Centre for Society and Policy
Indian Institute of Science

COMPREHENSIVE REPORT ON THE GENERAL DATA PROTECTION REGULATION (GDPR) - THE REGULATION (EU) 2016/679

By

Rahul Patil

Anjula Gurtoo

26 August 2020

INDIAN INSTITUTE OF SCIENCE

BANGALORE

Table of Contents

Citation: Patil, R. and Gurtoo, A. (2020). Comprehensive Report on the General Data Protection Regulation (GDPR) - The Regulation (EU) 2016/679. IISc CSP Working Paper Series. 2C/08/2020.

General Data Protection Regulation (GDPR)

Introduction:

This contribution covers the provisions of GDPR relevant to the operationalisation of goods and services related to personal data and its management.

The report elaborates on personal data, which is at the core of the Regulation. Further, it has five sections, namely, 1. Respecting Data Subject Rights; 2. Data Ecosystem Stakeholders Respecting Data Subject Rights; 3. Personal Data Management; 4. Judicial Interventions; and 5. Cross-border Data Management. These five sections detail salient provisions carved under relevant GDPR articles and Recitals, which are also cited thereunder along with the case laws.

Under Sect. 1, three primary rights of the data subject are discussed whose personal data will be collected, stored, and transmitted. These rights include the right to access, the right to be forgotten, and the right to be informed. In the Sect. 2, regulatory provisions for the important stakeholders of the data economy such as data protection officer, controller, Processor, and Supervisory authorities are discussed. Sect. 3 enlists the regulatory provisions obligatory for the controllers and processors regarding personal data management practices, whereas penalties due to non-compliance to these obligations are summarised in the following section. It also includes remedies for the stakeholders invoked in adverse circumstances such as personal data breach, objections on controllers, processors, or supervisory authorities. The final section deals with the cross-border data transmission provisions where international trade and cooperation are sought.

Personal data of the Data Subjects are either directly or indirectly collected by the Controllers, processed by Processors, and such proceedings are managed by the Data Protection Officers. They can be an internal employee of the Controller or hired from outside. Overall supervision of the ecosystem and particular Controller is carried out by Independent Supervisory Authority established by the EU Member States. The Controller must communicate with Data Subjects about his/her collection, processing, or transmission of personal data. Data Subject can exercise his rights by requesting the Controller per the provisions prescribed by the Regulation.

The Regulation (EU) 2016/679 (i.e., GDPR) has 99 articles and 173 recitals and applies *to* all the organisations in the EU or outside involved in handling data of Europeans.

Personal Data — Any information related to an identified or identifiable natural person

Data Identifiers: name, identification number, location data, online identifier, physical, physiological, genetic, mental, commercial, cultural, or social identity

GDPR → Only applicable, if personal data is being processed

Once the data is anonymised, it goes outside the purview of GDPR

Here are the major provisions of the General Data Protection Regulation (GDPR) categorised under five sections:

1. *Respecting Data Subject Rights*

Right to Access | Right to be Forgotten | Right to be Informed

2. *Data Ecosystem Stakeholders*

Data Protection Officer | Controller | Processor | Supervisory Authorities

3. *Data Management*

Data Processing | Security of Processing | Records of Processing Operations

4. *Judicial Interventions*

Remedies | Liability | Penalties

5. *Cross-border Data Management*

International Trade and Cooperation

Section 0: *More about personal data concerning GDPR*

Personal Data — Any information related to an identified or identifiable natural person

Reference to GDPR – Articles and Recitals

- *Article 4(1):* Definition of personal data
- *Article 9(1):* Processing of personal data for uniquely identifying a natural person is prohibited
  - Article 9(2h): In purview of public interests, scientific or historical research purposes, or statistical purposes – Processing is necessary
    - An obligation of professional secrecy has to be followed – Article 9(3)
- *Recital 26:* GDPR not applicable to anonymous data
- *Recital 51:* Sensitive personal data protection

Data Identifiers: name, identification number, location data, online identifier, physical, physiological, genetic, mental, commercial, cultural, or social identity

Examples: genetic, biometric, and health data; data for racial and ethnic origin; political, religious, or ideological opinion/convictions; association or trade union membership details, etc.

Sensitive personal data: If the nature of personal data is such that it is sensitive in relation to fundamental rights and freedoms, its processing can create significant risks to the fundamental rights and freedoms.

Explicit consent of the data subject is required along with the special category of data while following the legitimate processing activities

Section 1 *Respecting Data Subject Rights*

(1a) Right to Access

- Importance:
  - 'Right to access' facilitates the right to rectification and erasure
  - An omitted or incomplete disclosure is subject to fines

- Salient Features:
  - Information has to be provided free of charge.
  - Reasonable payment reflecting administrative charges can be sought in case copies are requested.
  - If data subjects' requests seem unjustified or excessive, the Controller might reject the right to access the request
  - Data request needs to be answered without undue delay but within one month and can be extended under reasoned cases
  - Information needs to be given in writing, electronically, or verbally depending on the circumstances.

Reference to GDPR – Articles and Recitals

- *Article 12:* Transparent information, communication, and modalities for the exercise of the rights of the data subject
- *Article 15:* Right of access by the data subject
- *Article 46:* Transfers subject to appropriate safeguards
- *Recital 58:* The Principle of Transparency
- *Recital 63*: Right of Access
- *Recital 64:* Identity Verification
- *Recital 73:* Restrictions of Rights and Principles

If the data subject exercises his/her rights –

That is: If there is a request for data of access by a natural person:

Two stages will be followed:

1. The Controller needs to check whether any personal data of the person seeking information is being processed.
   – It's obligatory to answer either positive or negative
2. If yes, then in the second stage:
   – A whole range of information needs to be provided
   Information: processing purposes; categories of personal data processed; recipients or categories of recipients; planned duration of storage or criteria for their definition; information about the rights of the data subject such as rectification, erasure, or restriction of processing; the right to object; instructions on the right to lodge a complaint with the authorities; information about the origin of the data; existence or application of an automated decision-making process (e.g., profiling, etc.), and information about the data transferred to another country (even if the transfer happened without an adequate level of protection)

(1b) Right to be Forgotten

- Importance:
  - 'Right to be forgotten' regulates erasure obligations.
  - Statutory erasure obligations over Controller

- Salient Features:
  - The Regulation does not prescribe methods to be followed for data erasure in individual cases
  - If the data controller publishes data, he/she should covey the reasonable measures to other data controllers regarding eraser of personal data copies and their replicates.
  - If the sufficient identity of the data subject is not provided, the controller may request additional identity information or otherwise refuse the request to erasure.
  - The Controller must inform to data subject about measures (erasure or refuse to erasure with reasons) taken within a month.
  - The right to forgotten is limited in the cases of conflict with the right of freedom of expression and information, necessary to comply with legal obligations, for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes, or the defence of legal claims

Reference to Case Law –

- *Case Law:* Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)

Reference to GDPR – Articles and Recitals

- *Article 17(2):* Right to erasure ('right to be forgotten')
- *Article 19:* Notification obligation regarding rectification or erasure of personal data or restriction of processing
- *Recital 39:* Principles of Data Processing
- *Recital* 65: Right of Rectification and Erasure
- *Recital* 66: Right to be Forgotten

If data is subject to the right to erasure –

That is the circumstances under which data needs to be deleted or erased:

- Personal data need to be erased immediately if the data are no longer required for original processing purposes
- If the data subject withdraws his/her consent and in the absence of legal ground for the processing of the data
- If the data subject objects and in the absence of legitimate ground for the data processing
- Erasure is required to fulfil a statutory obligation by state authorities
- If the processing of such data is against the law

(1c) Right to be Informed

- Importance:
  - 'Right to be informed' promotes transparency in gathering and using personal data.

- Salient Features:
  - Informing obligations over data controller to subject whose personal data is gathered

Reference to GDPR – Articles and Recitals

- *Article 12:* Transparency in information/communication/modalities for exercising data subject rights
- *Article 13:*Applicable if personal data is directly obtained from the data subject
- *Article 14:* Applicable if personal data is not directly obtained from the data subject

- *Recital 39:* Principles of Data Processing
- *Recital* 58: Principle of Transparency
- *Recital* 59: Procedures for the Exercise of the Rights of the Data Subjects
- *Recital* 60: Information Obligation
- *Recital* 61: Time of Information
- *Recital* 62: Exceptions to the Obligation to Provide Information
- *Recital* 73: Restrictions of Rights and Principles

Enforcement of controller's obligation about right to be informed –

That is: the information that needs to be informed to the data subject includes:

[If the data is directly obtained] – Article 13

- Individual's identity and the contact data of the Data Protection Officer
- Processing purposes and the legal basis
- Any legitimate interests pursued
- List of recipients on transmitting data or about the intentions to transfer of data (maybe to other countries)

[If the data is not directly obtained] – Article 14

- The Controller has to provide the same specification/information as in the case of data being directly obtained.
- The Controller has to additionally convey the details about the source of data and the details of whether the data is available in the public domain.
- It should be informed in writing or electronically.
- Exceptions: no obligation to inform the data subject if – the data gathering and transmission are required by law or with respect to the confidentiality due to professional or statutory secrecy

Section 2 *Data Ecosystem Stakeholders*

(2a) Data Protection Officer

- Importance:
  - 'Data Protection Officer' regulates and monitors data collection, processing, and transmission of personal data within/outside the company
- Salient Features:
  - Appointment of DPO does not depend upon the size of the organisation but on the data processing activities involved.

- Even after monitoring the duties of the DPO, statutory compliance with the data protection regulation is the company's responsibility.
- On the recruitment of the DPO, his/her supervisor must publish & communicate his/her contact data for appointment and contact data to the data protection supervisory authorities
- These obligations are mandatory to the organisations even if the appointment of a DPO is voluntary

Reference to GDPR – Articles and Recitals

- *Article 37:* Designation of the data protection officer
- *Article 38:* Position of the data protection officer
- *Article 39:* Tasks of the data protection officer
- *Article 35:* Data protection impact assessment
- *Recital 97*: Data protection officer
- *Recital 91:* Necessity of a data protection impact assessment

The duties of a Data Protection Officer –

1. Working towards the compliance with all relevant data protection laws
2. Monitoring specific processes, such as data protection impact assessments
3. Increasing employee awareness and training them for data protection
4. Collaborating with the supervisory authorities

(2b) Controller

- Importance:
  - 'Controller' determines the nature, scope, context, and purposes of processing personal data.
  - The Controller is responsible for implementing the technical and organisational measures to ensure/demonstrate data regulation compliance.
  - The Controller is the first point of contact for the data subject.

- Salient Features:
  - A controller might be a natural or legal person; public authority; agency; single body, or joint body
  - In the case of joint controllers, an arrangement may designate a point of contact for data subjects
  - Even in any arrangement of the controller, the data subject may exercise his/her rights against each controller.

Reference to GDPR – Articles and Recitals

- *Article 4(7):* Definition of controller
- *Article 24(1):* Responsibilities of the controller
- *Recital 74:* Responsibility and liability of the controller
- *Article 76 & 77:* Risk assessment and guidelines
- *Recital 79:* Allocation of the responsibilities

Compliance features –

That is: How to demonstrate compliance with the statutory obligations over the controller:

- Adherence to the approved codes of conduct – Prescribed in Article 40
- Adherence to the approved certification mechanisms – Prescribed in Article 42

(2c) Processor

- Importance:
  - 'Processor' is responsible for the processing of personal data on behalf of the controller

- Salient Features:
  - The Controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures for personal data processing to comply with requirement of the regulation.
  - The Controller and Processor are jointly liable for the data processing.

Reference to GDPR – Articles and Recitals

- *Article 4 (8):* Definition of the Processor
- *Article 28:* Processor
- *Article 39:* Tasks of the data protection officer
- *Article 32:* Security of processing
- *Article 33:* Notification of a personal data breach to the supervisory authority
- *Article 34:* Communication of a personal data breach to the data subject
- *Article 35:* Data protection impact assessment
- *Article 36:* Prior consultation
- *Recital 97*: Data protection officer
- *Recital 91:* Necessity of a data protection impact assessment

The guidelines for and duties of a processor –

1. The Processor shall not engage another processor without prior specific or general written authorisation of the controller.
2. The Processor should process the personal data only on the documented instructions from the controller.
3. The Processor shall inform the controller regarding legal requirements before processing data where necessary.
4. Processors should commit themselves to confidentiality.
5. The Processor should undertake all required measures related to the security of processing – Article 32
6. Assist Controller with technical and organisational measures to fulfil controller's obligation – Article 32-36

(2d) (Independent) Supervisory Authorities

- Importance:
  - 'Supervisory Authorities' are responsible for monitoring the application of this Regulation.
  - Such monitoring facilitates the protection of fundamental rights and freedoms of natural persons and the free flow of personal data within the Union.

- Salient Features:
  - Member States may establish one or more independent public authorities as Supervisory authorities.
  - Supervisory Authorities should contribute to the consistent application of the Regulation across the EU.
  - In the case of multiple supervisory authorities, Member State should designate the supervisory authority and establish a compliance mechanism within such authorities.
  - Regulation empowers independence to the supervisory authority in performing tasks and excursing its powers and empowers members to remain free from direct/indirect external influence.
  - Supervisory authority (of the main establishment of the controller/processor) can function as a lead supervisory authority for the cross-border processing carried out by that controller/processor.
  - Members are advised to refrain from any action non-compatible with their duties during the term of office.

Reference to GDPR – Articles and Recitals

- *Article 4(21):* Supervisory authority definition
- *Article 4(22):* supervisory authority concerned

- *Article 51:* Establishing supervisory authorities by the Member States
- *Article 52:* Independence to supervisory authorities
- *Article 60:* Cooperation between the lead supervisory authority and the other supervisory authorities concerned – cross-border data processing of data
- *Chapter 7:* Cooperation and consistencies among supervisory authorities
- *Recital 117:* Establishment of Supervisory Authorities
- *Recital 118*: Monitoring of the Supervisory Authorities
- *Recital 119*: Organisation of Several Supervisory Authorities of a Member State
- *Recital 120*: Features of Supervisory Authorities
- *Recital 121:* Independence of the Supervisory Authorities

General conditions for the members of the supervisory authority –

That is: How do the Members States appoint Members of the supervisory authority?

- Members should be either appointed by the parliament, government, head of State, or an independent body entrusted with the appointment under Member State law
- Members should have qualifications, experience, and skills in the area of protection of personal data
- A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for performing the duties.

Section 3 *Data Management*

(3a) (Commissioned) Data Processing

- Importance:
  - 'Commissioned Data Processing' creates the possibility of uniform processing mechanisms throughout the EU.

- Salient Features:
  - Data processing involves any operation (or their set) which is performed on personal data (either automatically or not), such as collection, recording, organisation, structuring, storage, adaptation/alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
  - Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.
  - Such processing by the Processor is in accordance with the instructions of the controller based on a contract.
  - The Processor has to follow written instruction from the controller that is based on the contract.

- Prior written authorisation by the Controller is required if multiple processors engage with one another.

Reference to GDPR – Articles and Recitals

- *Article 27:* Representatives of controllers or processors not established in the Union
- *Article 28:* Personal data processor
- *Article 29:* Records of processing activities
- *Articles 40 & 42:* Codes of conduct and certification for controllers
- *Articles 44, 45, & 46:* General principle for transfers, adequacy decision & safeguards
- *Article 82:* Right to compensation and liability
- *Recital 24*: Applicable to processors not established in the Union if data subjects within the Union are profiled
- *Recital 98:* Preparation of Codes of Conduct by Organisations and Associations

The controller-processor relationship –

That is: What kind of instructions should be prescribed by the controller to the Processor in the contract?

- The contract should address the type of personal data that will be processed along with the object and purpose of the processing.

That is: What kind of objections are there for the Processor?

- The Processor has to maintain a record of the data processing activities and
- Names and contact of data of controller who he/she is working for.
- Categories of data being processed for respective controllers
- Maintenance of index for the transfer of data to other countries
- Recording description of technical and organisational measures employed.

(3b) Security of Processing

- Importance:
  - Adopting security of processing can be a way of reducing the data breach and the liability of adverse events leading to the penalty
  - It can be employed as a risk management practice at controllers and processors.
- Salient Features:

- The regulations suggest controller and Processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- It seeks controllers and processors to adhere to approved codes of conduct and approved certification mechanisms refereed on the Regulation.
- The Regulation suggests controllers adopt an appropriate level of security account to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the stored or transmitted personal data.
- The Controller and Processor should adopt a mechanism under which no natural person (authority under controller) should be able to process the data except the on the instruction of the controller or Union/State law.

Reference to GDPR – Articles and Recitals

- *Article 6:* Lawfulness of processing
- *Article 38:* Security of processing
- *Article 39:* Communication of a personal data breach to the data subject
- *Articles 40 & 42:* Codes of conduct and certification mechanisms
- *Recital 83*: Security of Processing
- *Recital 98*: Preparation of Codes of Conduct by Organisations and Associations
- *Recital 99*: Consultation of Stakeholders and Data Subjects in the Development of Codes of Conduct
- *Recital 100*: Certification mechanism

The technical and organisational measures –

That is: What kind of technical and organisational measures should the controllers and Processor take to adopt secure data processing?

- Adopting the pseudonymisation and encryption of personal data
- Ensuring confidentiality, integrity, availability, and resilience of processing systems and services
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures

(3c) Records of Processing Operations

- Importance:
  - 'Data Protection Officer' regulates and monitors data collection, processing, and transmission of personal data within/outside the company

- Salient Features:
  - Regulation has obliged the Controllers and Processors to create records of processing activities.
  - Each Processor shall maintain a record of all categories of processing activities carried out on behalf of a controller
  - All such records should be written and accessible in electronic form.
  - Such obligation shall not apply to an enterprise or an organisation employing fewer than 250 persons – unless (a) the processing being carried out poses a risk to the rights and freedoms of data subjects; (b) the processing is not occasional, (c) the processing includes special categories of data or personal data relating to criminal convictions and offences
  - If the organisation involved in processing activities does not provide data to authorities, such organisations are liable to fines as per Article 83(4).

Reference to GDPR – Articles and Recitals

- *Article 5:* Principles relating to the processing of personal data
- *Article 30:* Records of processing activities
- *Article 32:* Security of personal data processing
- *Article 49(1):* Derogations for specific situations
- Article 83(4)(a): Fines for incomplete disclosure to authorities
- *Recital 13:* Taking account of micro, small and medium-sized enterprises
- *Recital 82:* Record of processing activities

The technical and organisational measures –

That is: What kind of technical and organisational measures should be by the controllers and Processor to adopt secure data processing?

- Name and contact details of the controller (or the joint controller), the controller's representative, and the data protection officer
- Purposes of the processing
- Description of the categories of data subjects and the categories of personal data
- Categories of recipients to whom the personal data have been or will be disclosed, including recipients in other countries
- The documentation of suitable safeguards if data is transferred or will be transferred to another country

- Envisaged time limits for erasure of the different categories of data
- General description of the technical and organisational security measures

Section 4: *Judicial Intervention*

(4a) Remedies / Corrective Powers / Liability

- Importance:
  - Various provisions under the Regulation facilitate the judicial remedies, which include:
    - Right to lodge a complaint with a supervisory authority,
    - Right to an effective judicial remedy against a supervisory authority,
    - Right to an effective judicial remedy against a controller or Processor

- Salient Features:
  - A concerned person can seek either judicial remedy against a supervisory authority or a controller/processor
  - Every natural/legal person can seek an effective judicial remedy against a legally binding decision of a supervisory authority
  - The data subject can seek a remedy of competent supervisory authority does not handle a complaint or does not inform the data subject of a progress/outcome within three months
  - Proceeding against a supervisory authority shall be brought before the courts
  - Proceeding against the Controller or Processor can be brought before the court in the Member State of an establishment or where the habitual residence of the data subject.

Reference to GDPR – Articles and Recitals

- *Article 77:* Right to lodge a complaint with a supervisory authority
- *Article 78:* Right to an effective judicial remedy against a supervisory authority
- *Article 79:* Right to an effective judicial remedy against a controller or Processor
- *Recital 141:* Right to Lodge a Complaint
- *Recital 143*: Judicial Remedies
- *Recital 145*: Choice of Venue

General remedies or corrective powers –

That is: What kind of remedies or corrective powers can be suggested before the court in proceedings against the Controller or Processor?

- Order to end a violation,

- an instruction to adjust the data processing to comply with the GDPR, and
- power to impose a temporary or definitive limitation, including a ban on data processing.

(4b) Fines / Penalties

- Importance:
  - Such provisions empower various entities to control the personal data economy –
    - data protection authorities,
    - employee
    - customers or potential customers who complain to the authorities,
    - press (investigative journalism)

- Salient Features:
  - Fines might be applied in addition to /instead of the remedies or corrective powers
  - Such provisions are either directly applicable to the processors or in addition to the controller
  - The fines must be effective, proportionate, and dissuasive for each individual case.
  - Administrative fines are calculated by national authorities are based on various factors
  - Administrative fine: 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the preceding financial year
    - obligations of the controller and the Processor
    - obligations of the certification body
    - obligations of the monitoring body
  - Administrative fine: 20 000 000 EUR or up to 4% of the total worldwide annual turnover of the preceding financial year
    - basic principles for processing, including conditions for consent
    - data subjects' rights
    - transfers of personal data to a recipient to another country
    - obligations pursuant to Member State law
    - non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority

Reference to GDPR – Articles and Recitals

- *Article 58:* Powers
- *Article 70:* Tasks of the Board

- *Article 83:* General conditions for imposing administrative fines
- *Article 84:* Penalties
- *Recital 148*: Penalties
- *Recital 149:* Penalties for Infringements of National Rules
- *Recital 150:* Administrative Fines
- *Recital 151:* Administrative Fines in Denmark and Estonia
- *Recital 152:* Power of Sanction of the Member States

General conditions for imposing administrative fines –

That is: What factors need to be considered when deciding administrative fine or its amount?

- Nature, gravity, and duration of the infringement – considering:
  - nature scope or purpose of the processing;
  - number of data subjects affected; and
  - level of damage suffered by them
- The intentional or negligent character of the infringement
- Action taken by the Controller or Processor to mitigate the damage suffered by data subjects
- Degree of responsibility of the controller or Processor
  - considering account technical and organisational measures implemented
- Any relevant previous infringements by the controller or Processor
- Degree of cooperation with the supervisory authority
  - to remedy/mitigate the possible adverse effects of the infringement
- Categories of personal data affected by the infringement
- The way by which the infringement became known to the supervisory authority
- Whether the same subject matter, compliance with the measures is previously ordered or not
- Adherence to approved codes of conduct and certification mechanisms
- Other aggravating or mitigating factor applicable to the circumstances

Section 5 *Cross-border Data Management*

(5a) International Trade and Cooperation

- Importance:
  - These provisions facilitate the cross-border transmission of personal data by examining the legitimacy of for transfer

- Salient Features:
    - Examination of the legitimacy of data transfer has two stages – 1. Data transfer meets general legal requirements, and 2. Such transfer must be allowed to the third country
    - Secure third countries: Countries confirmed by the EU with a suitable level of data protection on the basis of an adequacy decision
    - Adequacy of the EU-US data protection shield (Privacy Shield) is invalid with immediate effect – as per the ECJ judgment of 16 July 2020

Reference to Case Law –

- *Case Law:* ECJ judgment in 'Schrems II' (case C-311/18) – 16 July 2020 – Immediate invalidation of the data protection shield (US-EP Privacy Shield)

Reference to GDPR – Articles and Recitals

- *Article 44:* General principle for transfers
- *Article 45:* Transfers on the basis of an adequacy decision
- *Article 46:* Transfers subject to appropriate safeguards
- *Article 47:* Binding corporate rules
- *Article 48:* Transfers or disclosures not authorised by Union law
- *Recital 102:* International Agreements for an Appropriate Level of Data Protection
- *Recital 103*: Appropriate Level of Data Protection Based on an Adequacy Decision
- *Recital 104*: Criteria for an Adequacy Decision
- *Recital 105*: Consideration of International Agreements for an Adequacy Decision
- *Recital 111*: Exceptions for Certain Cases of International Transfers
- *Recital 115*: Rules in Third Countries Contrary to the Regulation

General Proceedings for the data transfer to the third country –

That is: Ways under which the data transfer can be permitted to the country without adequate decisions?

- The controller must ensure in another way that the personal data will be sufficiently protected by the recipient
    - Through assurance of standard contractual clauses
    - Adherence to binding corporate rules
    - Commitment of adherence to GDPR codes of conduct
    - Adherence to certification of the data processing procedure