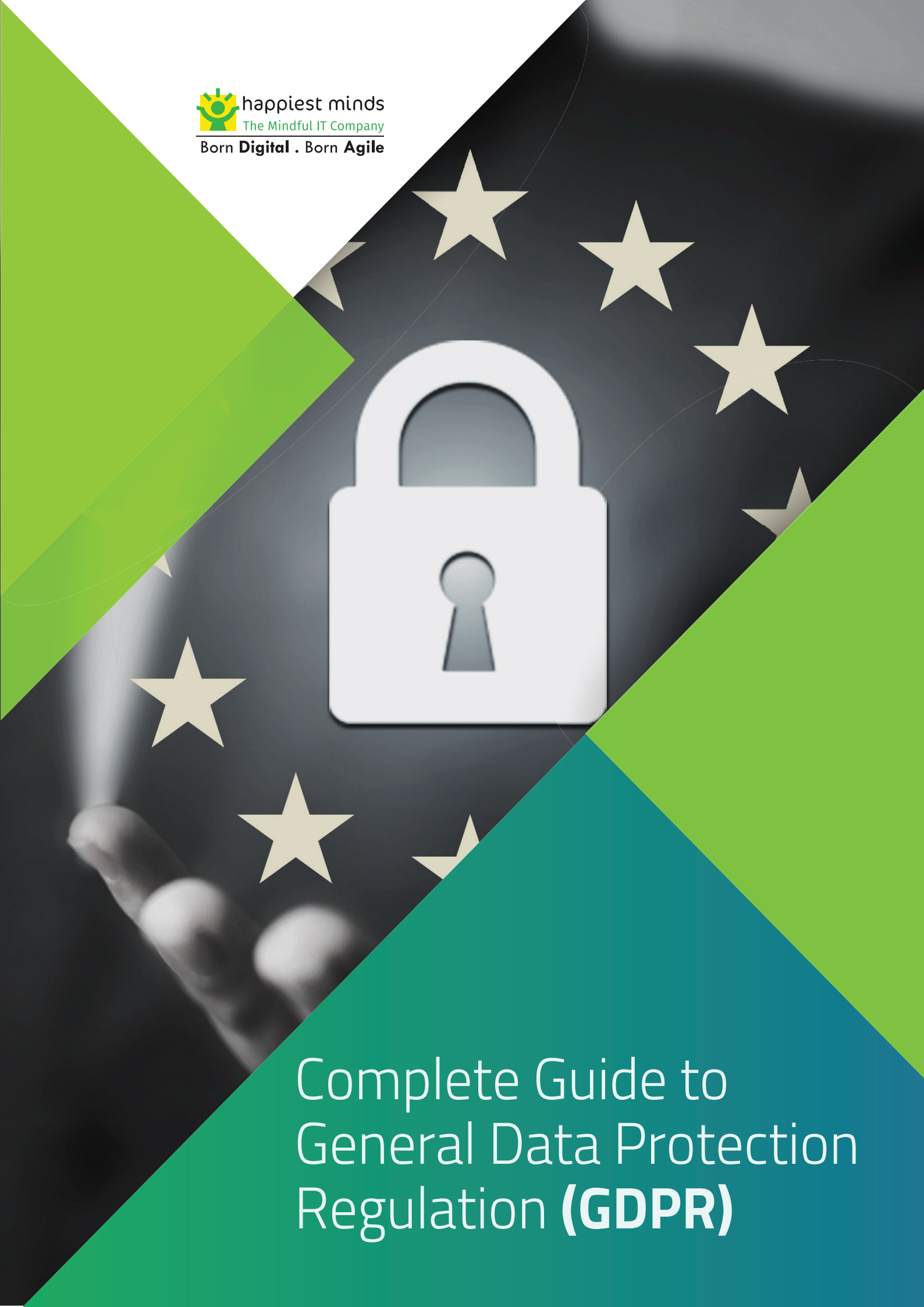
happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**



Complete Guide to General Data Protection Regulation **(GDPR)**

Over the past few year's technologies have transformed us beyond our imagination; Data has played a significant role in this transformation. Data is considered the new gold, and most businesses depend on these data for various business functions. There are many instances where this data has been misused and has affected individuals and business operations.

European government in 2016 adopted **General Data Protection Regulation (GDPR)** and was put into effect on May 25, 2018, replacing the 1995's **Data Protection** Directive to protect the personal information of EU citizens. GDPR aims to govern personal data processing and ensure processing is fair and lawful. It is also designed to emphasize the fundamental right to privacy.

THE DIRECTIVE AND COMPLIANCE OF GDPR

- protect the fundamental rights and freedoms of the persons concerned
- enabling the free flow of personal data across the EU
- contribute to economic, social, and commercial progress
- address the processing of personal data in the light of technological advancements
- harmonize data protection laws within the EU

In theory, the more harmonized approach under the GDPR increases the ability of organizations to do business across the EU, with fewer inconsistent national compliance requirements. The GDPR will thereby provide greater legal certainty for organizations.

GDPR DEFINITION

Personal Data - "Personal Data" means any information relating to an identified or identifiable individual directly or indirectly concerning an identification number or to a factor or factors specific to its physical, physiological, mental, economic, cultural, or social identity.

Sensitive Personal Data - "Sensitive Personal Data" are personal data that disclose racial or ethnic origin, political views, religious or philosophical beliefs, union membership, and data concerning health or sex life. This kind of data will be subject to additional protection and restrictions.

Data relating to criminal offenses and Anonymous data - GDPR doesn't change the way it is processed already. GDPR doesn't apply to anonymous data.

Pseudonymous data - GDPR explicitly encourages organizations to consider pseudonymizing as a security measure.

Controller - "Controller" means the natural or legal person, public authority, or any other body that, alone or together with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU.

Data Breach - "Data Breach" means security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized access to personal data transmitted, stored, or otherwise processed.

Health-related data - Physical and mental health-related personal data relating to an individual's physical or mental health, providing health care services, which reveal information about his or her health status.

GDPR PRINCIPLES

According to Article 5.1-2 of GDPR Act you must follow seven protection and accountability principles if you process data

Fair, lawful, and transparent processing – You need to communicate what the individual data is used and processed.

Purpose limitation principle - Personal data may only be collected for specified, explicit and legitimate purposes. States are responsible for implementing safeguards if data is processed than for what was collected.

Data minimization - Personal data must be adequate, relevant and not excessive with the purposes for which those data are collected and/or further processed.

Accuracy - personal data collected must be accurate and up to date. Inaccurate data must be identified at the early stage to ensure it is erased or rectified without delay.

Data retention periods - Personal data must be store for as long as necessary for the specified purpose. In some cases may be stored for more extended periods as the data will be processed solely for archiving purposes in the public interest, scientific, historical, or statistical purposes, according to Art.89(1), subject to the implementation of appropriate safeguards.

Data security - Data must be implemented with appropriate security with a view of both technical and organizational measures. Ensure no unauthorized access or unlawful processing, accidental loss, destruction or damage is caused.

Accountability - The Controller must demonstrate that its processing activities are compliant with the Data Protection Principles.

GDPR APPLICABILITY

GDPR is applicable to those organizations who process the personal data of EU citizens or residents even if you're not in EU.

The following processing is outside the scope of the GDPR:

- Any activity not falling within the scope of EU law (for example, the activities of a Member State in connection with national criminal law)
- Any activity carried on by the Member States with activities covered by the standard foreign and security policy of the EU
- Any activity performed by a natural person during a purely personal or household activity
- Any processing carried out by the EU itself or any activity carried out by national authorities with a view to prevention, investigation, detection, or process

GDPR – LAWFUL BASIS

Under EU Data Protection Law, for all processing of personal data (unless an exemption or derogation applies) there must be a lawful basis. The basis will depend on the purpose and relation with the individual.

Consent - Personal data may be processed based on an individual providing clear consent to process his/her data for a specific purpose.

Contractual necessity - Processing is permitted if they must enter a contract with the individual or take steps at their request before entering a contract.

Compliance with legal obligations - Personal data may be processed because the Controller has a comply with the law to perform such processing.

Data related criminal offences - Restrictions on the processing of personal data relating to criminal offences or convictions and issues relating to the application of civil law do not materially change.

Protecting sensitive personal Data - Explicit consent, Employment Law or laws relating to social security, vital Interests, charity bodies, data manifestly made public by the data subject, legal claims, public interest, medical diagnosis and treatment, public health, historical/scientific/statistical purposes, exemptions under the law.

Processing for new purposes - Notwithstanding the "data minimization principle ", there are certain circumstances in which personal data can be processed for new purposes which go beyond the original purpose for which the data was collected.

Processing not requiring identification - In case the purposes for which the Controller processes the personal data do not require the identification of the data subject, the Controller is under no obligation to retain information identifying the data subject to comply with the GDPR

GDPR – TRANSPARENCY

The technological complexity of practice makes it hard for individuals to understand whether by whom and for what purpose personal data belonging to him or her being collected. So, to make the data subject concise, easily accessible, and easy to understand following points need to be followed:

Transparent communication - EU Data Protection law obliges controllers to communicate transparently and ensures fair handling of personal information.

Rights of data subjects - Controllers have a legal obligation to affect the rights of data subjects.

Identifying data subjects - The GDPR explicitly enables controllers to ask data subjects to verify their identity before granting rights.

Timeline for complying with the rights of data subjects - The influx of specified time limits under the GDPR results in more stringent compliance obligations for Controllers.

Right to basic information - Organizations remain obliged to provide basic information to individuals to ensure fair and transparent processing of personal data.

Right of access - Data subjects have the right to obtain the following:

01 confirmation of whether and where the Controller is processing their data

02 information about the purposes of the processing

03 information about the categories of data being processed

04 information about the categories of recipients with whom the data may be shared

05 information about data storage (or the criteria used to determine that period)

06 information about the existence of the rights to erasure, rectification, restriction of processing, and to object to processing

07 information about the existence of the right to complain to the DPA

08 where the data were not collected from the data subject, information as to the source of the data

09 information about the existence and an explanation of the logic involved in any automated processing that significantly affects data subjects

Fees in respect of access requests - To prevent data subjects from making annoying requests, data controllers can charge a small fee for each such request.

Right of rectification - The Controller must ensure that no inaccurate or incomplete information is stored. Either they must erase or rectify them. Individuals have all the right to rectification of inaccurate personal data.

Right to deletion (the "right to be forgotten") - Individuals have the right to request the Controller to delete their data such that continuing the processing of those data will not be justified. Notifying the third parties regarding the rectification/deletion/restriction of the data.

Right to data portability - the new right to transfer personal data between those responsible for the processing creates a significant additional burden, necessitating substantial investments in new systems and processes.

Right to object to processing - The GDPR reverses the burden and requires the organization to exhibit whether it has compelling grounds for continuing the processing or that the processing is necessary for connection with its legal rights.

Right to object to processing for use in direct marketing- Individuals have full rights to direct marketing under ePrivacy. Right to object to processing for science, history, or statistics.

Obligation to inform individuals of the right to object - Controllers are compelled to provide additional information to individuals.

Right not to be assessed based on automated processing - Data subjects shall have the right not to be subject to decisions based entirely on automated data processing for personal evaluation purposes. Such processing is allowed where:

01 it is necessary to enter or make a contract with the data subject provided that adequate protective measures are in place

02 it is authorized by law the data subject has explicitly consented, and appropriate safeguards are in place

GDPR – OBLIGATIONS OF CONTROLLERS

The first requirement is that the Controller takes care of the security of the personal data it processes. DPAs are only able to take appropriate enforcement action if they are aware of those breaches.

Controller - "Controller" is an entity that, alone or jointly with others, determines how and why personal data are processed.

Accountability - The Controller is responsible for and must demonstrate compliance with the Data Protection Principles.

Responsibility of Controllers - Where an organization acts as a Controller, it is responsible for ensuring that its processing activities are lawful.

Protecting the Data by design and by default - Controllers must ensure proper data protection principles and appropriate security are followed during the planning phase of activities processing and the implementation phase of new products/services.

Joint Controllers - Where two or more controllers jointly determine the purposes and means of personal processing data, they are joint controllers.

Liability of Joint Controllers - Each joint Controller, is liable for the entirety of the damage.

Appointment of Representatives - Controller, must appoint a representative (Where PII data resides) in one Member States if their establishment offers goods & services or monitors residents outside the EU.

Appointment of Processors - A Controller who appoints a Processor must comply with GDPR and should be done through an agreement which states that the Processor must:

- Act on the controller's instructions as per the document
- Impose confidentiality obligations on all staff who process pertinent data
- To guarantee the security of the personal data it processes
- Comply with the rules for appointing subcontractors
- Implementation of measures to support the Controller complies with the rights of data subjects
- Assist the Controller in obtaining approval of DPAs, if applicable
- Return or destroy the personal data upon the termination of the relationship
- Provide the Controller with all the information necessary to demonstrate compliance with the GDPR

Records of processing activities - The Controller (and its representative, if any) must keep records of the controllers since there is no obligation to notify DPAs.

Cooperation with DPAs - Controllers (and their representatives, if any) are required to cooperate with DPAs in the performance of their tasks.

Data Protection- The Controller must implement appropriate technical and organizational security measures to protect personal data against accidental or unauthorized disclosure or access.

Reporting data breaches to DPA - The Controller must report immediately to the DPA whenever a data breach happens and in any event within 72 hours.

Notifying data breaches to affected data subjects - the Controller must report the affected data subjects immediately in any data breach incident which might cause a high risk to data subjects.

GDPR - OBLIGATIONS OF PROCESSORS

Definition of Processor - A "Processor" is an entity that processes personal data on behalf of the Controller.

Application - GDPR applies to both the Controllers processing data and the Processor who falls within the scope of the GDPR.

Conflicts between the controller's instructions and relevant (EU) law - The Processor must immediately bring to the notice of the Controller in case there is a conflict between the controller's instructions and GDPR requirements or other EU laws.

Appointment of sub Processors - The Processor must not appoint a Sub-Processor without the prior written consent of the controller.

Processor's obligation of confidentiality - The Processor must ensure confidentiality of any personal data that it processes. The Processor must ensure that all persons authorized to process the personal data are under an appropriate obligation of confidentiality.

Compliance with the controller's instructions - Processors (and any Sub-Processors) should not process personal data without the controller's consent or the provisions of EU laws or the national law of Member States.

Failure to comply with the controller's instructions - Where a Processor, in breach of the GDPR, determines the purposes and means of any processing activity.

Records of processing activities - Each Processor (and its representative, if any) must maintain records of its processing activities performed on behalf of the controller:

- Details of the Sontroller/ Processor and any representatives/DPO
- Activities performed and the categories of processing
- Cross-border data transfers information
- Detailed information on the security measures implemented in respect of the processed data

Cooperation with DPAs - Processors (and their representatives, if any) are required to cooperate with DPAs in the performance of their tasks.

Data Security - Processors must implement appropriate technical and organizational security measures to protect personal data against accidental or unauthorized disclosure or access.

Depending on the nature of the processing, these may include:

01 Encryption of the personal data

02 On-going reviews of security measures

03 Redundancy and backup facilities

04 Regular security testing

Data breach reporting - Processors must notify any data breach to the Controller without undue delay.

Obligation to appoint a DPO - If the GDPR requires the appointment of a DPO, this requirement applies to Processors.

Restrictions on Cross-Border Data Transfers - Under the GDPR, the obligations regarding Cross Border Data Transfers apply directly to Processors.

Liability of Processors - Directly claims against Processors can be brought by the data subjects. But the Processor is liable for the damage only when:

- Not complied with obligations under the GDPR that specifically directed to Processors
- Acted outside or contrary to lawful instructions of the Controller

GDPR – Impact Assessments, DPOs and code of conduct

Impact Assessments - Whenever processing activity is proposed, or new technology is introduced results in a high degree of risk for data subjects.

- Evaluation of data subjects (e.g., performance at work, health; behavior; or location)
- Automated decision making with a significant effect on a person (e.g., automated refusal of credit)
- Systematic monitoring (especially covert monitoring)
- Processing Sensitive Personal Data
- Large-scale processing
- Combining or matching separate datasets
- Processing affecting vulnerable individuals
- Processing using untested technology
- Cross-Border Data Transfers

Prior Consultation - DPAs are responsible for creating a list of the types of processing subject to impact assessments.

Appointment of a DPO - A Controller or Processor must appoint a DPO upon the requirement of local laws or if the data processing activities are involved:

01 Systematic monitoring of data subjects is carried on a large scale

02 Regular and systematic monitoring of data subjects on a large scale

03 Processing of sensitive personal data on a large scale

Qualifications of DPO - A Data Protection Officer (DPO) must have in-depth knowledge about Data Protection Law and Practices. He/She must be capable enough to perform the function of DPO.

Role of a DPO

The DPO must administer all data protection matters affecting the Controller or Processor effectively

DPO must be well equipped with the necessary resources and support. Data subjects may contact the DPO (e.g., to exercise their rights under the GDPR). A confidentiality obligation must bind the DPO concerning his or her work

Special protection for DPOs - No instruction is given to DPO in performing his or her duties, and organizations have no authority to terminate the DPO's employment.

Tasks of a DPO - A DPO must fulfil at least the following functions:

01 Controller or Processor or any employees who process personal data are provided with the necessary information and advice related GDPR obligations

02 Ensure Controller or Processor monitors compliance with the GDPR

03 Act as a point of contact and coordinate with DPAs

Purpose of Codes of Conduct - Associations and other industry bodies may prepare Codes of Conduct covering compliance with the GDPR regarding general or specific aspects of the GDPR.

Encouragement of Codes of Conduct - Associations and other industry bodies may prepare Codes of Conduct covering compliance with the GDPR regarding general or specific aspects of the GDPR.

Adhering to Codes of Conduct by non-EEA Controllers and Processors - Controllers and Processors outside the EEA, which are not subject to the GDPR, may adhere to Codes of Conduct to provide a framework for adequate protection to personal data in third countries. The GDPR allows non-EEA Controllers and Processors to comply explicitly with an approved Code of Conduct to serve as the foundation for cross-border data transfers.

Enforcement of Codes of Conduct - The relevant DPA may appoint an independent body to monitor and enforce a code of conduct.

Must have demonstrated its expertise and independent

Must have procedures in place to review and evaluate compliance with a code of conduct

Must have established procedures for dealing with complaints or infringements of the code of conduct

Must demonstrate that there are no conflicts of interest in this role

Advantages of Complying to approved Codes of Conduct - Adherence to an approved code of conduct

01 Guiding on specific compliance issues

02 Evidence of compliance with the GDPR

03 Might become a positive factor in an impact assessment

04 Might provide the basis for Cross-Border Data Transfers

05 Fines imposed on the adherent Controller or Processor may get affected

Approval of Codes of Conduct by DPAs - The competent DPA must have the draft Codes of Conduct, which must then:

- Provide approval for the Code of Conduct if it holds sufficient protection under the GDPR, or amend it if it does not
- Ensuring approved codes of conduct is registered and published
- Publish the criteria for gaining such approval
- DPAs must review the Code of Conduct following the consistency mechanism and see if a Code of Conduct affects processing in several Member States

Approval of Codes of Conduct by the WP29/EDPB - The EDPB is required to give an opinion on any draft code of conduct before its approval. The approved Codes of Conduct must also be registered and publish by the EDPB.

Purpose of seals and certifications - The GDPR provides a voluntary accreditation system under which Controllers or Processors can comply with the requirements of a seal or certification scheme to demonstrate compliance with the GDPR.

Encouragement of seals and certification - Member States, DPAs, the EDPB and the Commission are all under an obligation to encourage the establishment of certification mechanisms focusing mainly on small and medium enterprises. It is the responsibility of the EDPB to maintain and publish a register of seal and certification systems.

GDPR - Cross Border Data Transfers

General prohibition on transfers - Cross-Border Data Transfers may only occur if the transfer is made to an adequate jurisdiction. The data exporter has implemented a lawful data transfer mechanism.

Commission Adequacy Decisions - Cross-Border Data Transfers to a recipient in a third country may occur if the third country receives an adequate decision from the commission. Factors that affect an adequacy decision include:

- The law and legal protections for fundamental freedoms and human rights
- Transferred data access by public authorities
- Existence and effective functioning of DPAs
- Obligations concerning to personal data protection and international commitments

Review of Adequacy Decisions - A periodic review of adequacy decisions related to all relevant developments. The commission may revoke, amend, or suspend decisions relating to adequacy for jurisdictions that no longer provide an adequate level of data protection.

Agreements between public authorities - Cross-Border Data Transfers between public authorities do not require any specific authorization from a DPA; it can take place with the agreements between public authorities themselves. But the public authorities must comply with GDPR requirements.

Binding Corporate Rules – The GDPR directly addresses the concept of BCRs. The competent DPA shall approve the BCRs as an appropriate mechanism for cross-border data transfers within a group of companies. They will approve if the BCRs meet the requirements set out in the GDPR, and no further DPA approval is required to transfer personal data made under the BCRs.

Content of BCRs - BCRs must include a mechanism to make the BCRs legally binding on group companies.

- It is necessary to specify the purpose of the transfer and the categories of data affected
- Should match the requirements of the GDPR
- Need to verify whether EU-based data exporters accept liability on behalf of the entire group
- Justify complaint procedures
- Need to provide the mechanisms for ensuring compliance (e.g., audits)

Approval of BCRs - The competent DPA must approve BCRs that meets the criteria outlined in the GDPR. Where the BCRs aims to cover data transfers from multiple Member States, the consistency mechanism applies.

Model Clauses - Cross-Border Sata Transfers are permitted if the Controller or Processor adduces appropriate safeguards in the form of Model Clauses. These do not require any further authorization from a DPA.

DPA Clauses - Cross-Border Data Transfers may be carried out using standard data protection clauses adopted by one or more DPAs, in line with the GDPR. No further approval is required for the transfers done based on DPA clauses. DPA clauses may be considered on a broader contract provided the original wording of the authorized DPA Clauses is not contradicted.

Codes of Conduct - A Cross-Border Data Transfer may be carried out based on an approved code of conduct, accompanied by enforceable commitments to provide proper protection. No DPA approval is required for the transfers made on this basis.

Certification - A Cross-Border Data Transfer may be carried based on certificates and with the data importer's enforceable commitments to transfer the data to apply the certification to the transferred data. No DPA approval is required for the transfers made on this basis.

Ad hoc clauses - A Cross-Border Data Transfer may take place based on ad hoc clauses. These clauses must adhere to the requirements of the GDPR and must have the approval of the associated DPA subject to the consistency mechanism before transfers can begin.

Administrative arrangements - A Cross-Border Data Transfers may occur based on administrative agreements between public authorities (e.g., a Memorandum of Understanding), including sufficient protection for the individual's rights. DPA approval is not mandatory for the transfers made on this basis.

Public registers - A Cross-Border Data Transfer may occur if the transferred data are taken from a record made available to the public or upon request of any person who can showcase genuine interest in examining it. This does not allow a transfer of the entire register.1

Controller's compelling legitimate interests - A Cross-Border Data Transfer may be carried out if:

- None of the other Laws is applicable
- The transfer is not monotonous
- Only affects a limited number of data subjects
- the transfer is necessary for compelling legitimate interests pursued by the Controller which are not overridden by those of the data subject
- The Controller has mentioned suitable protection for the transferred data
- The Controller must bring it to the notice of relevant DPA and the data subjects about the transfer

Specific transfer mechanisms may be limited by law - EU law or law of the Member States may expressly limit Cross–Border Data Transfers relating to specific categories of personal data for important reasons of public interest. The Member States must notify such restrictions to the commission.

GDPR - DATA PROTECTION AUTHORITIES

Responsibilities of DPAs - It is necessary to implement the regulation and protect the rights and freedoms of the individuals. So, each Member State is required to appoint one or more DPAs.

Jurisdiction - Each DPA can only exercise its powers on the territory of its Member State. Under the "One-Stop-Shop", the DPA's regulatory actions may affect processing in the other Member States.

Independence - Each DPA must act with complete independence in carrying out its functions.

Establishment and appointment of DPAs -

- Each DPA must be appointed through a transparent procedure
- DPA must have the required skills and experience to perform the role
- DPA must follow professional secrecy

The "One-Stop-Shop "- Identifying a lead DPA is only relevant where a Controller or Processor established in the EU carries out cross-border processing of personal data. If a Controller has companies in the multiple Member States, its "main establishment" will be its lead DPA. The lead DPA holds power to regulate that Controller across all Member States.

Organizations should be able to demonstrate the basis for claiming the main establishment, considering the following factors:

- Where the processing decisions are made
- Where the decisions lie for power implementation
- Where registrations are carried out for the relevant entity
- The location of the decision-makers responsible for processing

Tasks of DPAs - The tasks of DPAs include obligations to:

Monitor and fortify the application of the GDPR	Raise awareness of the risks, rules, protection, and about personal data rights (especially regarding children)	Advise national and governmental institutions on the importance of the GDPR
Gather claims brought by data subjects or their agents and inform the outcome of such claims to the data subjects	Establish requirements for impact assessments	Support the creation of codes of conduct and review certifi-cations
Authorize Model Clauses and BCRs	Keep records of sanctions and enforcement actions	Fulfil "any other tasks related to the protection of personal data"

Powers of DPAs - DPAs are empowered to oversee the GDPR, investigate breaches of the GDPR and bring legal proceedings where necessary.

Activity reports - Each DPA must draw up an annual report on its activities. The information must be made available to the public.

EU-level DPA coordination - The EDPB is formed by deputies of DPAs from each Member State. Along with providing advice, it also actively participate in enforcing the Data Protection Law of the European Union. Whichever Member State has more than one DPA (e.g., Bundesland of Germany has a DPA), only a single representative to the EDPB is appointed by the Member State.

DPA cooperation - DPAs are required to cooperate and provide each other with mutual assistance. They also have the formal legal authority to carry out joint operations.

Consistency mechanism - Where an organization engages in cross-border data processing that affects data subjects in the multiple Member States, a DPA that wishes to act must consult with the other affected DPAs to ensure consistency in applying the GDPR.

GDPR - COOPERATION AND CONSISTENCY

The consistency mechanism - All Member States' DPAs must cooperate among themselves with the EDPB and commission to ensure consistent implementation of the GDPR.

Opinion of the EDPB - DPAs must submit a draft to the EDPB before taking any of the following measures:

Specify the processing measures that should undergo an impact assessment

Approving a code of conduct

Approving accreditation criteria

Determining the content of DPA clauses

Authorizing ad hoc

Approving BCRs

The EDPS may examine each of these measures and deliver an opinion if the issue in question affects the several Member States The relevant DPA must take EDPB's opinion as the "greatest account" while proceeding with its decision

Dispute resolution by the EDPB - If DPAs disagree with the key data protection law issues, then the EDPB may issue a binding decision, which needs to be adopted by the concerned DPAs within a month from the date of notification of the EDPB's decision

Urgency procedure -In some cases, DPA might have to immediately adopt provisional measures for up to three months in case of an urgent need for protecting data subjects' rights

A detailed explanation must be given to other concerned DPAs, to the EDPB and the commission. May also request an instant opinion from the EDPB if necessary

Exchange of information - The Commission may implement acts that specify arrangements for the electronic exchange of information between DPAs and the EDPB. The EDPB may advise on these issues

GDPR - REMEDIES AND SANCTIONS

Right to complain to a DPA - Data Subjects have the right to complain about their personal data processing with a DPA in the Member State where they live/work/Member State in which the alleged violation happened. It is the responsibility of the DPA to keep the data subject informed about the progress or the outcome of the complaint lodged.

Right to a judicial remedy - Data subjects have all the right to an effective judicial remedy against:

01 DPA if the decisions concerning them

02 DPA if they fail to deal or respond to a complaint lodged within three months

03 Any illegal processing of their personal data by a Controller or Processor

Venue for proceedings - Proceedings against a DPA or public authority shall be initiated in the Member State where the DPA is established. May bring in proceedings against a Controller or Processor if:

Member State where the Controller or Processor has a corporation

Member State where the data subject resides

Representation of data subjects – A not-for-profit body or association whose legal objectives are in the public interest and who is involved in protecting the rights and freedoms of data subjects may complain with a DPA on behalf of a data subject.

Suspension of proceedings -When a court of a Member State becomes aware of a proceeding pending in another Member State, involving the same Controller or Processor and the same subject, that court may contact the relevant court and confirm with the other Member State about the existence of such proceedings and suspend its proceedings if appropriate.

Compensation and liability - A data subject who has suffered damage due to the illegal processing of their personal data have all the right to obtain compensation from the Controller or Processor for the damage caused.

01 Any Controller connected in the processing is liable for the damage caused

02 The Processor will be liable for any damage caused by any of its processing activities (or its Sub-Processors) that do not comply with its obligations as per GDPR or are in breach of the controller's instructions

03 To ensure fair compensation, each Controller or Processor will be held liable for the overall damage caused by the same processing

Liability of joint controllers - Data subjects are entitled to enforce their rights against any joint controllers. Each joint Controller is liable for the total damage. However, national law may apportion liability between them if one joint Controller has paid total compensation. Proceedings will be initiated against the other joint controllers to recover their share of the damages.

Exemptions from liability - A Controller or Processor will not be liable if it is proved that they are not responsible for the event giving rise to the damage. There is no mention of an inevitable accident.

Administrative fines - Each DPA shall ensure the imposition of administrative penalties and fines in a practical, proportionate, and deterrent manner. The law of a Member State does not provide for administrative fines. Fines can be imposed by DPA and by national jurisdictions.

Maximum administrative fines - For any serious infringements of the GDPR, the maximum penalty that can be imposed is €20 million or four per cent of an undertaking's worldwide turnover for the preceding financial year. Application of administrative fines by DPAs - DPAs is required to give due regard to a range of issues while deciding whether to impose a penalty or on the amount, including:

The nature, force, and duration of the breach	The number of individuals affected, and the level of damage born by them	The intended or negligence caused the violation
Any action was taken by the Processor or Sontroller to mitigate the damage	Any relevant previous violations by the Controller or Processor	The level of cooperation with the relevant DPA
Whether the violation was self-reported by the Controller or Processor	Any other aggravating or mitigating factors	

Penalties and criminal sanctions - Member States set their own rules on penalties applicable to the GDPR, particularly those violations that are not subject to administrative fines. Member States may also implement their regulations on unlawful sanctions for breach of the GDPR.

GDPR - ALL ABOUT LAW

ISSUES RELATED TO NATIONAL LAW

Out-of-scope areas of law - Any data processing activities that fall outside the scope of EU law are not subject to the GDPR.

Processing of personal data and freedom to express and inform- Member States must regulate the right to the protection of personal data in the framework of the GDPR with the right to freedom of expression and information, including the processing of personal data for editorial, academic, artistic purpose.

Personal data contained in official documents - Personal data contained in official documents may be processed to regulate public access to official documents with the right to protect personal data.

Processing - national ID numbers -Member States are free to determine the conditions under which national identification numbers can be dealt with, subject to appropriate guarantees for rights and freedoms of data subjects according to the GDPR.

Processing in the employment context - Member States may create new laws or conclude collective agreements to protect personal data in the context of national employment law. These must include appropriate protection. Any rules adopted in this area by Member States must inform the commission.

Personal data processing for scientific, historical, or statistical purposes - Subject to appropriate safeguards, and if there is no risk of a data breach, Member States may restrict the rights to access, rectify and restrict the processing of the data subject and object to the handling of their personal data for scientific, historical or statistical purposes.

Obligations of professional secrecy - Member States may create their own rules concerning Controllers or Processors subject to professional secrecy obligations and must inform the commission.

Personal data processing in the context of churches and religious establishments- Where, in a Member State, churches and religious associations or communities lay down rules relating to the processing of personal data, those rules may be applied if they are brought into line with the provisions of the GDPR. Churches and religious associations that impose such laws are subject to the oversight of the relevant DPA.

GDPR – RELATIONSHIP WITH OTHER LAWS

Repeal of the directive - The GDPR repeals the directive as the date on which the GDPR enters into force. Therefore, any reference to the directive shall be interpreted as a reference to the GDPR. Any references to the WP29 shall be interpreted as references to the EDPB.

Relationship with the ePrivacy directive - The GDPR does not impose any additional obligations on suppliers of telecommunications services that process personal data under the ePrivacy directive. However, there is still some uncertainty about the relationship between the ePrivacy directive and the GDPR, which requires further clarification.

Relationship with existing international agreements - International agreements involving the transfer of personal data to third countries or international organizations that the Member States concluded before the entry into force of the GDPR and compliant with applicable EU law remain in force until amended, replaced, or revoked.

GDPR – TRANSITIONAL PROVISIONS

Transitional period - Once the GDPR comes into force, there will be a two-year moratorium on implementation.

Evaluation - The commission is required to submit reports on the assessment of the GDPR to the European parliament and the council every four years, providing (if necessary) suitable proposals for amendments to the GDPR. The commission is also required to review other EU data protection instruments regularly.

AUTHOR BIO

Satheesh L Kamath
Senior Project Manager, IMSS

Satheesh L Kamath has over 25+ years in the IT development, services and consulting experience spanning ERP, Mainframes, iSeries, Cloud and Process related expertise. He has had rendezvous with retail, manufacturing, healthcare, insurance and jewelry domains. Currently he is part of the **Infrastructure Management** and **Security Services** business unit in Happiest Minds Technologies Pvt Ltd. Recent endeavors being in **Governance, Risk and Compliance** space, he has versatile cross domain and technology expertise with a keen interest in emerging Digital Technologies.