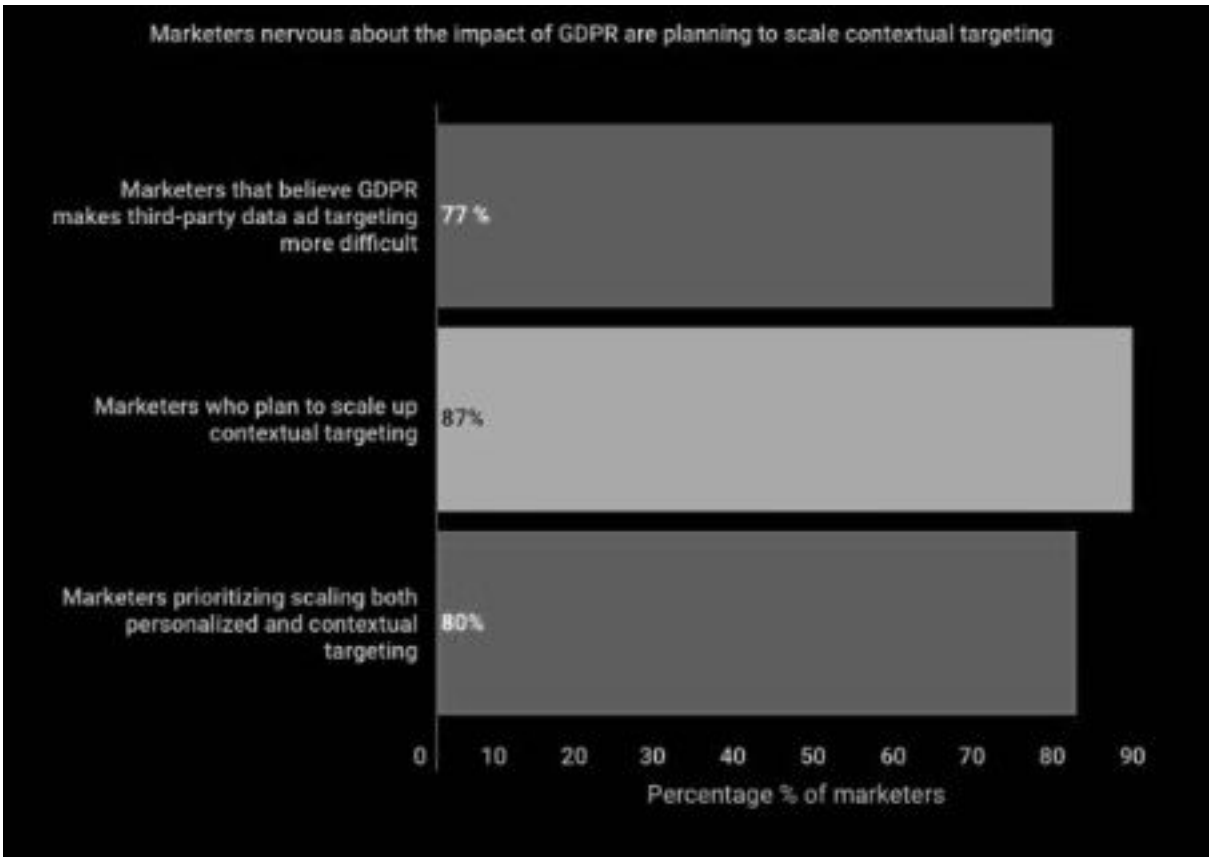
The average use of third-party cookies per page across Europe has dropped 22 percent, according to a report from Reuters Institute for the Study of Journalism. The report examined third-party cookie use between April and July — before and after the May 25 GDPR enforcement date — across seven countries: the U.K., Germany, France, Italy, Spain, Finland and Poland. U.K. news publishers had the highest proportion of third-party cookies per page prior to GDPR, and so have seen the biggest drop, of 45 percent, while Germany showed the smallest change with just a 6 percent drop, according to the report.



GDPR requirements for consent mean some news organizations may be deferring some tracking cookies until after a user clicks to accept to the site's terms for using their data — a factor the report's authors attributed to the drop in average third-party cookies per page. Sites also may have undergone a GDPR-inspired clean-up, ridding their sites of out-of-date features and code, which could also have contributed to the drop-offs.

Resurgence for contextual targeting

Just under 80 percent of 500 decision-making brand marketers across Europe and the U.S. believe GDPR will make targeting audiences using third-party data more difficult, according to research from ad tech firm Sizmek. But contextual targeting can help fill the gap, for now at least. In fact, 87 percent of marketers said they plan to increase contextual targeting in the next 12 months, while maintaining personalized advertising where possible, according to the same report.



Distinguished features from the former

An overview of the main changes under GDPR and how they differ from the previous directive. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Increased Territorial Scope (extraterritorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GDPR makes its applicability very clear – it applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.

Penalties
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g.not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors – meaning 'clouds' are not exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened, and companies are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data Subject Rights

Breach Notification

Under the GDPR, breach notifications are now mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces data portability – the right for a data subject to receive the personal data concerning them – which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically, 'The controller shall… implement appropriate technical and organisational measures… in an effective way… in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Under GDPR it is not necessary to submit notifications / registrations to each local DPA of data processing activities, nor is it a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there are internal record keeping requirements, as further explained below, and DPO appointment is mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the Data Protection Officer:

A. Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
B. May be a staff member or an external service provider
C. Contact details must be provided to the relevant DPA
D. Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
E. Must report directly to the highest level of management

F. Must not carry out any other tasks that could results in a conflict of interest.

Enabled Opportunities

GDPR answers the need for updated legislation in the face of rapidly evolving technology, higher rates of security breaches, and unequal playing rules between countries. Perhaps most importantly, the GDPR aims to give consumers back control over their personal data. They will have the right to access the personal data they have given to a company, as well as the right to delete it, and/or transfer it to new companies who can create value from it. In an economy shifting towards platform business models, the free movement of data becomes a prerequisite for growth. Yet for this growth to be realised, there must be individual control over personal data, clear consent, and trust.

Personal data is often referred to as 'the new oil'. It is data-intensive sectors that are driving growth in the economy, and many of the most valuable companies in the world work exclusively with handling data. At the same time, there is concern that the GDPR will inhibit business growth where personal data is concerned. Strict security and clear rules are nevertheless necessary if personal data is to reach its full potential as an asset class.

After May 2018 your business will fall into one of two groups. You will either be GDPR compliant, which will enable you to continue to use your customer data to market your products and services. Or you will be in a group that finds itself unable to use its data for fear of getting hit with some very large fines by the Information Commission Office.

These new regulations come into force in May 2018. It means better safeguards for us all as individuals. All organisations need to take some steps to make sure that they remain on the right side of the law.

1. It provides an opportunity to get your data in order – and better data means better return on marketing spend.

2. Staying on the right side of the law avoids the risk of damaging your brand.

3. You avoid the massive fines that are going to be imposed on those organisations that do not comply.

Aligned Nations with Brexit Input

GDPR covers all of the European Union Member States, which includes:-

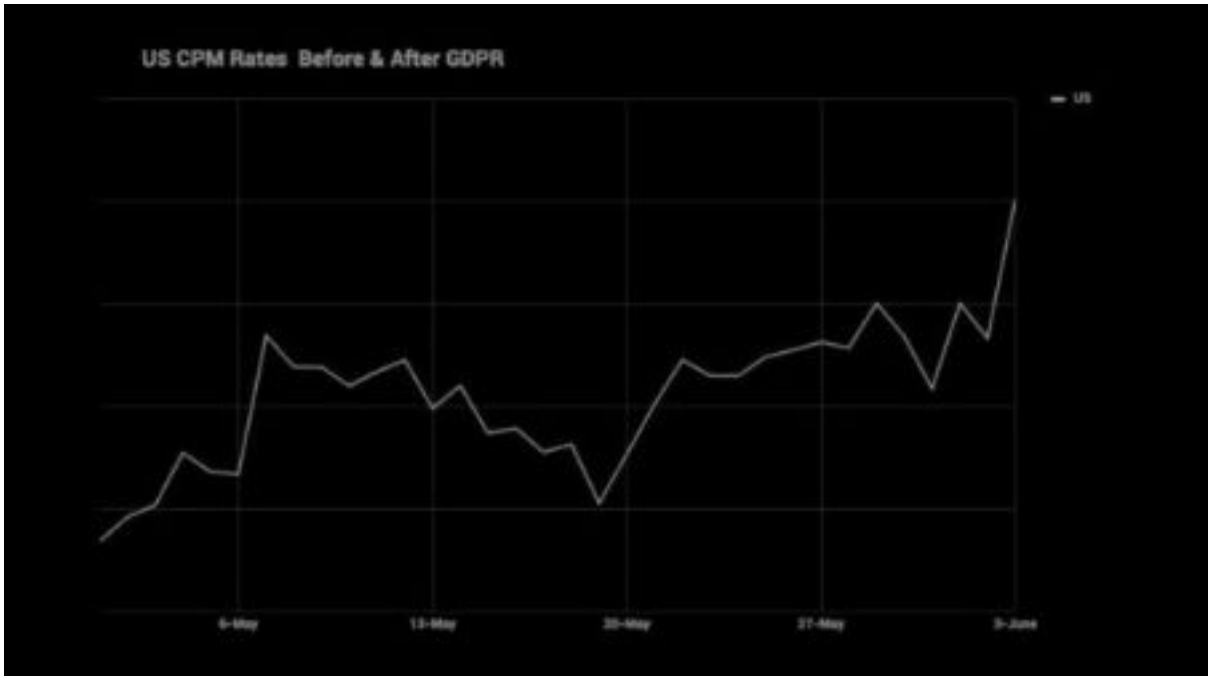
- ★ Austria
- ★ Belgium
- ★ Bulgaria
- ★ Croatia
- ★ Cyprus
- ★ Czech Republic
- ★ Denmark
- ★ Estonia
- ★ Finland
- ★ France
- ★ Germany
- ★ Greece
- ★ Hungary
- ★ Ireland
- ★ Italy
- ★ Latvia
- ★ Lithuania
- ★ Luxembourg
- ★ Malta
- ★ Netherlands
- ★ Poland
- ★ Portugal
- ★ Romania
- ★ Slovakia
- ★ Slovenia
- ★ Spain
- ★ Sweden

Case for Brexit

The regulation will shortly be part of UK law, thanks to the data protection bill that has been working its way through parliament since September 2017, and the government has committed to maintaining it following Brexit. In theory, a future government could change the law again – but even then, any British company wishing to do business with Europeans would have to follow the regulation.

GDPR For US Marketers

U.S. news sites have had a different experience with GDPR then European sites. Two months after the law's enforcement, more than 1,000 news publishers chose to block European visitors from their sites. According to research from ad tech firm Catchpoint, the U.S. version of USA Today's site had an average web-page load time of 9.9 seconds following GDPR's implementation. The version in the U.K. loaded in 0.42 seconds, 0.75 seconds in France and 0.51 in Germany. Those faster load times are attributed to the removal of most external third-party features such as ad servers, Google services and analytics, and social media plugins. Ad rates have increased 10 percent in the U.S. since May 25 and dropped in Europe, according to research from analytics firm Ezoic.



Chances are, even if you're a US company, you have European Union residents in your database. I discussed this with a small regional bank client recently. The marketing manager thinks of her company as being local. But after thinking about it more, she suddenly realized they have foreign investors applying for mortgages, opening bank accounts, etc. This put her in a panic, knowing she needs to get her data collection, website and company policies aligned with GDPR compliance.

Many US companies have been collecting email addresses for years through lead generation programs and eNewsletter subscriptions, without collecting the country

of residence for the subscribers. If this is your situation, you need to get compliant or stop emailing your list.

If you need help with updating your marketing automation platform for GDPR compliance, we can help. We help clients manage their campaigns on several marketing automation platforms, such as Marketo, Salesforce Marketing Cloud (Pardot and ExactTarget), Hubspot, and IBM Marketing Cloud (Silverpop).

Creation of Economic challenges

At the end of May 2018, the most far reaching data protection and privacy regime ever seen will come into effect. Although the **General Data Protection Regulation** (**GDPR**) is a European law, it will have a **global impact**. There are likely to be some unintended consequences of the GDPR.

The implementation of the GDPR opens the potential for new data markets in tradable (possibly securitised) financial instruments. The protection of people's data is better protected through self-governance solutions, including the application of **blockchain technology**.

The GDPR is in effect a **global regulation**. It applies to any company which has a European customer, no matter where that company is based. Even offering the use of a European currency on your website, or having information in a European language may be considered offering goods and services to an EU data subject for the purposes of the GDPR.

The remit of the regulation is as broad as its territorial scope. The rights of data subjects include that of data access, rectification, **the right to withdraw consent**, erasure and portability. Organisations using personal data in the course of business must abide by strict technical and organisational requirements. These restrictions include gaining explicit consent and justifying the collection of each individual piece of personal data. Organisations must also employ a Data Protection Officer (DPO) to monitor compliance with the 261-page document.

Organisations collect data from customers for a range of reasons, both commercial and regulatory—**organisations need to know who they are dealing with**. Banks will not lend money to someone they don't know; they need to have a level of assurance over their customer's willingness and ability to repay. Similarly, many organisations are forced to collect increasingly large amounts of personal data about their customers. Anti-money laundering and counter-terrorism financing legislation (AML/CTF) requires many institutions to monitor their customers activity on an ongoing basis. In addition, many organisations derive significant value from personal data. Consumers and organisations exchange data for services, much off which is voluntary and to their mutual benefit.

One of the most discussed aspects of the GDPR is the **right to erasure**—often referred to as the right to be forgotten. This allows data subjects to use the government to compel companies who hold their personal data to delete it.

We propose that the right to erasure creates uncertainty over the value of data held by organisations. This creates an **option** on that data.

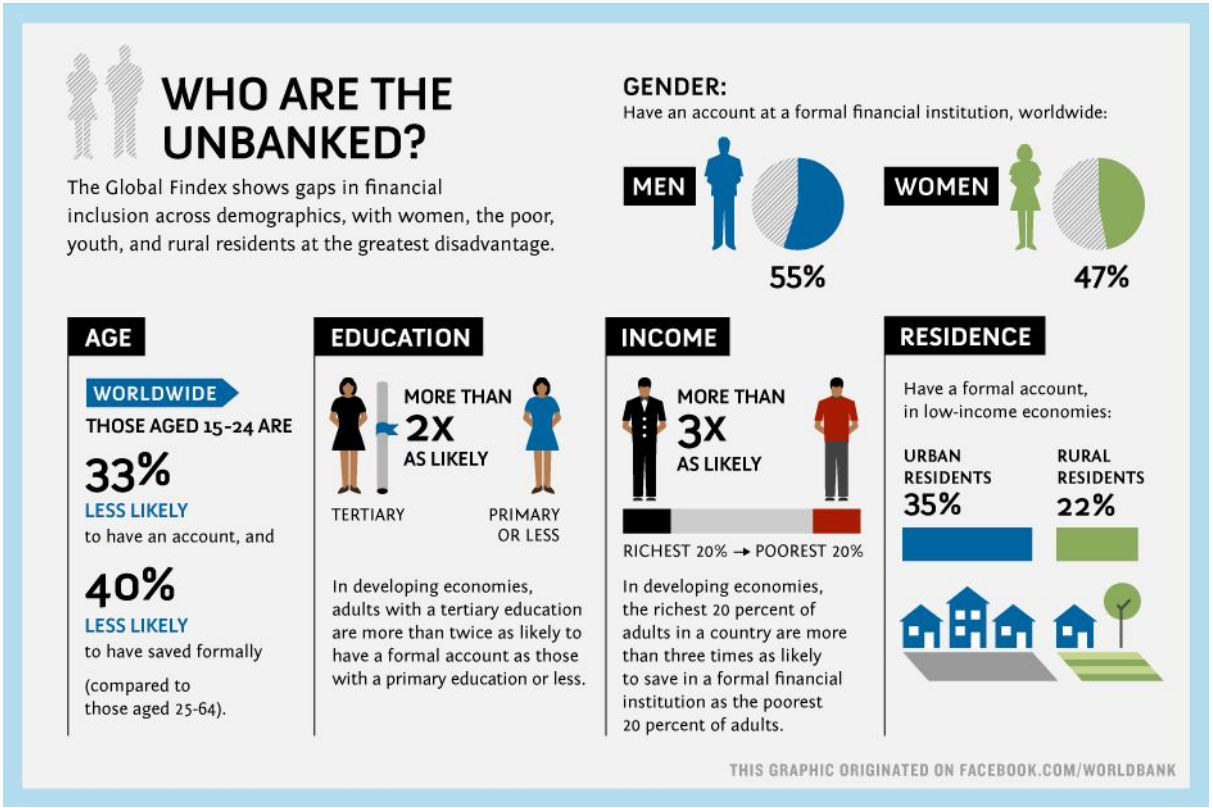
The right to erasure creates uncertainty over the value of the data to the data collector. At any point in time, the data subject may **withdraw consent**. During a transaction, or perhaps in return for some free service, a data subject may consent to have their personal data sold to a third party such as an advertiser or market researcher. Up until an (unknown) point in time—when the data subject may or may not withdraw consent to their data being used—that personal data holds positive value. This is in effect an option on that data—the option to sell that data to a third party.

The value of such an option is derived from the value of the underlying asset—the data—which in turn depends on the continued consent by the data subject.

Rational economic actors will respond in predictable ways to manage such risk. **Data-Backed Securities** (**DBS**) might allow organisations to convert unpredictable future revenue streams into one single payment. **Collateralised Data Obligations** (**CDO**) might allow data collectors to package personal data into tranches of varying risk of consent withdrawal. A secondary data derivative market is thus created—one that we have very little idea of how it will operate, and what any secondary effects may be.

Such responses to regulatory intervention are not new. The Global Financial Crisis (GFC) was at least in part caused by complex and rarely understood financial instruments like Mortgage-Backed Securities (MBS) and Collateralized Debt Obligations (CBS). These were developed in response to **poorly designed capital requirements**.

Similarly, global AML/CTF requirements faced by financial institutions have caused many firms to simply stop offering their products to certain individuals and even whole regions of the world. **The unbanked and underbanked are all the poorer as a result**.



Sources

https://www.superoffice.com/blog/gdpr-crm/

http://data.consilium.europa.eu/doc/document/ST-8394-2018-REV-1/en/pdf

https://www.superoffice.com/blog/gdpra

https://digiday.com/media/gdpr-will-lead-scramble-pass-off-liability-others/

https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you

https://eugdpr.org/the-process/

https://beasleydirect.com/gdpr-countries/

https://www.hopewiser.com/blog/gdpr-opportunity-not-threat

https://youtu.be/S0aTpvBmVnY

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#Timeline

https://gdpr-info.eu/art-1-gdpr/