General Data Protection Regulation (GDPR):  
Reshaping the global data ecosystem and Data rights

Megha R. Rao

San Jose State University

Megha Rajam Rao, M.S. Program in Data Analytics, SJSU

Correspondence address: [megha.rrao90@gmail.com](mailto:megha.rrao90@gmail.com)

12 December 2018

**Abstract**

General Data Protection Regulation (GDPR) is a pan-European legal framework for data privacy and protection of personal information. Effective 25 May 2018, the regulation, enacted by the countries in European union and European Economic area, consists of 99 Articles and 173 Recitals along with explanatory text. A violation can invoke sanctions for regulatory infringement, raking fines of up to 4% of global revenue or 20 million Euros whichever is greater. A breach must be announced within the first 72 hours. Therefore, the landmark bill, while ensuring superior data standards, is heading towards reshaping the global data ecosystem and encouraging other countries to follow suit (Gotts, 2017).

Keywords: General Data Protection Regulation, GDPR, European union, European Economic area

**Table of contents**

Introduction …………………………………………………………… ……………………… 4

The Birth of GDPR: What is GDPR and why was it needed?.…………………………………. 5

List of Rights……………………...…………………………………………………………….. 6

Right to Privacy ……………………………...…………………………………………. 6

Right to Access ……………………………………………………………………….… 6

Right to Erasure…………………………………………………………………………. 6

Right to Suppress……………...…………………………………………………………. 6

Right to Opt out………………..………………………………………………………… 6

Scope of GDPR …………………………………………………………………………………. 7

Exemptions………………...……………………………………………………………………. 7

Impact of GDPR on the EU……………………………………………………………………… 7

Impact of GDPR on US - based Organizations………………………………....……………….. 8

Business Strategies………………………………………………………………………………. 9

The Ethics of Working with Big Data…...…………………………………………..…………. 10

Terminology and key concepts…………….…………………………………………………… 11

Conclusion and Further study …………………………………………………..………...…. 15

References ……………………………………………………………………………………. 16

Figures…….……………………………………………………………………………………. 17

**Introduction**

Before we delve deep into the subject matter at hand, let us take a closer look at the basic and fundamental concept of ethical behavior. Ethics governs the righteous and moral course of action, or simply put – the right thing to do, under circumstances ranging from an insignificant minor situation to a taxing complex conundrum. Prominent ancient scholars such as Pythagoras, Socrates and Aristotle have relentlessly scrutinized, theorized and debated this area of philosophy. Therefore, it comes as no surprise that European Union, a keeper of superior standards, deliberated and deployed a sweeping regulation named General Data Protection regulation, abbreviated as GDPR, to enforce and administer stringent data privacy and protection laws, an acknowledged desideratum in this digital age.

Not an explicit global law, the territorial scope of this regulation specifies businesses in European Economic Area (EEA) as well as all external businesses controlling, processing and/or handling any data pertaining to individuals situated in the EEA. Nevertheless, GDPR precisely stipulates and prescribes the conditions that ensure the adoption of proper data management practices throughout the world. As a preparatory and procedural step towards Brexit, Britain drafted a similar version of the law in 2018 with the royal consent. South Korea, Japan and Brazil are set to follow suit, while California became a frontrunner in the United States by unanimously passing their own data privacy legislature named ‘The California Consumer Privacy Act 2018’.

The historic Californian data privacy bill nicknamed ‘GDPR LITE’ or ‘Mini-GDPR’ inadvertently highlights the humongous global impact of GDPR. According to Roberts (2018), this phenomenon of usage of EU standards as global baseline is called “Brussels effect”. Even though the framework is not all-encompassing, the new data protection regime can spell disaster for non-complaint entities due to the imposition of sanctions and penalties, up to 4% of their revenue, effective the second quarter of 2018. Another point to note is the 72-hour deadline to disclose any data breaches.

# The Birth of GDPR: What is it and why was it needed?

The General Data Protection Regulation, abbreviated as GDPR (2016/679), is the uniform pan-European data protection and privacy regulation jointly formulated by the European Parliament, the Council of the European Union and European Commission, coming under European Economic Area (EEA), aiming to harmonize, strengthen and unify data protection laws for individuals within the European Union in recent times. GDPR consists of 99 Articles, plus 173 Recitals, which provide explanatory text to aid interpretation of the Articles. The new regulation, coming to fruition in the second quarter of 2018, is set to replace the old Data Protection Directive [95/46/EC], which was enacted in 1995 (Gotts, 2018).

The initial proposal to strengthen online privacy rights and digital economy on 25 January 2012 paved the path for the new regulation. It was subsequently adopted by both European Parliament and European Council in April 2016 after rigorous discussions and amendment, followed by the review and approval process. The regulation came into force on 25th May 2018 granting a two-year period for businesses and public bodies to prepare for the paradigm shift. Refer the Figure 1 infographic for the pictorial representation of the timeline in chronological order (Akshita, 2018).

GDPR is a binding legal instrument and not a mere directive like its dated predecessor - The Data Protection Directive [95/46/EC] from 1995. The superseded directive was customized and altered by member countries.

Given the global climate, recent data breaches and subsequent outcry, there was an urgent need to force business entities to comply to higher standards of secure data management. Further, the meteoric pace of technological transformation necessitates the adoption of stringent scrutiny and regulation across all landscapes when dealing with personally identifiable information (PII).

## 

## List of Rights

From my understanding, below are the important rights.

1. **Privacy by Design** - This right disallows the auto-collection of data such as location information, unless the user approves it explicitly upon reading a clearly worded succinct consent form or verbal agreement.
2. **Right to Access** - User is entitled to access and obtain the personal information collected from them.
3. **Right to Erasure** - End users have the right to request for deletion of their personal data by the corresponding data handlers (Controllers or processors) without any undue delay.
4. **Right to Suppress** – User is entitled to demand the ceasing of all activities involving the processing of his/her personal data.
5. **Right to Opt out** – opt out option is mandatory at all times when users are subject to marketing or any other connected activity. Upon opting out, all user information must be removed.

**Scope of GDPR**

It comes as no surprise that entities based in the EU and EEA are subject to this law. External entities with a stake in the data generated from the aforementioned region come under the purview of this law. They could be engaged in offering free or paid good or services; or monitoring the behavior of the EU/ EEA residents.

**Exemptions**

Following are the few sparse exemptions.

* **Personal or household activity**

The law does not apply to individuals using data for purely personal and household activity.

* **Previously collected data**

This must come as a relief to businesses as the law does not apply to personal data collected prior to its enactment, and hence it does not mandate the grandfathering of previously collected data. ("The Regulation," n.d.).

## Impact of GDPR on the EU

Critics of the law expect substantial chunk of content to disappear from the world wide web, especially in Europe. However, the law will guarantee superior quality of life in the region. At least, users will not be bombarded with pages of legal verbose (in the form of ‘Terms and Conditions’) for availing a service or installing a software. The law mandates simple understandable consent forms that do not deny service if we turn decline access to our personal data. A new benchmark in an increasingly notorious world.

GDPR as a measure envisions to achieve the following goals in EU and EEA region.

* Empower and protect EU/EEA citizens and ensure data privacy.
* ‘Harmonize’ or implement uniform binding data privacy laws across the EEA.
* Alter and positively amend the general business approach towards data privacy and protection.
* Penalize violators – A violation can invoke sanctions for regulatory infringement, gathering fines of up to 4% of global revenue or 20 million Euros whichever is greater. Organizations in breach of GDPR can be fined anywhere from 2% up to 4% of annual global revenue (based on the magnitude of the breach) or €20 Million, whichever is higher, in case of a major breach ("General Data Protection Regulation," n.d.).
* Breach notification - A breach must be announced within the first 72 hours, without any undue delay ("General Data Protection Regulation," n.d.).

### Impact of GDPR on US - based Organizations

Organizations in the United States have been in the spotlight owing to scandalous data breaches that affected millions of users in recent times. Notorious security issues have garnered global attention and massive public outcry. Nevertheless, the likes of Google and Facebook may not develop a parallel data model for EU/EEA customers, as it will result in exorbitant costs along with a convoluted data management system. They are most likely to reshape their data ecosystem and collect only essential data from their users throughout the world.

Ironically, Mark Zuckerberg, the leader of Facebook (FB), had welcomed GDPR in his testimony during his congressional hearing at Capitol Hill. Juxtaposing the rift of lawsuits FB accumulated due to GDPR enforcement, its seems hard to believe. Facebook and its subsidiaries such as Instagram, and Google have raked more than 8 billion dollars in fines since the enforcement of GDPR.

It is clearly evident that companies on the road to GDPR compliance are anxious as they evaluate their current status, preparedness and susceptibility to breaches and hacks. Surprisingly, bigger companies are more relaxed about their enforcement because they have resources such as money and manpower to deal with this seemingly massive endeavor. Also, it will eliminate budding competitors who struggle with the high operational costs and end up leveraging their data assets to thrive in the business world. Furthermore, they are vulnerable and lack the necessary financial resources to refine and strictly control their data processing model. Therefore, small businesses bear the brunt and suffer the most.

As explained before, Brussels effects is the phenomenon where European standards form the foundation of changes throughout the world. This milestone law has already trickled down and convinced administrations across the world to deliberate and introduce new laws to ensure better quality of life for their citizens in the form of superior data rights. A bill nicknamed ‘Mini-GDPR’, unanimously passed in California, is the foremost copycat law, bearing stark resemblance to GDPR in the United States.

**Business Strategy**

Companies must seriously analyze their data footprint in the EU/EEA, evaluate their data management and control strategy, design a roadmap to GDPR compliance if it is not already on track, fastrack their data privacy and protection mechanisms with crisis and breach management plan, ensure data transparency, and control and anticipate any data hacks and attacks. They may also need to upgrade their security tools, appoint a Data Protection officer (DPO), gather documentation and proof of GDPR compliance ("General Data Protection Regulation (GDPR)," n.d.).

**Ethics & Working with Big Data**

Since time immemorial, ethics has been a constant subject of debate. But in a contemporary setting, Susan Etlinger, a leading industry analyst, pointed out in her [2014 TED talk](https://www.ted.com/talks/susan_etlinger_what_do_we_do_with_all_this_big_data) that Big Data is as powerful and error-prone as it is big. Even though we can process data at rapid pace, mistakes can be made quickly as well. Furthermore, general population tends to blindly believe the attractive infographics presented by Data analysts, which could be misleading many a times. Hence, it is imperative to implement an ethical framework to govern and guide our decisions. As illustrated in Figure 2, Ms. Etlinger suggests the following steps to incorporate ethics in big data. We need to analyze and gauge the value and insights offered by the evaluation beforehand. The methods should be progressive, with minimal data usage, lower costs and quicker processing. If possible, design a less – intensive and economical process. Overall, we should aim for the most efficient data analytics mechanism. The resultant insights should also be sustainable and applicable to different diverse data sets along with algorithm and device longevity. Not to forget, we need to be respectful to businesses and anticipate the tremendous downstream impact of a small analytics decision. We should also keep confidential information secure. Finally, we need to be fair and decline from producing discriminatory content based on race, gender or age. There are the pragmatic steps to follow while handling emerging Big data technologies, varied business models and data of immense complexity (Kassner, 2017).

Regarding Hadoop, it comes a long way since its initial conception and remediated security issues and upgraded in-built mechanisms in recent times. As explained in the class lecture, the five pillars of security are Administration, Authentication, Authorization, Audit, & Data Protection. However, any breach, internal or external will dislodge its elevated position and tarnish its image and reputation. Stakeholder such as shareholders, customers and users will lose confidence and trust in Hadoop (Mules, 2018).

Let us not forget that numerous benefits, such as value-added processing, low cost and so on, placed Hadoop at the apex of modern technological architecture. Fall from the top can result in serious injuries. Privacy violations and sanctions, as well as, regulatory infractions can have a detriment impact on Hadoop’s pleasant Elephant image. Therefore, it is vital to innovate and progress with newer superior products. Hadoop Data Plane Service is the answer to our woes. It is an extendible, reliable, consistent service which is a definite upgrade from the previous services. It provides consistent security and governance across all landscapes (Mules, 2018).

As aspiring data practitioners, it is our personal responsibility to ensure and aim for higher integrity, refrain from exploiting sensitive data, anticipate attacks, secure confidential information, check for sustainability and efficiency, authenticate data and adopt superior business standards.

## Terminology and key concepts

Taken from GDPR EU.org, below are the definitions and key concepts pertaining to the law ("General Data Protection Regulation (GDPR)," n.d.; “GDPR key changes”, n.d.).

* **Personal data**

Article 4(1) defines “personal data” as any information directly or indirectly relating to an identified / identifiable natural person  called the **‘data subject’**; even with reference to specific traits of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

* **Behavioral analysis**

Recital 24 states: “In order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes.” This sounds like Data Analytics.

* **Online identifier definition**

Recital 30 clarifies “online identifier” as mentioned in the Article 4 definition – “Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”

* **Prohibited categories**

Collection of following types of personal sensitive information is forbidden -

* Race and ethnicity
* Political, religious, or philosophical beliefs, including union membership
* Health, sex life, and sexual orientation
* Genetic and biometric data (for the purpose of uniquely identification)

**Exemptions**: Explicit consent, Employment, Vital interests, Membership organizations, Publicly disclosed data, Legal proceedings, Substantial public interest, Medicine, Public health and Research.

* **Consent**

One of the six possible legal grounds for data processing is Consent and Article 4 defines consent as - freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. It can be a written statement, including by electronic means, or an oral statement.

This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out and for multiple purposes, consent should be given for each of them. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.”

* **Legitimate interest**

According to Article 6(1): “Processing shall be lawful only if: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party; (c) processing is necessary for compliance with a legal obligation; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by fundamental rights; (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.” Hence, law enforcement agencies can override this clause.

## Data Controller and Data Processor

Article 4 defines data controllers and data processors as below: **‘controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; (8) **‘processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

* **Data Protection officer (DPO)** According to Article 37(1), data controllers and processors shall designate a DPO where: (a) the processing is carried out by a public authority, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

DPO can be contractors or employees with expert knowledge in GDPR and data protection laws. They must prioritize GDPR-related tasks above other tasks. Hence, major operational changes would be the appointment of a DPO, acquiring and managing user consent and breach management within the assigned 72 hours (“GDPR key changes”, n.d.).

##### **Conclusions and Future Study.**

Even though GDPR does not prohibit use of personal data for analytics, it does restrict access and obligate compliance to a comprehensive legal framework making the EU a pioneer data watchdog. It is predicted to rapidly extend beyond the European borders and become a de facto law providing a fundamental foundational framework for other countries to act upon. For the world, this landmark bill is a positive move, whereas for businesses, an expensive move, although quintessentially ethical. Nonetheless, critics of the regulation believe that it fails to address the subtle intricacies of data collection, storage and transfer. Another challenge is the rapid pace of technological evolution bringing forth newer scenario to confront and apprehend at lightning pace for both lawmakers and enforcers.

EU/EEA has gained prominence as the foremost player, influencer and global exporter of data protection and privacy laws. The benchmark bill reiterates the proactive stance of the zone in establishing global standards and implementing futuristic solutions. Data privacy and protection, succinctly encapsulated in the term ‘data rights’ is most likely to be considered a basic human right in the near future. Hence, GDPR is bound to become the leading exemplar with potentially far-reaching implications, renewing interest, re-igniting contemporary debate, and eventually sparking a positive movement in this data-driven world. The effectiveness of the regulation, amendments and subsequent global impact will serve as an area for perusal and future study.

**References**

# Gotts, I. (2018). Trickle Down GDPR — Why Every ISV is Impacted [Blog post]. Retrieved from <https://medium.com/inside-the-salesforce-ecosystem/trickle-down-gdpr-why-every-isv-is-impacted-7e913db6047c>

# Roberts, J. J. (2018).[The GDPR Is in Effect: Should U.S. Companies Be Afraid?](http://fortune.com/2018/05/24/the-gdpr-is-in-effect-should-u-s-companies-be-afraid/) [Blog post]. Retrieved from <http://fortune.com/2018/05/24/the-gdpr-is-in-effect-should-u-s-companies-be-afraid/>

# Akshita. (May 2018). What is GDPR? User Rights and Business guidelines[Blog Post]. Retrieved from <https://opensenselabs.com/blog/articles/gdpr-user-rights-business-guidelines>

# The Regulation, n.d. [Web Post]. Retrieved from [https://www.gdpreu.org/the-regulation/](https://www.gdpreu.org/the-regulation/who-must-comply/) ]

# General Data Protection Regulation, n.d. [Web Post]. Retrieved from <https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>

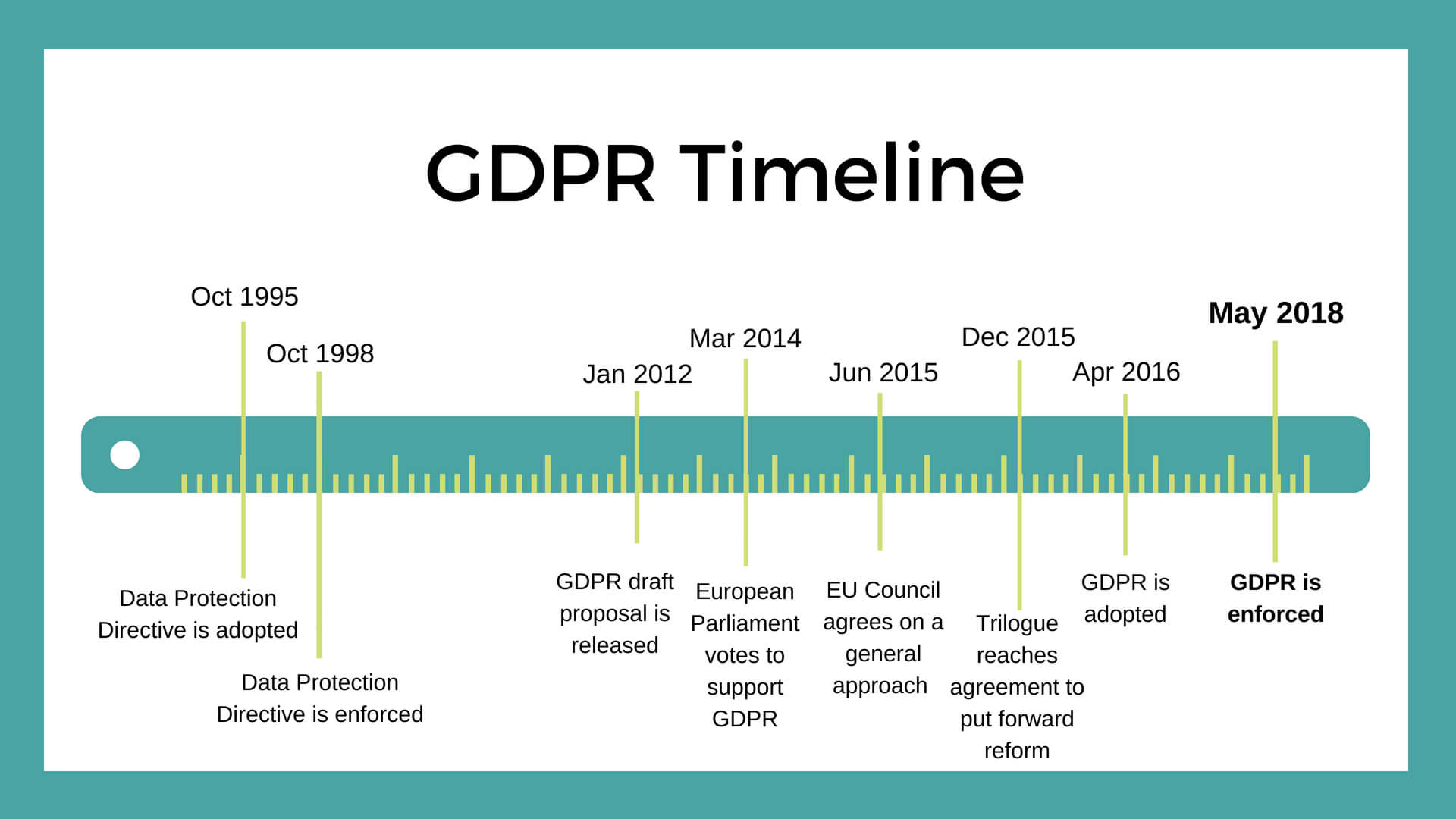
# General Data Protection Regulation (GDPR), n.d. [Blog Post]. Retrieved from <https://www.pwc.com/us/en/services/consulting/cybersecurity/general-data-protection-regulation.html>

# Altimeter, S. E., and Groopman, J., adapted by Kassner, M., 2017. Principles of Ethical Data Use [Blog post]. Retrieved from <https://www.techrepublic.com/article/5-ethics-principles-big-data-analysts-must-follow/>

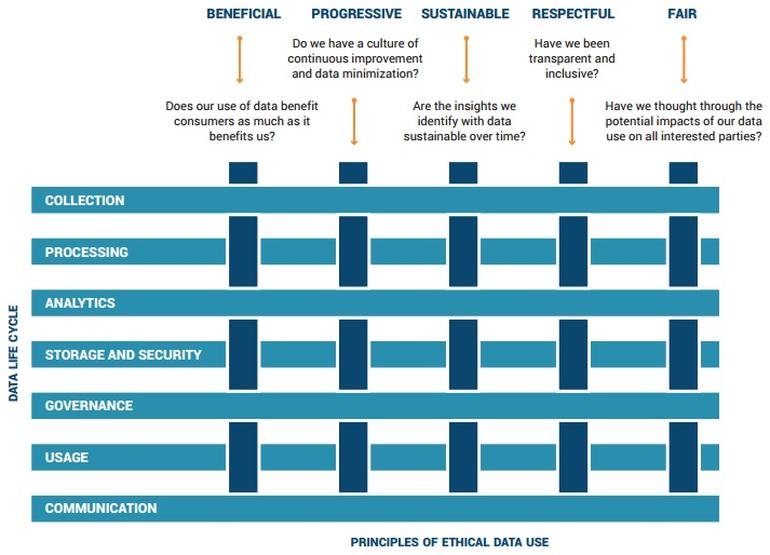
1. Mules, R. J. G. (2018). 09- Data Governance and Data Security [PowerPoint presentation]

# GDPR key changes, n.d. [Web post]. Retrieved from <https://eugdpr.org/>

Figures



*Figure 1*. GDPR Timeline infographic (Data from Akshita. (2018). *What is GDPR? User Rights and Business guidelines.* Retrieved from <https://opensenselabs.com/blog/articles/gdpr-user-rights-business-guidelines>



*F*igure 2. Principles of Ethical Data Use (Altimeter, S. E., and Groopman, J., re-printed by Kassner, M., 2017). Retrieved from <https://www.techrepublic.com/article/5-ethics-principles-big-data-analysts-must-follow/>