GDPR: The Need of the Hour

Manish K.Salian[1]

Abstract

The tremendous development of digital data has directed to an extensive intensification in data breaches. To encounter the confidentiality apprehensions of the digital world and place protections about personal data, the EU Parliament implemented the General Data Protection Regulation (GDPR) in April 2016. Enterprises can conquest client's goodwill if they fulfil with the real-world procedures enumerated in the GDPR. Therefore, this article will specifically focus on the GDPR regulations and its contribution to the society specially to the data protection of a man. This article shall also emphasize on the company purview of the same too.

Keywords: General Data Protection Regulation (GDPR); EU; privacy; data protection.

Introduction

Privacy per se is an unquestionable right of an individual comprehensively bonded with his/herlife. Privacy becomesa matter of disagreement when it is mishandled/intruded illegitimately by erroneous individuals. Breach of privacy by oneself is less effective whereas deployed by third party is heinous. The disclosure of private information by third party brings disgrace/shame to victims although they are ignorant of.

A privacy policy is one of the most vital and imperative document on any website. It details the corporation's interpretations and procedures on the information collected from visitors. Although a privacy policy is officially a legal document, prodigious effort should be made to craft a document that is both accurate, truthful and easy to understand, obscuring secreted clauses in reams of text is not acceptable.

General data protection regulation (GDPR)

The European Union's General Data Protection Regulation (GDPR) was permitted in April 2016 and will go into effect May 25, 2018. The regulation necessitates businesses to protect the personal data and privacy of EU citizens. It announces threatening fines for non-

[1] Assistant Manager – Legal99Games Online Pvt Ltd, Udupi 576105.

compliance and breaches, and gives people more say over what companies can do with their data. Any company that does businesses in Europe need to comply with GDPR. The GDPR arranges out in strong footings guidelines for what personal data is and how it can be used. In undertaking so, it places the right to personal data safety and protection in the same grouping as freedom of expression and the right to a fair trial. Once it goes into effect, the GDPR will be enforced in all EU member states. However, even if you aren't an EU citizen, if you conduct business with EU clients, you will have to ensure the organization is acquiescent. In fact, the possibility of the GDPR is so overarching, anyone conducting business online will prospectively see some correlatedvicissitudes. Many of the procedures go expressivelysupplementary than what is required by other regulations, including those of the United States and Canada.[2]

In the meekest standings,the GDPR can be explained down into three key concepts[3]:

Consent and control

Under the GDPR an individual has an elementary right to control over his or her personal data and is obligatory to give consensus by pure favourable action to any entity wishing to use their data for any reason. The individual is also entitled to withdraw consent as easily as it was given. The entity requesting the data must inform the individual of how their data will be used and only gather as much data as needed for the stated purpose.

Transparency

In case of a security breach when data possibly will have been negotiated, the controllers and individuals whose material data may have been compromised must be notified and provided full disclosure, including an explanation of what happened and what is taking place to remedy the situation, as well as a recommendation of what the individuals might do to protect themselves.

Granting of Individual Privileges

Have you ever signed up for a service that you later cancelled only to be continuously inundated by emails? Under the GDPR, individuals are given comprehensive rights to access, correct, port, erase, and object to the processing and storage of their data.

[2]Reiner's, ZD 2015, 51,55; Martini, in: Paal/Pauly, DSGVO, Art 25(2017), rec 45.
[3] Patrick O'Kane, *GDPR - Fix it Fast: Apply GDPR to Your Company in Ten Simple Steps Kindle Edition*. Brentham House Publishing Company Ltd. (12 December 2017).

Objective and Scope

The complete objective of GDPR is to give citizens back control of their personal data and to streamline the regulatory environments for global business by amalgamating data and privacy regulations. GDPR is a regulation and substitutes a directive (the Data Protection Directive). With a regulation, GDPR supports to unify data and privacy regulation in EU to diminish administration and inconsistencies among native laws. With directives, unlike regulations, each member state has discretion as to implementation of data protection regulation and can thus differ from country to country.

Despite the fact the regulation initiates from EU, it correspondingly applies to companies outside EU offerings goods and services (paid or free) or who monitor the behaviour of individuals in EU. Under the former Data Protection Directive, a business was subject to the data protection law only if it was located in an EU country or used equipment in an EU country to process data. Nevertheless, the new regulation also applies to any business that offers goods or services to individuals in the EU or monitors such individuals' behaviour. This is a far-reachingenlargement of the necessities that will affect many more organizations across the world.[4]

Requirements of General Data Protection Regulation 2018[5]

The GDPR itself contains 11 chapters and 91 articles. The following are some of the chapters and articles that have the greatest potential impact on security operations:

Articles 17 & 18– Articles 17 and 18 of the GDPR give data subjects more control over personal data that is processed automatically. The result is that data subjects may transfer their personal data between service providers more easily (also called the "right to portability"), and they may direct a controller to erase their personal data under certain circumstances (also called the "right to erasure").

Articles 23 & 30– Articles 23 and 30 require companies to implement reasonable data protection measures to protect consumers' personal data and privacy against loss or exposure.

Articles 31 & 32– Data breach notifications play a large role in the GDPR text. Article 31 specifies requirements for single data breaches: controllers must notify SAs of a personal data

[4]It Governance Privacy Team. Eu General Data Protection Regulation (Gdpr): An Implementation and Compliance Guide. Itgp; 2nd ed. edition (31 August 2017).
[5]DIGITALGUARDIAN (April 26, 2018),https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.

breach within 72 hours of learning of the breach and must provide specific details of the breach such as the nature of it and the approximate number of data subjects affected. Article 32 requires data controllers to notify data subjects as quickly as possible of breaches when the breaches place their rights and freedoms at high risk.

Articles 33 & 33a– Articles 33 and 33a require companies to perform Data Protection Impact Assessments to identify risks to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed.

Article 35– Article 35 requires that certain companies appoint data protection officers. Specifically, any company that processes data revealing a subject's genetic data, health, racial or ethnic origin, religious beliefs, etc. must designate a data protection officer; these officers serve to advise companies about compliance with the regulation and act as a point of contact with Supervising Authorities (SAs). Some companies may be subjected to this aspect of the GDPR simply because they collect personal information about their employees as part of human resources processes.

Articles 36 & 37– Articles 36 and 37 outline the data protection officer position and its responsibilities in ensuring GDPR compliance as well as reporting to Supervisory Authorities and data subjects.

Article 45– Article 45 extends data protection requirements to international companies that collect or process EU citizens' personal data, subjecting them to the same requirements and penalties as EU-based companies.

Article 79– Article 79 outlines the penalties for GDPR non-compliance, which can be up to 4% of the violating company's global annual revenue depending on the nature of the violation.

Consent policy under GDPR[6]

There are definite requirements to obtain valid and lawful consent. The consent must be informed, unambiguous, explicit, freely given, specific and have the right to withdraw and written in a pain language that it's evidently visible. For consent to be informed, the individual must receive at least the following information:

- the identity of the organisation processing data;

[6] Stephen R Massey, *The Ultimate GDPR Practitioner Guide: Demystifying Privacy & Data Protection.* Fox Red Risk (18 December 2017).

- the purposes for which the data is being processed;
- the type of data that will be processed;
- the possibility to withdraw the given consent (for example, an unsubscribe link at the end of an email)
- if the consent is related to an international transfer, the possible risks of data transfers to third countries.

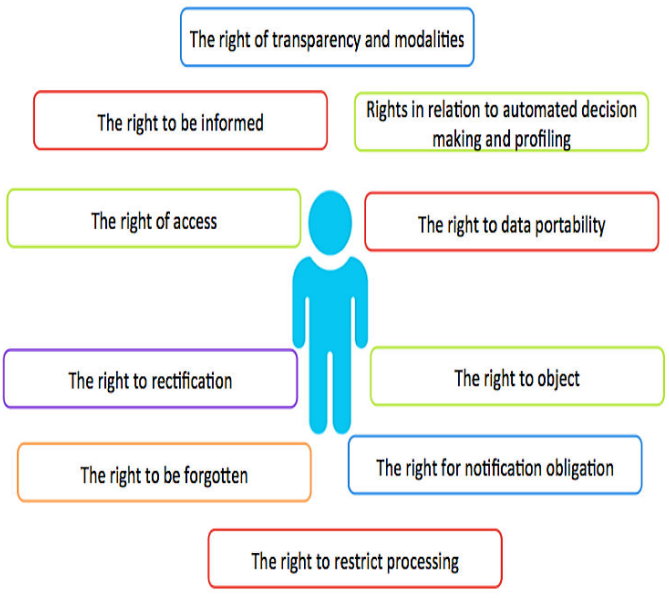
It should be as easy to pull out as to give consent. If consent is withdrawn the company/organisation can no longer progress the data. Once consent has been withdrawn, thecompany/organisation needs to ensure that the data is deleted unless it can be processed on another legal ground (for example storage requirements or as far as it is a necessity to fulfil the contract). If the data was being processed for several purposes the company/organisation can't use the personal data for the part of the processing for which consent has been withdrawn or for any of the purposes, depending on the nature of the withdrawal of consent.[7]

Example: You're providing an online magazine. The patron gives their consent to subscribe to the online magazine that permits you to process all the data on their interests to build a profile of what articles they consult. One year on, they inform you that they no longer wish to receive the online magazine. You must delete all personal data relating to that person collected in the context of the magazine subscription from the database, including the profile(s) relating to that person.

GDPR also requires you to keep evidence of consent – who, when, how, and what you told people. Good practice would be to document both consent given and rejected for visitors and customers when you process their personal data.

Individual rights under GDPR[8]

Recognition of individual's control over his/her personal data is the fundamental achievement of the GDPR. To materialize this fundamental principle, the GDPR



[7]Clader, Alan. Eu Gdpr: A Pocket Guide Pap
[8] Sagara Gunathunga (Director @WSO2, Tec
Open Source Developer, Committer @ Apacl
rights-under-gdpr-3256fb3f356c.

define set of well-defined rights and introduce well defined process for individuals to execute these rights, to be in compliance with the GDPR data processing organizations should accept these set of rights and should facilitate each individual to execute these rights.

- The right of transparency and modalities[9].
- The right to be informed.
- The right of access.[10]
- The right to rectification.[11]
- The right to be forgotten.[12]
- The right to restrict processing.[13]
- The right for notification obligation[14].
- The right to data portability[15].
- The right to object[16].
- The Right in relation to automated decision making and profiling.[17]

The right of transparency and modalities

The data processing organizations must provide the information related to following activities in a concise, transparent, intelligible and easily accessible form, using clear and plain language, it is also possible to use appropriate visualizations such as standardized icons. Additionally, it's expecting special care on information specially addressed to a child.

- When personal data are collected from the data subject.
- When personal data are not collected directly from the data subject.
- When communicating with an individual related to right of access.
- When communicating with an individual related automated individual decision-making.
- When communicating with an individual about personal data breach.

Data processing organizations must facilitate to execute 'right for access information' and 'right for not to be subject to a decision based solely on automated processing' by their

[9]Article 12 – GDPR.
[10] Art. 15 GDPR.
[11] Art. 16 GDPR.
[12] Art. 17 GDPR.
[13] Art. 18 GDPR
[14] Art. 19 GDPR.
[15] Art. 20 GDPR.
[16] Art.21 GDPR.
[17] Art.22 GDPR.

consumers. The only exception here is, cases where the organization can't identify the requested individual uniquely.

When an individual made a request to access information, the processing organizations must respond to the individual without any delays according to the following time constraints.

- Generally, within the one month of receipt of the request.
- Considering the complexity and number of the requests, an organization can extend above one-month period by two further months but the organization must inform any such extension to the individual within one-month period together with the reasons for the delay.
- In case an organization does not take action on the request, it should inform the individual within one-month period with the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority.

Additionally, organizations should provide above information's free of charge but it's possible to include .administrative fee, also organizations should properly identify the individual before provide any information, if required organizations can request additional data for user identification/verification purposes.[18]

The right to be informed

According to this principle individual must be informed before data is gathered. If personal data is collected directly from an individual, the processing organization must provide the following information to the individual at the time of collection of those data.

- Organization's identity and contact details including representatives within EU.
- Contact details of the data protection officer (if applicable).
- Purposes of and legal basis for the processing of personal data.
- Recipients or categories of recipients.
- Details of data transfer outside the EU, including how the data will be protected and how an individual can obtain a copy of the implemented safeguards.
- Retention period for the personal data, or if that is not possible the criteria used to determine the retention period (e.g. 1 year after the end of the contractual relationship);

[18] Ruth Boardman, James Mullock, Ariane Mole; *Guide to the General Data Protection Regulation*, Bird and Bird, May 2017.

- That the data subject has a right to access and rectify its personal data, to object to or request erasure or restriction of the processing, and to data portability.
- Where the processing is based on consent, that the data subject has a right to withdraw its consent for the processing at any time.
- That the data subject can lodge a complaint with a supervisory authority;
- whether there is a statutory or contractual requirement to provide the data or if the provision of data is necessary to enter into a contract.
- Whether there will be any automated decision taking.

In cases personal data are NOT collected directly from individuals, processing organizations should provide following details to individuals.

- Organization's identity and contact details including representatives within EU.
- Contact details of the data protection officer (if applicable).
- Purposes of and legal basis for the processing of personal data.
- Recipients or categories of recipients.
- Details of data transfer outside the EU, including how the data will be protected and how an individual can obtain a copy of the implemented safeguards.
- Retention period for the personal data, or if that is not possible the criteria used to determine the retention period (e.g. 1 year after the end of the contractual relationship);
- That the data subject has a right to access and rectify its personal data, to object to or request erasure or restriction of the processing, and to data portability.
- Where the processing is based on consent, that the data subject has a right to withdraw its consent for the processing at any time.
- That the data subject can lodge a complaint with a supervisory authority;
- whether there is a statutory or contractual requirement to provide the data or if the provision of data is necessary to enter into a contract.
- Whether there will be any automated decision taking.
- The categories of personal data concerned
- From which source the personal data originates, and if applicable whether it came from publicly accessible sources.

If a processing organization intends to further process personal data for a purpose other than the original purpose, then it must provide information on new purposes to each individual

prior to the further processing. Also, it should be noted that above information sharing or communications with an individual should not contradict with EU laws and member state laws.[19]

The right of access

According to this right each individual has the right to request access to his/her own personal data and to ask how their data is used by the processing organization once it has been gathered.[20] Usually this can be done by submitting a subject access request (SAR). When requested the processing organization is obligated to provide a copy of the data. According to the GDPR processing organizations should provide following information to individuals when requested.

- Confirmation on whether or not personal data concerning him/her are being processed.
- If processed where that.
- Access to proceed personal data.
- Purposes of the processing.
- The categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed.
- If possible, the envisaged period for which the personal data will be stored.
- The existence of the right to request for rectification or erasure of personal data or restriction of processing of personal data.
- Where the personal data are not collected from the data subject, any available information as to their source;
- The existence of automated decision-making.

In addition to above when personal data are transferred to a third country or to an international organization, an individual has the right to be informed. However, this right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property or copyrights.[21]

[19]James Walker,*Preparing for the EU GDPR: What You Need To Know*, SC Media (April 27, 2018), https://www.scmagazineuk.com/preparing-for-the-eu-gdpr-what-you-need-to-know/article/531492/
[20]*Ibid.*
[21]*Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now*.Information Commissioner's Office (April 27, 2018),https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

The right to rectification

Individuals should have the right to require the processing organization to correct errors in personal data processed without any delays.

The right to be forgotten

Individuals should have the right to request the processing organizations to erase of personal data without any delays and the processing organizations should obligate to such requests in any of the following situations.

- Personal data captured no longer required for the captured purpose.
- When the individual withdraws consent on the processing of data and there is no other legal context to process the data.
- When the individual objects to the processing pursuant.
- When personal data have been unlawfully processed.
- When personal data have to be erased to be in compliance with a legal obligation.
- Personal data have been collected in relation to the offer of information society services related to a child.

As an example, if an individual is no longer a customer of your business, or if the particular individual has withdrawn his/her consent from your company to use the personal data, then the individual has the right request for data deletion. Additionally, when a processing organization make personal data public, an individual can request to erase any links to, or copy or replication of those personal data.[22]

The right to restrict processing

It's possible for an individual to request from a processing organization to restrict his/her personal data processing. In such cases the processing organization may continue to store the data, but the purposes for which the data can be processed are strictly limited. To support such features processing organizations should have capabilities to segregate affected data from the processing system. According to the GDPR an individual can make restriction requests in following situations.

- An individual opposes to erase the data instead request to restrict the use.

[22] GENERAL DATA PROTECTION REGULATION (GDPR), RECITALS (April 27, 2018), https://gdpr-info.eu/.

- When the personal data are inaccurate, for the period during which the processing organization is verifying the data.
- Cases where the personal data are no longer required for the processing of the original purpose but the processing organization is not in position to erase those data due to legal background.
- According to GDPR an individual can object for processing his/her personal data, in such cases processing organization can verify whether there is legal ground exists to override the such requests. In a situation where the results of such verification process are pending, effected personal data should be restricted for processing.
- Additionally, before lifting any processing restrictions, the processing organization must inform the individual in a concise manner.

The right for notification obligation regarding rectification/erasure/restriction

In following cases processing organization should communicate to the individual in a concise manner.

- Personal data rectification.
- Personal data erasure.
- Personal data restriction.

Additionally, when requested by an individual, the processing organization should reveal information about the recipients of individual's personal data.

The right to data portability[23]

When the data processing is based on consent or contract, individuals have the right to receive own personal data from a processing organization which he/she has provided. However, the right to portability does not apply where the processing is based on any other legal ground than consent or contract such as public interests.

When responding to such requests, an individual has right to receive that information in a structured, commonly used and machine-readable format. This facilitate to transmit received information to another organization easily.

[23]PaulDeHert, VagelisPapakonstantinou, GianclaudioMalgieri, Laurent Beslay, Ignacio Sanchez; *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, Elsevier Publications, Volume 34, Issue 2, April 2018.

When technical feasibility exists, an individual can request to transfer his/her personal data from one processing organization to another directly. In practise in order to support this feature both of the organizations should have mutual contract and technical capabilities to transfer the data. For example, System for Cross-domain Identity Management (SCIM) can be used to transfer identity related personal data from one organization to another.

The right to object

An individual can object to processing of own personal data at any time, in such cases the processing organization should stop the processing of affected data unless they can demonstrate legitimate ground to carry out processing of affected data. This regulation is applicable for scientific, historical research or statistical purposes as well.

According to GDPR direct marketing is a special case where an individual can object to processing of own personal data at any time and upon receiving a such objection the processing organization should not process concerned personal data for the purpose of direct marketing.

GDPR also expect from processing organization to present above "right to object" and "right to object for direct marketing" in a clearly and separately from any other information at least during 1st communication with an individual. For example, you cannot hide above information of objects to rights with the applicable general terms and conditions policy.

Rights in relation to automated decision making and profiling

An individual has the right not to be subject to decisions based solely on automated processing which significantly affect them. Online credit application, e-recruiting or e-evaluation of performance without any human intervention are some of the examples for solely automated processing.

Also, even the cases where an individual consent for automated decision-making, he/she has rights to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision etc. By the way execution of above rights should not be contradictory with public safeguard matters such as national & public security, defence, rights and freedoms of others, judicial proceedings

GDPR Enforcement and Penalties[24]

The EU General Data Protection Regulation (GDPR) has fascinated media and business interest for the reason that it has augmented administrative fines for non-compliance. Not all infringements of the GDPR will lead to those serious fines. Above and beyond the power to impose fines, the Information Commissioner's Office (ICO) has a range of corrective powers and sanctions to enforce the GDPR. These include issuing warnings and admonishments; imposing an impermanent or permanent ban on data processing; ordering the rectification, restriction or erasure of data; and suspending data transfers to third countries.

Administrative Fines

The administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be "effective, proportionate and dissuasive".

There are two tiers of administrative fines that can be levied:

1) Up to €10 million, or 2% annual global turnover – whichever is higher.

2) Up to €20 million, or 4% annual global turnover – whichever is higher.

The fines are based on the specific articles of the Regulation that the organisation has breached. Infringements of the organisation's obligations, including data security breaches, will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level.

When deciding whether to impose a fine and the level, the ICO must consider:

- The nature, gravity and duration of the infringement;

[24] Per-Arne Fors: *GDPR Compliance – All you need to Know,* CreateSpace Independent Publishing Platform, 2018, Pg 35-38.

- The intentional or negligent character of the infringement;
- Any action taken by the organisation to mitigate the damage suffered by individuals;
- Technical and organisational measures that have been implemented by the organisation;
- Any previous infringements by the organisation or data processor;
- The degree of cooperation with the regulator to remedy the infringement;
- The types of personal data involved;
- The way the regulator found out about the infringement;
- The manner in which the infringement became known to the supervisory authority, in particular whether and to what extent the organisation notified the infringement;
- Whether, and, if so, to what extent, the controller or processor notified the infringement; and
- Adherence to approved codes of conduct or certification schemes.[25]

Liability for damages

The GDPR also gives individuals the right to compensation of any material and/or non-material damages resulting from an infringement of the GDPR. In certain cases, not-for-profit bodies can bring representative action on behalf of individuals. This opens the door for mass claims in cases of large-scale infringements.[26]

Enforcement authority

\The GDPR implementation is done through Data Protection Authorities (DPA's) who make availableprofessionalguidance on data protection issues and handle complaints against desecrations of GDPR. There is one in each EU Member State.The foremostconnection point for questions on data protection is the DPA in the EU Member State where the company/organisation is grounded. Nevertheless, if the company/organisation processes data in different EU Member States or is part of anassemblage of companies established in different EU Member States, that main contact point may be a DPA in additional EU Member State.

The company/organisation needs to appoint a DPO, whether it's a controller or a processor, if its fundamental activities encompass dispensation of sensitive data on a bulky gage or

[25] Michael Nadeau, General Data Protection Regulation (GDPR): What you need to know to stay compliant, APR 23, 2018, https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.
[26] Stephen R Massey; *The Ultimate GDPR Practitioner Guide: Demystifying Privacy & Data Protection*, Fox Red Risk, 2017.

involve large scale, consistent and systematic monitoring of individuals. In that respect, monitoring the behaviour of data subjects includes all forms of tracking and profiling on the internet, including for the purposes of behavioural advertising. The DPO may be a staff member of the organisation or may be contracted externally on the basis of a service contact. A DPO can be an individual or an organisation. It is worth mentioning that the GDPR is based on a risk-based approach and organisations are encouraged to implement protective measures corresponding to the level of risk of their data processing activities.[27]

If data breach occurs when the data for which the company/organisation is accountablegrieves a security incident resulting in a breach of confidentiality, availability or integrity. If that occurs, and it is likely that the breach poses a risk to an individual's rights and freedoms, the company/organisation has to notify the supervisory authority/DPO (if an internal person in staff) without undue delay, and at the latest within 72 hours after having become aware of the breach. If the company/organisation is a data processor it must notify every data breach to the data controller.[28]

Conclusion

The General Data Protection Regulation (GDPR) is grounded on the risk-based approach. Companies/organisations dealing out personal data are stimulated to contrivance protective measures conforming to the level of jeopardy of their data processing activities. Therefore, the obligations on a company processing a lot of data are more onerous than on a company processing a small amount of data.

For example, the likelihood of engaging a data protection officer for a company/organisation dealing outwith a lot of data is higher than for a company/organisation processing a small amount of data. Next to the equivalentperiod, the nature of the personal data and the impact of the envisaged processing also play a role. Processing of a small amount of data, but which is of a sensitive nature, for example health data, would require implementing more stringent measures to comply with the GDPR.

[27] Paul Lambert; *The Data Protection Officer: Profession, Rules, and Role,* Auerbach Publishers, Incorporated, 2016.
[28] *Ibid.*