Data Protection

Understanding the General Data Protection Regulation

ADITI CHATURVEDI
Centre for Internet and Society, India

Designed by **Anisha Baid**

Introduction

As recently as May 27, 2016, the General Data Protection Regulation (REGULATION (EU) 2016/679) (hereinafter referred to as GDPR) was adopted. The Data Protection Directive (1995/46/EC) (hereinafter referred to as DPD) will be replaced by this Regulation. It will come **into force on 25th May 2018** and it is expected that under this Regulation data privacy will be strengthened. Substantive and procedural changes have been introduced and for compliance, **industries and law enforcement agencies will have to adjust the ways in which they have operated thus far.**

History of GDPR

- Universal Declaration of Human Rights 1948 recognizes Right to Privacy.
- OECD Guideline of Privacy and Trans Border Flows of Personal Data passed in 1980
- Guidelines for Regulation of Computerized Personal Data Files adopted by United Nations General Assembly in 1990
- Treaty of Lisbon and Charter of Fundamental Rights (Art 7 & 8)
- Data Protection Directive (1995/46/EC), Directive on E-Privacy (2002/58/EC) and the Directive on Data Retention (2006/24/EC) were adopted
- Adoption of General Data Protection Regulation (REGULATION (EU) 2016/679) in 2016

Key Aspects of GDPR and Changes from DPD

One stop shop

GDPR puts in place a uniform law for EU

Changes

On the other hand, DPD has been an enabling legislation that permits different Members to make different laws resulting in variance in compliance norms in different jurisdictions

Data Subject focused approach (Art 3)

According to Art 3, GDPR will apply irrespective of location of controller or processor subject to the condition that data subject in is EU and processing activity is related to offering of goods or services or monitoring their behaviour within EU.

Changes

I. Art 4 of DPD states that application of DPD depends on recognition of national law by virtue of public international law or requires that processing equipment should to be situated in the Member State.[1]

II. DPD is silent on processors[2].

Rights

Rights retained from DPD have been strengthened and a new right has been introduced.

I. Right to Data Portability (Art 20)

New Right called Right to Data Portability allows portability of data from one controller to another.

Changes

This right is not given in the DPD

II. Right to restrict processing (Art 18)

- Data subject has the right to restrict processing under certain conditions.
- Includes steps like removing published data from website or temporarily moving data to another processing system

Changes

- Art 12(b) DPD allows blocking of data on the grounds of data inaccuracy or incomplete data
- The Right under GDPR is elaborate. It specifies four conditions under which this right can be exercised, the implications of enforcing this right and obligations of the controller. Similar provisions have not been given under the DPD[3].

III. Right to erasure (Art 17)

- It enables the data subject to erase personal data under certain conditions.
- Is also known as the Right to be forgotten

Changes

- As compared to DPD, the GDPR mentions more grounds for enforcing this right.
- Only three grounds are mentioned under Art 12(b) of the DPD for the purpose of exercising this right. These are unlawful processing or incomplete or inaccurate data.
- GDPR lists the conditions under which the right cannot be exercised and obligations of the controller when data has been made public. DPD does not contain such provisions.

---

1 Art 4, Data Protection Directive (1995/46/EC)

2 Art 4, Data Protection Directive (1995/46/EC)

3 Art 12(b), Data Protection Directive (1995/46/EC)

IV. Right to access (Art 15)

- Data subject has the right to access information related to her personal data so that she can be aware of and verify lawfulness of processing.
- GDPR states the obligations of the controller in this regard.

Changes

Under the GDPR the data subject can get access to more information than she could under Art 12 of the DPD.

V. Right to rectification (Art 16)

Data subject has the Right to rectify her personal data.

Changes

Art 12 (b) of the DPD lists conditions under which the right can be exercised; when processing does not comply with provisions of Directive, in particular when data is incomplete or inaccurate.

GDPR on the other hand stipulates incomplete data as the only ground for exercising this right.

VI. Right to be informed (Art 14)

- Requires the controller to provide information to data subject where personal data has not been obtained with consent of data subject.
- Type of information to be provided and exceptions to this right have been listed.

Changes

- GDPR specifies time period within which the information should be provided. Art 10 of DPD does not provide this.
- To ensure fair and transparent processing GDPR obligates the controller to provide "additional information" like storage period of personal data, legitimate interests of controller and third party. These are not given in the DPD[4].

VII. Right to object (Art 21)

Confers the right to object to processing on number of grounds mentioned in the Article

Changes

- Visible shift of burden of proof from data subject to controller: To prevent exercise of this right, the controller will have to demonstrate that compelling legitimate grounds exist for processing. Under Art 14 of the DPD, the onus was on the data subject to demonstrate that compelling legitimate grounds exist that justifies her objection.
- As compared to the DPD[5], the GDPR provides one additional ground for enforcing the right i.e. when data is processed for scientific/historical research/statistical purpose.

4 Art 10, Data Protection Directive (1995/46/EC)

5 Art 14, Data Protection Directive (1995/46/EC)

VIII. Automated individual decision making including profiling (Art 22)

Enables data subject to challenge automated decisions under certain conditions. The aim is to protect data subject from a decision taken without human intervention, and prevent automated privacy harms such as profiling.

Changes

- GDPR excludes child's data and special category data except in case where processing is in public interest or where data subject has give consent. Art 15 of DPD did not stipulate these criteria.
- Controller's obligation with respect to automated individual decision making that are mentioned in the GDPR are absent in the DPD[6].

Consent (Art 4(11), Art 7, Art 8)

- GDPR has brought clarity by including an elaborate definition of consent.
- There can be no assumptions that consent was freely given
- Controller must be able to demonstrate consent (Art 7)
- Consent must be unambiguous, specific and informed (Art 4 (11))
- Examples of a valid consent have been mentioned in Recitals, such as ticking boxes on Internet website includes consent but a pre-ticked box will not (Recital 32)
- Stricter conditions govern child's consent in relation to information society services (Art 8)

Changes

DPD does not contain an elaborate definition of consent. According to the definition mentioned in Art 2(h) of DPD, consent must be informed, specific and informed. No further explanation has been given.

Expanded definition of personal data (Art 4(1))

- Personal data includes "online identifiers" when used in combination with other information, can cause identification of natural persons and their profiling.
- Example of online identifiers includes Internet Protocols, Radio Frequency Identifiers

Changes

The definition of personal data has been expanded under the GDPR keeping in mind the technological changes.

Principles (Art 5)

Data protection compliance is guided by principles of fairness, lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality.

Changes

- Transparency, public interest, data integrity and confidentiality are some of the other terms that have been added to the new Regulation.

6 Art 15, Data Protection Directive (1995/46/EC

- GDPR clearly and specifically states that the controller will be accountable for demonstrating compliance with these principles. Art 6 of DPD called “Principles relating to data quality”, did not mention this.

Security practices

Organisations must be able to demonstrate that they comply with data security principles. Following tools aid in fulfilling the requirement of demonstrating compliance.

I. Privacy by design and default (Art 25)

- Data privacy to be an integral part of project from inception
- Organisation should have appropriate technical and organisational measures such as data minimisation and pseudonymisation

II. Privacy Impact Assessment (Art 35)

- To be carried out where processing is likely to cause high risk to rights and freedoms of natural persons
- Details of PIA have been listed in GDPR

III. Data Protection Officer (Art 37)

- To be appointed in those organisations whose core activity pertains to processing operations that require regular and systemic monitoring of data subjects on a large scale, or large scale processing of special categories of data, or of data relating to criminal convictions and offences.
- DPO to act as the point of contact for the data subject, as well as a supervisory authority in the organization
- DPO may be appointed on contract basis i.e. he may be external to the organization
- Independence of the DPO is essential in performance of his tasks

IV. Breach Notification in 72 hours (Art 33)

- Controller is accountable for reporting data breach to the supervisory authority within 72 hours
- If processor becomes aware of the breach, the same has to be notified to the controller without undue delay
- Art 34 of GDPR also provides for communication of data breach to the data subject when breach is likely to cause high risk to rights and freedoms of natural persons

V. Records of processing activities (Art 30)

- Every controller and processor is required to keep records of all processing activities consisting of details that have been mentioned in Article 30 of the GDPR.

VI. Certificate mechanism and code of conduct (Art 42, Art 40)

- These are voluntary mechanisms. DPD only provided for code of conduct.[7]

7 Art 27, Data Protection Directive (1995/46/EC)

Changes

The requirements listed above have not been stipulated in the DPD

Data transfer (Art 45- Art 50)

- Data transfer between EU and third country or international organisations is governed by adequacy decision of the Commission (Art 45)
- In absence of adequacy decision, data transfer can take place if appropriate safeguards are in place (Art 46)
- Derogations for specific situations have been provided for enabling data transfer when neither adequacy decision not appropriate safeguards is available (Art 49)
- As on 24 November 2016, Andorra, Argentina, Canada (commercial organizations),Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay were recognized by Commission as countries that provide adequate protection.[8]

Changes

- DPD does not mention the term ”international organisations”
- Art 25 of DPD provides for “adequacy decisions” but does not make provisions for “appropriate safeguards”
- GDPR has a separate and detailed provision for Binding Corporate Rules as a tool for data transfer under Art 47. DPD does not mention a similar arrangement.
- Art 48 provides clarification with regard to decisions given by judicial and administrative authorities in third countries with respect to data transfer. DPD does not provide this.
- Art 26 of DPD confers the Member States with power to authorize transfers even when conditions that permit derogations are not met. On the other hand, conditions for derogations have been specified under Art 49 of GDPR and Member States have not been given the option to permit the transfer if these are not complied with.
- The GDPR also allows transfers not only to third countries, but also to a territory or a specified sector within a third country, or to an international organization, provided they have been awarded the Commission’s adequacy designation.

Remedy as a Right

- Data subject has the right to lodge complaints, against unlawful processing, with supervisory authority (Art 77)
- Data subject has the right to judicial remedy against decision of supervisory authority (Art 78)
- Data subject has the right to judicial remedy against controllers and processor due to infringement of Rights because of non compliance of Regulation during processing (Art 79)

8 Commission decisions on the adequacy of the protection of personal data in third countries, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Changes

- Art 28(4) of DPD obliges supervisory authority to hear claims concerning rights and freedoms but did not provide this option by way of "Right"
- DPD does not provide access to effect judicial remedy against supervisory authority
- Though access to effect judicial remedy against controller of processor is not given in the Articles of DPD, Recital 55 clarifies that when controller fails to respect the rights of subjects or fails to obey national legislation the data subject can resort to judicial remedy.

Right to compensation and liability (Art 82)

Person who has suffered from material and non-material damage has the right to receive compensation from controller or processor.

Changes

Art 23 of DPD imposes compensation liability on controllers only.

Administrative fines and Penalties (Art 83 and Art 84)

- Effective, proportionate and dissuasive fines and penalties provided under GDPR
- For infringement of certain provisions fines can be as high as 20 000 000 EUR or 4% of worldwide annual turnover.
- Penalties have been provided for violations that are not subject to administrative fines

Changes

There is no provision for administrative fines and penalties in DPD

Relevant Case Law

Google Spain V. AEPD and Mario Costeja Gonzalez

- ECJ held that Google is a data processor as well as a data aggregator, thus bound by DPD.
- Hence ,Right to be forgotten could be enforced against Google when requested by the data subject.

Maximillian Shrems V. Data protection Commissioner

- ECJ invalidated the Safe Harbour scheme stating that it violated Right to Privacy[9]
- Commission did not have the competence to restrict power of national supervisory authorities[10]
- Petitioner challenged transfer of his Facebook data to servers in USA in the backdrop of PRISM mass surveillance program unveiled by Snowden.

9 Court of Justice of the European Union , Press Release No 117/15 , 6 October 2015 curia.europa.eu/jcms/jcms/P_180250/

10 Court of Justice of the European Union , Press Release No 117/15 , 6 October 2015 curia.europa.eu/jcms/jcms/P_180250/

- This case re-articulated the threshold required for an adequacy decision to that of “essential equivalence.” Recital 104 confirms that an adequacy decision by the European Commission means that the third country or specified entity ensures “an adequate level of protection essentially equivalent to that ensured within the European Union.”

Conclusion

The GDPR has been enacted keeping in mind novel disruptions induced by technological changes, around issues of privacy and ownership of data. In a way, it represents the first comprehensive regulatory framework for data sharing wherein corporations are enjoined with immense responsibilities in the manner they handle and employ consumer data. Preparations for successful implementation are on way. The EU-US Privacy Shield has replaced the Safe Harbour Agreement and Swiss-US Privacy Shield has also been signed. Many more efforts are being made to comply with the new regulations. A contemporary dialogue on data security is gaining momentum.