Rights of Data Subject (GDPR) and Data Principal (PDPB)

Personal Data Protection Bill, 2018	General Data Protection Regulation, 2016
Data Principal Rights Chapter VI (Sections 24 to 28) provides a list of rights available to data principals such as right to confirmation and access, correction, data portability etc.	**Rights of Data Subjects** Chapter 3 (Articles 12 to 22) contain right to transparency, access, erasure etc.
	Duties on Data Controllers(Art 12): Information requested by data subject should be given in transparent, concise and easily accessible format by data controller(Art 12(1)) Data controller shall not refuse on data subject requests for rights under Art 15 to 22; and shall respond within one month. Information provided under Art 13, 14 and actions taken under Art 15 to 22 shall be provided free of charge. A reasonable fee can be charged in exceptional circumstances. Art 12(5)
Right to Confirmation and Access(Sec 24) The data prinicipal has the right to obtain from data fiduciary: • Confirmation on whether the personal information of data principal is being processed or has been processed; • A summary of personal data of data prinicipal being processed or has been processed; • A brief summary of processing activities undertaken by data fiduciary on the personal data of data principal, including any information mentioned in notices under Section 8. The above information shall be provided by data fiduciary in easily comprehensible manner for understanding of data principal.	**Right to Information and Access(Art 13):** During collection of personal data, data controller shall provide information relating to: • identity, contact details of controller; • contact details of data protection officer; • purpose of data collection; • recipients of personal data including a third country transfer(if applicable). To ensure fair and transparent processing controller shall also provide following information: • duration of storing personal data; • existence of automated processing and rights available to data subject namely right to erasure, rectification, withdrawal of consent, lodging complaint.
	Right of Access(Art 15): Data subject has right to confirm whether his/her personal data is being processed and if yes, purposes of processing, period of storage, rectification and erasure(if required), complaint mechanism to supervisory authority, existence of automated processing, recipients of personal data and adequate safeguards if personal data is transferred to third countries or international organisations.

Right to Correction, etc(Sec 25) This section provides for correction, completion and updating of personal data of data principal by data fiduciary on request. The data fiduciary may refuse such correction, completion, updating if not deemed necessary, but must provide justification for refusing such correction requests. Neverthess, if data principal is not satisfied by such justification, he/she can get his objection recorded alongside the relevant personal data. On correction, completion or updating of personal data by data fiduciary, it must notify about such changes to all relevant entities or individuals to whom such personal data has been disclosed.	**Right to Rectification(Art 16):** Data subject to have right to rectify inaccurate personal data and incomplete data completed without delay.
Right to be Forgotten(Sec 27) It provides for right of data principle for restricting or preventing further disclosure of personal data by data fiduciary in cases when it has served the purpose for its collection or when consent is withdrawn by data principal or when such disclosure violated law of land. This right can only be exercised when the Adjudicating Officer (AO) (u/s 68) is satisfied with applicability of above-mentioned conditions and when rights of data principal override freedom of speech and expression of other citizens. There are a list of considerations which the AO must note while deciding applicability such as sensitivity of personal data, its relevance to public, scale of disclosure etc. The section also provides for filing a review when any person finds that AO has restricted disclosure without satisfying the conditions in Sec 27(2).	**Right to Erasure/Right to be Forgotten(Art 17):** Data controller shall erase personal data in any of the following events: • purpose for collection served, • unlawful processing, • withdrawal of consent by data subject, • objection of data subject under Art 21(1)- Right to Object. Controller shall take reasonable steps to erase personal data with other controllers having a copy or replication, or when its in public domain. Exceptions: Right to freedom of expression and information; public interest(public health); scientific or historical or statistical purposes; legal compliance. **Right to Restriction of Processing(Art 18):** Data subject has right to restrict controller from processing data in following events: personal data is inaccurate (according to data subject), unlawful processing, purpose served (but storage is required for legal claims), data subject exercises his/her right to object under Art 21(1). **Notification Obligation(Art 19)** Data controller shall inform all recipients of

	personal data (including other controllers) in event of rectification or erasure or processing restriction being exercised under Arts 16, 17, 18 respectively.
Right to Data Portability(Sec 26) The data principal has the right to receive personal data which he/she has given to the data fiduciary or which is generated during provision of services/goods by data fiduciary or which forms part of data principal's profile or is otherwise obtained by data fiduciary. Such personal data should be provided in a structured, commonly used and machine-readable format. This is done to allow easy portability of data between service providers. However, this section applies only when processing has been done through automated means. Also, data cannot be revealed under this provision if it's processed u/s 13, 14 or when it's technically not feasible or when a trade secret of fiduciary could be revealed.	**Right to Data Portability(Art 20):** Data subject has right to receive personal data from controller in structured, machine-readable format and get it transmitted to another controller. It's exercised only when data is received on consent of data subject and processing is carried by automated means. Exceptions: Right to Erasure(Art 17), Rights and Freedoms of Others.
No such provision	**Right to Object(Art 21):** Data subject has right to object processing of his/her personal data including profiling by controller on grounds relating to his/her personal situation or when it's processed for direct marketing purposes. Exceptions: Existence of 'compelling legitimate grounds' that override rights and freedoms of data subject; legal claims; public interest(scientific or historical research). **Automated Individual Decision-Making, Including Profiling(Art 22):** The data subject shall have right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects him/her. **Restrictions(Exceptions) (Art 23):** Exercise of data subject rights are restricted, while ensuring essence of fundamental rights and freedoms and only proportionate to democratic society, to safeguard: • national security, defence, public security; • law enforcement/investigation/prosecution; • general public interest(public health, social security, monetary matters); • judicial proceedings;

	• protection of rights of other data subjects etc.

Penalties, Fines and Remedies

Personal Data Protection Bill, 2018	General Data Protection Regulation, 2016
Chapter XI of the Bill provides for a gradation of penalties on data fiduciaries.	Chapter VIII provides for Remedies, Liability and Penalties
Grievance Redressal(Sec 39): A data principal, on encountering violation of this Bill, can first raise issue with respective Data Protection Officer(DPO). However, if no proper action is taken, a complaint can be filed to Adjudicating Officer.	**Right to Lodge a Complaint (Art 77):** The data subject has right to lodge complaint to Supervisory Authority; and be updated on its progress, outcome.
Appellate Tribunal(Chapter XII of the Act) Section 79 provides for establishment of an Appellate Tribunal to hear and dispose of any appeal from orders of Adjuticating Officers or the Data Protection Authority of India(DPAI). It has the powers similar to the civil court under Code of Civil Procedure, 1908. The appeal against the order of shall lie before the Supreme Court of India.	**Right to an Effective Judicial Remedy Against a Supervisory Authority(Art 78):** Each person has right to an effective judicial remedy against decision of a supervisory authority. Each data subject has right to judicial remedy where the supervisory authority does not handle a complaint or does not inform on its progress or outcome within 3 months. Proceedings against a supervisory authority shall be brought before the courts of the respective Member State. **Right to an Effective Judicial Remedy Against a Controller or Processor(Art 79):** Each data subject has right of judicial remedy against controller or processor, if his/her rights are infringed because of processing of his/her personal data in non-compliance with GDPR.
No such provision	**Representation of Data Subjects(Art 80):** Any non-profit, organisation or association can represent data subjects in lodging complaint, seeking judicial remedy and receiving compensation on his/her behalf.
Adjudication by Adjudicating Officer(Art 74): A penalty can only be imposed after conduction of inquiry by Adjudicating Officer.	**'General Conditions for Imposing Administrative Fines' Art 83** Each supervisory authority can impose administrative fines for infringements by controller or processor mentioned in Art 58(2) viz. infringing

During such inquiry, the AO has power to summon and enforce attendance of any concerned person; besides data processor or fiduciary must be given opportunity of being heard. While imposing penalty, AO must consider following factors: nature, gravity and duration of violation; intentional or negligent character; mitigating steps taken by controller or processor; previous infringements etc.	provisions of GDPR, non-compliance with exercise of data subject rights, communicating personal data breach to subject, rectification or erasure, withdrawing certification if requirements not met, suspension of data flows to third country. While deciding on imposition of fine and its amount, following points should be considered: nature, gravity and duration of infringement; intentional or negligent character; mitigating steps taken by controller or processor; previous infringements etc.
Offences(Chapter XIII of the PDPB) This chapter provides for list of offences and consequent punishments related to this Act. Investigation of these offences shall be conducted under the Code of Criminal Procedure, 1973(Cr.P.C.) and they shall be cognizable and non-bailable. These include: • Obtaining, transferring or selling of personal data contrary to the Act; • Obtaining, transferring or selling of sensitive personal data contrary to the Act; • Re-identification and processing of de-identified personal data. • It provides for special procedures to deal with offences by Companies, Central or State Governments.	**Penalties(Art 84):** Member States shall lay down the rules on penalties for infringements especially for those no administrative fines are imposed in Art 83. Such penalties shall be effective, proportionate and dissuasive.
Compensation(Sec 75): Any data principal who has suffered harm due to violation of this Bill by data fiduciary or processor shall be liable for compensation. While imposing penalty, AO must consider following factors: nature, duration of violation; intentional or negligent character; harm caused; mitigating steps taken by controller or processor etc.	**Right to Compensation and Liability(Art 82):** Any person who has suffered material or non-material damage as a result of an infringement of GDPR shall have the right to receive compensation from the controller or processor for the damage suffered.
Penalties(Sec 69-73): • 5 crore rupees or 2% worldwide turnover for not complying to obligations under the Act such as responding to data security breach, undertaking data audits etc.;	**Administrative Fines:** Fines upto 10,000,000 EUR or 2% worldwide annual previous year turnover (whichever is higher) can be imposed in violation of following provisions: • Obligations of controller or processor under Arts 8(child's consent), 11(processing

• 15 crore rupees or 4% worldwide turnover for violating obligations given in Chapters II to V; • Upto 10 lakhs on failure to comply with data principal requests under Chapter VI; • Upto 20 lakhs on failure to furnish report, returns, information, etc.; • Upto 2 crores on failure to comply with direction or order issued by the Authority; • Besides, any data principal who has suffered harm due to violation of any provision by data processor or data fiduciary, has right to seek compensation.	without requirement of identification), Art 25-39(provisions related to general obligations, personal data security, data protection impact assessment, data protection officer); • Obligations of certification body(Art 42, 43); • Obligations of monitoring body(Art 41(4)). Fines upto 20,000,000 EUR or 4% worldwide annual previous year turnover(whichever is higher) can be imposed in following violations: • Basic principles for processing, including conditions for consent (Arts 5-7, 9); • Data subjects' rights (Arts 12 to 22); • International personal data transfers in violation of Arts 44-49; • Obligations to member state laws adopted under Chapter IX (specific processing situations eg. employment, official documents etc); • Non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority under Art 58(powers of supervisory authority).

Authorities, Bodies Setup Under PDPB, 2018 and GDPR

Personal Data Protection Bill, 2018	General Data Protection Regulation, 2016
Data Protection Authority Of India(DPAI) (Chapter X of the Bill) Section 49 provides for establishment of DPAI by Central government.	**Supervisory Authorities** Chapter VI provides for setting up Supervisory Authorities and their independence, conditions of service, competence, tasks, powers etc. **Supervisory Authority(Art 51):** Each Member State shall provide for one or more independent public authorities for implementing the GDPR, protect rights and freedoms of natural persons and facilitate free flow of data within the Union.
Appointment(Sec 50): It shall have 1 chairperson and 6 whole-time members. They are appointed by a 3 member committee comprising of: Chief Justice of India or any SC judge of the Supreme Court, the Cabinet Secretary and one expert in field of data protection, IT, cyber and internet laws etc. They must be persons of ability, integrity and have at-least 10 years of relevant professional experience. Removal(Sec 52) It provides for their removal on grounds such as insolvency, physical or mental incapacity, moral turpitude, public interest and conflict of interest.	**Appointment of Members(Art 53):** States should appoint Members of Authority by a transparent procedure by parliament or government or Head of State or independent body entrusted for appointment. Removal It also provides for necessary qualifications and removal in cases of serious misconduct, incapacity.
Independence(Sec 51): It ensures their independence which includes tenure of 5 years or 65 years age and protection of salaries, allowances. To ensure integrity, they cannot hold government office or appointment with data fiduciary until 2 years after holding office.	**Independence(Art 52):** It ensures complete independence to supervisory authority and freedom from external influence(direct or indirect). It mandates Member States to provide authority with human, technical and financial resources for effective performance of its tasks; financial autonomy; and independence in appointing its staff, other administrative functions.
	Rules on the Establishment of the Supervisory Authority(Art 54): Each Member State shall provide law for: establishment of supervisory authority; member

	qualifications; procedure for appointment; term; conditions of service. The members and staff of supervisory authority shall ensure professional secrecy with regard to confidential information in course of their service. **Competence of Lead Supervisory Authority(Art 56):** These include: cross-border processing, handling complaints on possible infringement of GDPR etc. *Lead Supervisory Authority: 'A controller or processor that has operations in multiple countries can choose to appoint a single Supervisory Authority (SA) as their LSA. Once appointed, the LSA becomes the primary contact for GDPR compliance matters like registration of a Data Protection Officer, data breach notifications, etc.' [Ref: https://advisera.com/eugdpracademy/what-is-eugdpr/]
	Tasks of Supervisory Authority(Art 57): Each supervisory authority in its territory shall undertake following tasks: • Monitor and enforce GDPR; • Promote awareness on risks, obligations, safeguards on processing to data subjects, controllers, processors; • Advise public authorities on measures for data protection; • Handle complaints and investigate within reasonable period; encourage Codes Of Conduct and Data Protection Certifications; • Maintain list of Data Protection Impact Assessments etc. Performance of these tasks shall be free but reasonable fee may be charged in requests are unfounded, repetitive.

Powers of DPAI: Sections of 60 to 66 gives DPAI wide powers and functions to ensure enforcement of the Act. These include: • Monitoring and enforcement of the Act, taking prompt action of data security breach, examining data audit reports of data fiduciaries, monitoring data transfers outside country, awareness generation, conducting inquiries on data fiduciaries {with powers same as that of a civil court under CPC, 1908(Sec 60)}; • Issuing 'Codes Of Practice' to promote good practices and facilitate compliance under this Act(Sec 61); • Issuing directions to data fiduciaries and data processors, and ensuring their compliance(Sec 62), calling for information from data fiduciaries or data processors(Sec 63); • Power to conduct inquiry U/s 64 where Authority reasonably believes that activities of data fiduciary or data processor are detrimental to interest of data principals or where the former has violated provisions of this Act. • Pursuant to the inquiry, the Authority can take actions like issuing warnings, mandating business modification, suspending or cancelling any registration etc. (Sec 65); • Conducting search and seizure(Sec 66); • Section 68 provides for a separate Adjudication Wing with designated officers for purpose of conducting inquiries, imposing penalties.	**Powers of Supervisory Authority(Art 58):** Investigative Powers: • Taking information (including personal data) from controller or processor for performance of its tasks; • Data protection audits; • Reviewing certifications; • Notify controller or processor of an alleged infringement; • Accessing premises of controller or processor in accordance of procedural law of land. Corrective Powers: • Issuing warnings to controller or processor on likely infringement of GDPR; • Issuing reprimands on infringement; • Order controller or processor to comply with data subject's request to exercise his/her rights; • Ordering compliance with GDPR provisions; • Imposing temporary or definitive limitation including ban on processing; • Withdrawing certification; • Suspension of data flows to recipient of third country. Authorisation and Advisory Powers: • Advise controller on prior consultation(Art 36); • Advising national parliament, government or other bodies on protection of personal data; • Issue opinion and approve draft codes of conduct(Art 40); • Accredit certification authorities(Art 43); • Adopt standard data protection clauses and binding corporate rules(for third country transfers). The exercises of Supervisory Authority's powers shall be subject to appropriate safeguards including effective judicial remedy and due process.
	Other Obligations of Supervisory Authorities: Cooperation and Consistency Chapter 7 provides for cooperation, mutual assistance, consistency across supervisory authorities in the EU.

	Cooperation Between the Lead Supervisory Authority(LSA) and the other Supervisory Authorities(SA) Concerned(Art 60) It provides that LSA and other SA(s) should aim at reaching consensus and exchange relevant information. <u>Mutual Assistance(Art 61):</u> Supervisory authorities shall provide each other with relevant information and mutual assistance for consistent implementation of GDPR. <u>Joint Operations of Supervisory Authorities(Art 62):</u> It provides for joint operations between supervisory authorities including joint investigations and joint enforcement measures especially when controller or processor has establishments in several Member States. <u>Consistency Mechanism(Art 63):</u> The supervisory authorities shall cooperate with each other and, where relevant, with the Commission for consistent application of GDPR. <u>Urgency Procedure(Art 66):</u> In exceptional circumstances and in order to protect rights and freedoms of data subjects, the concerned supervisory authority may bypass consistency mechanisms referred to in Arts 63, 64 and 65 and immediately adopt provisional measures intended to produce legal effects. These shall be valid for 3 months.
	<u>European Data Protection Board (Art 68)</u> Its established as body of European Union and would be represented by its Chairperson. **<u>Composition:</u>** Head of one supervisory authority of each Member State and European Data Protection Supervisor(but with limited voting rights) or their respective representatives. **<u>Independence(Art 69):</u>** The Board shall act independent in performance of its tasks and not take instruction from anybody. **<u>Procedure(Art 72):</u>** Decision in Board shall be taken by simple majority and adopt its own rules and procedure by simple majority. **<u>Chair(Art 73):</u>** The Board shall elect a chair and two deputy chairs from amongst its members by simple majority. Their term shall be 5 years and renewable.

	Tasks of Chair(Art 74): These include: convening Board meetings, preparing agenda, notify decisions, timely performance of its tasks. **Tasks of Board(Art 70):** To ensure consistent application of GDPR, the Board shall undertake following tasks: • Monitor correct application of Art 64(providing opinions) and Art 65(dispute resolution) functions; • Advise Commission on protection of personal data, proposed amendments, binding corporate rules, certification requirements(Art 43(8)), adequacy test of third country or international organisation for data transfers; • Issue guidelines, recommendations, best practices on erasing personal data from public view(Art 17(2)), profiling criteria(Art 22(2)), personal data breaches (Art 33); • Promote common training programmes for supervisory authorities, exchange of best practices etc. **Opinion of the Board(Art 64):** The Board shall issue an opinion where a competent Supervisory Authority intends to adopt any of the following measures: • Listing processing operations for which data protection impact assessment is necessary; • Compliance of Draft Code Of Conduct with the Regulation; • Criteria of accreditation of certification body etc. • On request of Supervisory Authority or Commission or Chair of Board, the Board may give opinion on any general matter concerning Member State(s). **Dispute Resolution by the Board(Art 65):** To ensure consistent application of Regulation, the Board shall adopt binding decision in following matters: • Conflict between Lead Supervisory Authority and other Supervisory Authorities under Art 60(4); • Conflicting views on Supervisory Authorities' competence etc. The decision shall be adopted in one month by 2/3rd majority of Board.

Exemptions

Personal Data Protection Bill, 2018	General Data Protection Regulation, 2016
Chapter IX of the Bill exempts application of certain data protection safeguards for specific purposes.	Chapter IX of GDPR provides for 'Provisions Relating to Specific Processing Situations'.
The below mentioned data protections would not be applicable, if data is processed for: • Security of State(Sec 42); • Prevention, Detection, Investigation And Prosecution Of Contraventions Of Law(Sec 43); • Domestic Purposes i.e. non-commercial or undisclosed to public(Sec 46); • Journalistic purposes(Sec 47). Exemptions: • Ch II: Data Protection Obligations(Except Sec 4), • Ch III: Grounds For Processing Of Personal Data, • Ch IV: Grounds For Processing Of Sensitive Personal Data, • Ch V: Personal And Sensitive Personal Data Of Children, • Ch VI: Data Principal Rights, • Ch VII: Transparency And Accountability Measures(Except Sec 31), • Ch VIII: Transfer Of Personal Data Outside India Other Exemptions: • Compliance to Ch II to VII(except Sec 4, 31) are exempted for purpose of Legal Proceedings or by any Court or Tribunal(Sec 44). • Certain provisions may be exempted(except Sec 4, 31, 33) for Research, Archiving Or Statistical Purposes(Sec 45). • U/s 48, compliance of few other provisions is also exempted for manual processing by small entities.	**Journalistic, academic, artistic or literary purposes(Art 85):** It provides for reconciling(by law) right to protection of personal data with right to freedom of expression and information of general public. Based on necessity following provisions are exempted for above-mentioned purposes: • Chapter II (principles) • Chapter III (rights of the data subject) • Chapter IV (controller and processor) • Chapter V (transfer of personal data to third countries or international organisations) • Chapter VI (independent supervisory authorities) • Chapter VII (cooperation and consistency) and • Chapter IX (specific data processing situations) **Processing and Public Access to Official Documents(Art 86):** Allows disclosure, public access of official documents with public body, or with private body (for task carried out in public interest). **Processing of the National Identification Number(Art 87):** The National Identification Number or any other identifier can be processed only with safeguards for rights and freedoms of data subjects. Specific law may be made for the purpose. **Processing in the Context of Employment(Art 88):** Member States by law may provide for protection of rights and freedoms in processing of employees' personal data including for purposes of recruitment, work management, health and safety etc. Special safeguards must be given to data subject's dignity, fundamental rights, transparency of processing etc.

	Processing for Archiving Purposes in the Public Interest, **Scientific or Historical Research Purposes or Statistical Purpose(Art 89):** Provides for appropriate safeguards under GDPR and rights and freedoms of the data subject; besides measures like data minimisation, pseudonymisation, purpose limitation are also mentioned. Exemptions: • For scientific or historical research or statistical purposes: Art 15(Right to Access), Art 16(Rectification), Art 18(Restriction of Processing) and Art 21 (Right to Object). • For archival purposes in public interest: Art 15(Right to Access), Art 16(Rectification), Art 18(Restriction of Processing), Art 19(Notification Obligation), Art 20(Data Portability) and Art 21 (Right to Object).

Cross-border Transfer of Data

Personal Data Protection Bill, 2018	General Data Protection Regulation, 2016
Transfer Of Personal Data Outside India (Chapter VIII of the Act)	**Transfers Of Personal Data To Third Countries Or International Organisations** Chapter 5 provides for binding corporate rules, authorisation, safeguards etc to personal data of EU data subjects transferred to third countries or organisations.
S. 40 imposes restrictions on cross-border transfer of personal data. A copy personal data must be kept at a server or data centre in India. Besides, critical personal data, as determined by Central Government, shall only be processed in India. However, certain categories of personal data may be exempted from localisation requirement.	**General Principle for Transfers(Art 43):** Any personal data transferred to third country or international organisation for processing shall take place only if conditions in this chapter are complied and protections guaranteed by GDPR are not undermined.
Data Transfers with Permission of Government Under, S. 41, data besides one mentioned in S. 40 may be transferred outside India but after meeting certain conditions like consent of data principal or under contractual obligations/intra-group schemes prescribed the Authority or countries/sectors prescribed by Central Government with concurrence of the Authority or in a situation of necessity. Central government while permitting data transfer must ensure that it's subject to adequate level of protection such as applicable laws and international agreements; law enforcement. However, the transfer may be permitted without above conditions in case of health and emergency services, or where transfer is necessary for data fiduciaries or data principals and it doesn't hamper effective enforcement of the Act. While prescribing contractual obligations/intra-group schemes, the Authority must ensure adequate level of data protection for data transferred. In such cases data fiduciary must certify that it adheres to the contractual obligations and shall be liable	**Transfers on Basis of an Adequacy Decision(Art 45):** Transfer of personal data to third country or international organisation may be allowed if Commission has decided that such country or organisation has adequate level of protection. No specific authorisation shall be required for such transfers. While determining adequacy, following factors must be considered: • Rule of law, human rights and fundamental freedoms, relevant legislation on national security, criminal law and importantly data protection; • Enforceable data subject rights and judicial redressal; • Effective, independent Supervisory Authorities to ensure compliance with data protection rules; • International commitments for data protection. Such transfer permission may be subsequently repealed if third country dilutes adequate data protection. **Transfers Subject to Appropriate Safeguards(Art 46):** In absence of a decision by Commission under Art

for non-compliance.	46 for foreign data transfers, a controller or processor may transfer data to third country if appropriate safeguards, enforceable data subject rights and effective legal remedies are available. These safeguards may be provided by legally binding and enforceable instruments; binding corporate rules; acceptance of Code of Conduct(Art 40), Certification(Art 42) by controller or processor in third country. **Binding Corporate Rules(Art 47):** These are legally binding and apply to every undertaking, enterprise engaged in joint economic activity including their employees. These are approved by supervisory authorities. These must expressly confer enforceable rights on data subject and specify data transfers and purpose(to third country); their legally binding nature; application of data protection principles such as purpose limitation, data minimisation, storage limitation etc; mechanisms to ensure compliance; complaint procedure etc. **Transfers or Disclosures Not Authorised by Union Law(Art 48):** Any judgement or administrative order of third country for disclosure of personal data shall be only under the international agreement(MLAT). **Derogations for Specific Situations(Art 49):** In absence of adequacy decision under Art 45 or appropriate safeguards under Art 46, personal data can be transferred to a third country only if: • Consent of data subject after being informed of risks involved; or its necessary for performance of a contract; or • Public interest; or • Legal claims; or • Compelling legitimate interests of controller not overridden by rights and freedoms of data subject (Controller must explain the compelling legitimate interests involved) etc. **International Cooperation for the Protection of Personal Data(Art 50):** Commission and supervisory authorities shall take appropriate steps to develop international

	cooperation mechanisms on data protection; international mutual assistance on data exchange etc.