TABLE OF CONTENTS

1. INTRODUCTION

Recently, the General Data Protection Regulation (REGULATION (EU) 2016/679) was passed. It shall replace the present Data Protection Directive (DPD 95/46/EC), which is a step that is likely to impact the workings of many organizations. This document intends to offer a clear comparison between the General Data Protection Regulation (GDPR) a the Data Protection Direction (DPD).

The GDPR i.e. General Data Protection Regulation (REGULATION (EU) 2016/679) was adopted on May 27th, 2016. It will come into force after a two-year transition period on May 25th, 2018 and will replace the Data Protection Directive (DPD 95/46/EC). The Regulation intends to empower data subjects in the European Union by giving them control over the processing of their personal data. This is not an enabling legislation. Unlike the previous regime under the DPD (Data Protection Directive), wherein different member States legislated their own data protection laws, the new regulation intends uniformity in application with some room for individual member states to legislate on procedural mechanisms. While this will ensure a predictable environment for doing business, a number of obligations will have to be undertaken by organizations, which might initially burden them financially and administratively.

2. SUMMARY

The Regulation contains a number of new provisions as well as modified provisions that were under DPD and has removed certain requirements under the DPD. Some significant changes mentioned in the document have been summarized in this section.. These changes suggest that GDPR is a comprehensive law with detailed substantive and procedural provisions. Yet, some ambiguities remain with respect to its workability and interpretation. Clarifications will be required.

2.1 Provisions from the DPD that were retained but altered in the GDPR include:

2.1.1 Scope:

GDPR has an expanded territorial scope and is applicable under two scenarios; 1) when processor or controller is established in the Union, and 2) when processor or controller is not established in the Union. The conditions for applicability of the GDPR under the two are much wider than those provided for DPD. Also, the criteria under GDPR are more specific and clearer to demonstrate application.

2.1.2 Definitions:

Six definitions have remained the same while those of personal data and consent have been expanded.

2.1.3 Consent:

GDPR mentions "unambiguous" consent and spells out in detail what constitutes a valid consent. Demonstration of valid consent is an important obligation of the controller. Further, the GDPR also explains situations in which child's consent will be valid. Such provisions are absent in DPD.

2.1.4 Special categories of data:

Two new categories, biometric and genetic data have been added under GDPR.

2.1.5 Rights:

The GDPR strengthens certain rights granted under the DPD. These include:

a. **Right to restrict processing:** Under DPD the data subject can block processing of data on the grounds of data inaccuracy or incomplete nature of data. GDPR, on the other hand , is more elaborate and defined in this respect. Many more grounds are listed together with consequences of enforcement of this right and obligations on controller.
b. **Right to erasure:** This is known as the "right to be forgotten". Here, the DPD merely mentions that the data subject has the right to request erasure of data on grounds of data inaccuracy or incomplete nature of data or in case of unlawful processing. The GDPR has strengthened this right by laying out 7 conditions for enforcing this right including 5 grounds on which the request for erasure shall not be processed. This means that the "right to erasure" is not an absolute right. GDPR provides that if data has been made public, controllers are under an obligation to inform other controllers processing the data about the request.
c. **Right to rectification:** This right is similar under GDPR and DPD.

d. **Right to access:** GDPR has broadened the amount of information data subject can have regarding his/her own data. For example, under the DPD the data subject could know about the purpose of processing, categories of processing, recipients or categories to whom data are disclosed and extent of automated decision involved. Now under GDPR, the data subject can also know about retention period, existence of certain rights, about source of data and consequences of processing. It specifically states controllers obligations in this regard.
e. **Automated individual decision making including profiling:** This is an interesting provision that applies solely to automate decision-making. This includes profiling, which is a process by which personal data is evaluated solely by automated means for the purpose of analyzing a person's personal aspect such as performance at work, health, location etc. The intent is that data subjects should have the right to obtain human intervention into their personal data. This upholds philosophy of data safeguard as the subject can get an opportunity to express himself, obtain explanation and challenge the decision. Under GDPR, such decision-making excludes data concerning a child.

2.1.6 Code of conduct:

A voluntary self-regulating mechanism has been provided under both GDPR and DPD.

2.1.7 Supervisory Authority:

As compared to the DPD, the GDPR lays down detailed and elaborate provisions on Supervisory Authority.

2.1.8 Compensation and Liability:

Although compensation and liability provisions under GDPR and DPD are similar, the GDPR specifically mentions this as a right with a wider scope. While the Directive enforces liability on the controller only, under the GDPR, compensation can be claimed from both, processor and controller.

2.1.9 Effective judicial remedies:

Provisions in this area are also quite similar between the DPD and GDPR. The difference is that GDPR specifically mentions this as a "right" and the Directive does not. Use of such words is bound to bring legal clarity. It is interesting to note that in the DPD, recourse to remedy has been mentioned in the Recitals and it is the national law of individual member states, which shall regulate the enforceability. GDPR, on the other hand, mentions this under its Articles together with the jurisdiction of courts and exceptions to this right.

2.1.10 Right to lodge complaint with supervisory authority:

The right conferred to the data subject to seek remedy under unlawful processing has been strengthened under GDPR. Again, as mentioned above, GDRP specifically words this as a "right" while the DPD does not.

2.2 New provisions added to the GDPR include:

2.2.1 Data Transfer to third countries:

Provisions under Chapter V of GDPR regulate data transfers from EU to third countries and international organizations and data transfer onward. DPD only provides for data transfer to third countries without reference to international organizations.

A mechanism called adequacy decisions for such transfers remains the same under both laws. However, in situations where Commission does not take adequacy decisions, alternate and elaborate provisions on "Effective Safeguards" and "Binding Corporate Rules" have been mentioned under the GDPR. Other certain situations have been envisaged under both GDPR and DPD for data transfers in absence of adequacy decision. These are more or less similar with a only few modifications.

Significantly, GDPR brings clarity with respect to enforceability of judgments and orders of authorities that are outside of EU over their decision on such data transfer. Additionally, it provides for international cooperation for protection of personal data. These are not mentioned in the DPD.

2.2.2 Certification mechanism:

Just like code of conduct, this is also a voluntary mechanism, which can aid in demonstrating compliance with Regulation.

2.2.3 Records of processing activities:

This is a mandatory "compliance demonstration" mechanism under GDPR, which is not mentioned under DPD. Organizations are likely to face initial administrative and financial burdens in order to maintain records of processing activities.

2.2.4 Obligations of processor:

DPD fixes liability on controllers but leaves out processors. GDPR includes both. Consequently, GDPR specifies obligations of the processor, the kinds of processors the controller can use and what will govern processing.

2.2.5 Data Protection officer:

This finds no mention in the DPD. Under the GDPR, a data protection officer must be mandatorily appointed where the core business activity of the

organization pertains to processing, which requires regular and systematic monitoring of data subjects on large scale, processing of large scale special categories of data and offences, or processing carried out by public authority or public body.

2.2.6 Data protection impact assessment:

This is a Privacy Impact assessment for ensuring and demonstrating compliance with the Regulation. Such assessment can identify and minimize risks. GDPR mandates that such assessment must be carried out when processing is likely to result in high risk. The relevant Article mentions when to carry out processing, the type of information to be contained in assessment and a clause for prior consultation with supervisory authority prior to processing if assessment indicates high risk.

2.2.7 Data Breach:

Under this provision, the controller is responsible for two things: 1) reporting personal data breach to supervisory authority no later than 72 hours . Any delay in notifying the authority has to be accompanied by reasons for delay; and 2) communicating the breach to the data subject in case the breach is likely to cause high risk to right and freedoms of the person. As far as the processor is concerned, in the event of data breach, the processor must notify the controller. This provision is likely to push some major changes in the workings of various organizations. A number of detection and reporting mechanisms will have to be implemented. Above all, these mechanisms will have to be extremely efficient given the time limit.

2.2.8 Data Protection by design and default:

This entails a general obligation upon the controller to incorporate effective data protection in internal policies and implementation measures.

2.2.9 Rights:

Under the GDPR, a new right called the " Right to data portability " has been conferred upon the data subjects. This right empowers the data subject to receive personal data from one controller and transfer it to another.

2.2.10 New Definitions:

Out of 26 definitions, 18 new definitions have been added. "Pseudonymisation" is one such new concept that can aid data privacy. This data processing technique encourages processing in a way that personal data can no longer be attributed to a specific data subject without using additional information. This additional information is to be stored separately in a way that it is not attributed to an identified or identifiable natural person.

2.2.11 Administrative fines:

Perhaps much concern about GDPR is due to provisions on high fines for non-compliance of certain provisions. Organizations simply cannot afford to ignore it. Non-compliance can lead to imposition of very heavy fines up to 20,000,000 EUR or 4% of total worldwide turnover.

2.3 Deleted provisions under DPD include :

2.3.1 Working Party:

Working party under the DPD has been replaced by the European Data Protection Board provided by the GDPR. The purpose of the Board is to ensure consistent application of the Regulation.

2.3.2 Notification Requirement:

The general obligation to notify processing supervisory authorities has been removed. It was observed that this requirement imposed unnecessary financial and administrative burden on organizations and was not successful in achieving the real purpose that is protection of personal data. Instead, now the GDPR focuses on procedures and mechanisms like Privacy Impact assessment to ensure compliance.

3. BRIEF OVERVIEW

The GDPR is the new uniform law, which will now replace older laws. A brief overview has been given below:

Topic	**GDPR (General Data Protection Regulation)**	**DPD (Data Protection Directive)**
Name	REGULATION (EU) 2016/679	DPD 95/46/EC
Enforcement	Adopted on 27 May 2016 To be enforced on 25 May 2018	Adopted on 24 October 1995
Effect of legislation	It is a Regulation. Is directly applicable to all EU member states without requiring a	It is an enabling legislation. Countries have to pass their own separate

	separate national legislation.	legislations.
Objective	To protect "natural persons" with regard to processing of personal data and on free movement of such data. It repeals DPD 95/46/EC.	To protect "individuals" with regard to processing of personal data and on free movement of such data.
Number of Chapters	XI	VII
Number of Articles	99	34
Number of Recitals	173	72
Applicability	To processors and controllers	Same

4. COMPARATIVE ANALYSIS OF GDPR AND DPD

This section offers a comparative analysis through a set of tables and text analysing and comparing the provisions of General Data Protection Regulation (GDPR) with those of the Data Protection Direction (DPD). Spaces left blank in the tables imply lack of similar provisions under the respective data regime.

4.1 Territorial Scope

GDPR has expanded territorial scope. The application of Regulation is independent of the place where processing of personal data takes places under certain conditions. The focus is the data subject and not the location. The DPD made application of national law, a criterion for determining the applicability of the Directive. Under the GDPR, the following conditions need to be satisfied for application of Regulation.

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	3	4
When processor or controller is established in the Union, the Regulation/ Directive will apply if: *(DPD is silent on*	1. Processing is of personal data 2. Processing is in "context of activities" of the establishment 3. Processing may	Processing is of personal data.

location of processors)	or may not take place in the Union	
When processor or controller is not established in Union, the Regulation/Directive will apply if: *(DPD is silent on location of processors*)	1. Data subjects are in the Union; and 2. Processing activity is related to: I. Offering of goods or services; or II. Monitoring their behavior within Union 3. Will apply when Member State law is applicable to that place by the virtue of public international law	1. Like GDPR the DPD mentions that national law should be applicable to that place by virtue of public international law; Or 2. If the equipment for processing is situated on Member state territory unless it is used only for purpose of transit.

4.2 Material Scope

The Recital under GDPR explains that data protection is not an absolute right. Principle of proportionality has been adopted to respect other fundamental rights.

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	2	3
Applies to	Processing of personal data Processing is by automated means, wholly or partially When processing is not by automated means,	Same

	the personal data should form or are intended to form a part of filing system	
Does not apply to	Processing of personal data: 1. For activities which lie outside scope of Union law 2. By Member State under Chapter 2 Title V of TEU 3. By natural person in course of purely personal or household activity 4. By competent authorities in relation to criminal offences and penalties and threats to public security 5. Under Regulation (EC) No 45/2001. This needs to be adapted for consistency with GDPR 6. Which should not prejudice the E commerce Directive 2000/31/EC especially the liability rules of intermediary service providers	The provisions in DPD are similar to GDPR. In addition to Title V, the DPD did not apply to Title VI of TEU. DPD doesn't mention Regulation (EC) No 45/2001 or the E commerce Directive 2000/31/EC.

4.3 Definitions

GDPR incorporates 26 definitions as compared to 8 definitions under DPD. There are 18 new definitions in GDPR. Some definitions have been expanded.

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	4	2
New Definitions under GDPR	1. Restriction of processing 2. Profiling 3. Pseudonymisation 4. Personal data breach 5. Genetic data 6. Biometric data 7. Data concerning health 8. Main establishment 9. Representative 10. Enterprise 11. Group of undertakings 12. Binding corporate rules 13. Supervisory authority 14. Supervisory authority concerned 15. Cross border processing 16. Relevant and reasoned objection 17. Information society service 18. International organizations	
2 definitions that have been expanded under GDPR	1. Personal data 2. Consent	
6 Definitions which have remained same in GDPR and DPD	1. Processing of personal data 2. Personal data filing system 3. Controller	

	4. Processor 5. Third party recipient	

4.3.1 Expanded definition of personal data

Both DPD and GDPR apply to 'personal data'. The GDPR gives an expanded definition of 'personal data'. Recital 30 gives example of an online identifier such as IP addresses.

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	4(1)	2(a)
New term added in the definition	A new term " online identifier" has been added. Example of online identifier is given under Recital 30. An IP address is one such example.	

4.3.2 Expanded definition of consent

Valid consent must be given by the data subject. The definition of valid consent has been added under GDPR. Recital 32 further explains that consent can be given by "means of a written statement including electronic means or an oral statement". For example, ticking a box on websites signifies acceptance of processing while "pre ticked boxes, silence or inactivity" do not constitute consent.

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	4(11)	2(h)
Term added in GDPR	Consent must be unambiguous, freely given, specific and informed.	The word "unambiguous" is not contained in DPD.

Means of signifying assent to processing own data	Assent can be given by a *statement or by clear affirmative action* signifying assent to processing.	DPD merely mentions that *freely given, specific and informed consent* signifies assent.

4.4 Conditions for consent

GDPR lays down detailed provisions for valid consent. Such provisions are not given in DPD.

Sub-topics in the section	**GDPR**	**DPD**
Article	7	
Obligation of controller	Must demonstrate consent has been given	
Presentation of written declaration of consent	It should be in a clearly distinguishable, intelligible and easily accessible form. Language should be clear and plain.	
If declaration or any part of it infringes on Regulation	Declaration will be non-binding.	
Right of data subject	To withdraw consent at any time.	
	If consent is withdrawn, it will not make processing done earlier unlawful.	
For assessing whether consent is freely given	Must consider whether performance of contract or provision of service is made conditional on consent to processing of data not necessary for performance of contract.	

4.5 Conditions applicable to child's consent in relation to information society services

This article prescribes an age limit for making processing lawful when information society services (direct online service) are offered directly to a child.

Sub Topics in the Section	GDPR	DPD
Given in Article	8	
Conditions for valid consent in this case	If child is at least 16 years old his consent is valid. If child is below 16 years consent must be obtained from holder of parental responsibility over the child.	
Age relaxation can be given when	Member States provides a law lowering the age. Age cannot be lowered below 13 years.	
Controller's responsibility	Verify who has given the consent	
Exceptions	This law will not affect: General contract law of member states; Effect of contract law on a child;	

4.6 Processing of special categories of personal data

Like the DPD, the GDPR spells out the data that is considered sensitive and the conditions under which this data can be processed. Two new categories of special data, "genetic data" and "biometric data", have been added to the list in the GDPR.

Sub Topics in the Section	GDPR	DPD

Article	9	8
Categories of data considered sensitive	Racial or ethnic origin	Same
	Political opinions	Same
	Religious or philosophical beliefs	Same
	Trade union membership	Same
	Health or sex life or sexual orientation	Same
	Genetic data or Biometric data uniquely identifying natural person	
Circumstances in which processing of personal data may take place	If there is explicit consent of data subject provided Member State laws do not prohibit such processing	
	Necessary for carrying out specific rights of controller or data subject	Under DPD these rights can be for employment. The GDPR adds social security and social protection to this list. These rights are to be authorized by Member state or Union. The GDPR adds “Collective agreements” to this.
	In the vital interest of data subject who cannot give consent due to physical or legal causes.	Same
	In the vital interest of a Natural person physically or legally incapable of giving consent	Same
	For legitimate activities carried on by not-for profit-bodies for political, philosophical or trade union aims subject to	Same

	certain conditions.	
	When personal data is made public by data subject	Same
	For establishment, exercise of defense of legal claims or for courts	Same
	For substantial public interest in accordance with Member State or Union law	
	Is necessary for: Preventive or occupational medicine Assessing working capacity of employee Medical diagnosis Healthcare or social care services Contract with health professional	
	Is necessary in Public interest in the area of public health	
	For public interest, scientific or historical research or statistical purpose	
Data for preventive or occupational medicine, medical diagnosis etc. can be processed when:	Data is processed by or under responsibility of a professional under obligation of professional secrecy as state in law	Here the processing is done by health professional under obligation of professional secrecy

4.7 Principles relating to processing of personal data

The principles set out in GDPR are similar to the ones under DPD. Some changes have been introduced. Accountability of the controller has been specifically given under GDPR.

Sub-topics in this section	GDPR	DPD
Given in Article	5	6
Lawfulness, fairness, transparency	Processing must be Lawful, fair and transparent	Does not mention transparent
Purpose limitation	Data must be specified, explicit and legitimate.	Same
	Processing for achieving public interest, scientific or historical research or statistical purpose is not to be considered incompatible with initial purpose.	Same
Data minimization	Processing is adequate, relevant and limited to what is necessary	Same
Accuracy	Data is accurate, up to date, erased or rectified without delay	Same
Storage limitation	Data is to be stored in a way that data subject can be identified for no longer than is necessary for purpose of processing	Same
	Data can be stored for longer periods when it is processed solely in public interest, scientific or historical research or statistical purpose	Same However, public interest is not mentioned.
	There must be	Same

	appropriate technical and organizational measures to safeguard rights and freedoms	Additionally, it specifically states that Member States must lay down appropriate safeguards
Integrity and confidentiality	Manner of processing must: Ensure security of personal data, Protection against unlawful processing and accidental loss, destruction or damage	Not mentioned
Accountability	Controller is responsible for and must demonstrate compliance with all of the above.	DPD states it is for the controller to ensure compliance with this Article. Unlike GDPR, DPD doesn't specifically state the responsibility of controller for demonstrating compliance.

4.8 Lawfulness of processing

The conditions for "lawfulness of processing" under DPD have been retained in the GDPR with certain modifications allowing flexibility for member states to introduce specific provisions in public interest or under a legal obligation. It should be noted that protection given to child's data and rights and freedoms of data subject should not be prejudiced. Additionally, a non-exhaustive list has been laid down in the GDPR for determining if processing is permissible in situations where the new purpose of processing is different from original purpose.

Sub Topics in the Section	GDPR	DPD

Given in Article	6	7
Processing is lawful when :	If at least one of the principles applies: Data subject has given consent to processing for specific purpose(s).	Same However it mentions “unambiguous” consent.
	Processing is necessary for performance of contract to which data subject is party or at request of data subject before entering into a contract	Same
	Processing is necessary for controller’s compliance with legal obligation.	Same
	Is necessary for legitimate interests pursued by controller or by third party subject to exceptions (should not override rights and freedoms of data subject and protections given to child’s data.)	Same
	It is necessary for performance of task carried out in public interest or for exercise of official authority vested in controller	Same It additionally mentions third party: “...exercise of official authority vested in controller *or in a third party to whom data are disclosed”*
	For protections of vital interest of data subject or another natural	Same Does not mention

	person	natural person.
Member States may introduce specific provisions when:	When processing is necessary for compliance with a legal obligation or to protect public interest	
	Basis for processing for shall be laid down by: Union law or Member State law	
If processing is done for purpose other than for which data is collected and is without data subject's consent or is not collected under law:		
To determine if processing for another purpose is compatible with the original purpose	Controller shall take into account following factors:	
	Link between purposes for which data was collected and the other purpose	
	Context in which personal data have been collected	
	Nature of personal data	
	Possible consequences of other purpose	
	Existence of appropriate safeguards	

4.9 Processing which does not require identification:

This article lays down the conditions under which the controller is exempted from gathering additional data in order to identify a data subject for the purpose of complying with this Regulation. If the controller is able to demonstrate that identification is not possible, the data subject is to be informed if possible.

Sub Topics in the Section	GDPR	DPD
Given in Article	11	

Conditions under which the controller is not obliged to maintain process or acquire additional information to identify data subject	If purpose for processing doesn't not require identification of data subject by the controller	
Consequence of not maintaining the data	Art 15 to 20 shall not apply provided controller is able to demonstrate its inability to identify the data subject	
Exception to above consequence will apply when :	Data subject provides additional information enabling identification	

4.10 Rights of the data subject

The General Data Protection Rules (GDPR) confers 8 rights upon the data subject.These rights are to be honored by the controller:-

1. Right to be informed
2. Right of access
3. Right to rectification
4. Right to erasure
5. Right to restrict processing
6. Right to data portability
7. Right to object
8. Rights in relation to automated decision making and profiling

4.10.1 Right to be informed

The controller must provide information to the data subject in cases where personal data has not been obtained from the data subject. A number of exemptions have been listed. Additionally, GDPR lays down the time period within which the information has to be provided.

Sub Topics in the Section	GDPR	DPD
Given in Article	14	10

Type of information to be provided	Identity and contact details of the controller or controller's representative	Same
	Contact details of the data protection officer	
	Purpose and legal basis for processing	Purpose of processing
	Recipients or categories of recipients of personal data	Same
	Intention to transfer data to third country or international organization and Information regarding adequacy decision or suitable safeguards or Binding Corporate Rules or derogations. This includes means to obtain a copy of these as well as information on place of availability.	
Additional information to be provided by controller to ensure fair and transparent processing	Storage period of personal data and criteria for determining the period	
	Legitimate interests pursued by controller or third party	
	Existence of data	

	subject's rights with regard to access or rectification or erasure of personal data, automated decision making	
	Where applicable, existence of right to withdraw consent	
Time period within which information is to be provided	Information to be given within a reasonable period, latest within one month.	
	To be provided latest at the time of first communication to data subject, if personal data are to be used for communication with data subject	
	In case of intended disclosure to another recipient , at the latest when personal data are first disclosed.	
	If processing is intended for a new purpose other than original purpose, information to be provided prior to processing on new purpose.	
Situations in which	Data subject already	Same

exceptions are applicable	has information	
	Provision of information involves disproportionate effort or is impossible or renders impossible or seriously impairs achievement of objective of processing. This is particularly with respect to processing for archiving purposes in public interest, scientific or historical research or statistical purpose. However controller must take measures to protect data subject's rights and freedom and legitimate interests including make information public.	Provision involves impossible or disproportionate effort, in particular where processing is for historical or scientific research. However, appropriate safeguards must be provided by Member States.
	Obtaining or disclosure is mandatory under Union or member law and it provides protection to data subject's legitimate interests	Where law expressly lays down recording or disclosure provided appropriate safeguards are provided by Member States. This is particularly applicable to processing for scientific or historical research.
	Confidentiality of data	

	mandated by professional secrecy under Union or Member State law	

4.10.2 Right to access

Both Data Protection Directive (DPD) and General Data Protection Rules (GDPR) confer right to access information regarding personal data on the data subject.

CJEU in YS V. Minister voor Immigrate Integratie en Asiel stated that it is the data subject's right "to be aware of and verify the lawfulness of the processing".

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	15	12
Data subject has the right to know about:	Purpose of processing	Same
	Categories of processing the data	Same
	Recipients or categories to whom data are disclosed	Same
	Retention period of the data and criteria for this	
	Existence of right to request erasure, rectification or restriction of processing	
	Right to lodge complaint with supervisory authority	

	Knowledge about source of data	
	To know about any significant and envisaged consequences of processing for the data subject	
	Existence of automated decision making and logic involved	Same
In case of data transfer to third country	Right to be informed about the safeguards	
Controller's obligation	To provide a copy of data undergoing processing. Reasonable fee based on administrative costs can be charged for this.	

4.10.3 Right to rectification

GDPR and DPD both give the data subject the right to rectify their personal data. Under the GDPR the data subject can complete the incomplete data by giving a supplementary statement.

Sub-topics in the section	GDPR	DPD
Given in Article	16	12(b)
Right can be exercised when:		Processing does not comply with the Directive i.e. damage is caused due to unlawful processing (Recital 55) OR
	When data is incomplete	When data is incomplete or inaccurate
Obligations of controller	To enforce the right without undue delay	
Obligation of controller	Given under Art 19	Given under Article 12(c)

to give notification when data is disclosed to third party	Request of erasure of personal data to be communicated to each recipient of such data	Request must be communicated to third parties
	It should not involve an impossible or disproportionate effort	Same

4.10.4 Right to erasure

This is also referred to as the "right to be forgotten". It empowers the individual to erase personal data under certain circumstances. The data subject can request the controller to remove the data for attaining this purpose.

Sub-topics in the section	GDPR	DPD
Given in Article	17	12(b)
Obligation of the controller	To erase the data without undue delay	
Conditions under which the right can be exercised		When processing does not comply with the Directive i.e. damage is caused due to unlawful processing (Recital 55) OR When data is incomplete or inaccurate
	Personal data is no longer necessary for the purpose for which it was collected or processed	
	Data Subject withdraws consent for processing	
	Data subject objects to processing and there are no overriding legitimate grounds for processing	
	Data subject objects to processing for direct marketing purpose	
	Personal data has been	

	unlawfully processed	
	When personal data has to be erased under a legal obligation of Union or member State law	
	When personal data has been collected in offer of information society services to a child	
Condition of processing under which request to erasure shall not be granted	For exercising right of freedom of expression and information	
	Processing is done under Union or Member State law in public interest or exercise of official authority vested in controller	
	Done for public interest in public health	
	For public interest, scientific or historical research or statistical purpose.	
	For establishment, exercise or defense of legal claims.	
Controller's obligations when personal data has been made public	Controller to take reasonable steps to inform controllers who are processing the data, of the request of erasure. All links, copy or replication of personal data to be erased. Technology available and cost of implementation to be taken into account.	
Notification when data is disclosed to third party	Given under obligation of controller under Art 19:	Given under obligation of controller under 12(c) :

	Request of erasure of personal data to be communicated to each recipient of such data	Request must be communicated to third parties
	It should not involve an impossible or disproportionate effort	Same

4.10.5 Right to restrict processing

While DPD provided for “blocking”, the GDPR strengthened this right by specifically conferring the “ Right to Restrict Processing” upon the data subject. This Article gives data subject the right to restrict processing under certain conditions. Recital 67 explains that these methods could include steps like removing published data from website or temporarily moving the data to another processing system.

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	18	12(b)
About this right	Data subject can restrict processing of data	Data subject is allowed to erase, rectify or block processing of personal data.
Conditions under which the right can be exercised	When accuracy of personal data is contested	Besides accuracy, the DPD also mentions “incomplete nature of data” as grounds for exercising this right.
	When processing is unlawful and data subject opposes erasure and requests restriction of data use	
	When data is no longer needed by controller but is required by data subject for establishment, exercise or defense of legal claims.	

	Data subject objects to processing and the verification by controller of compelling legitimate grounds for processing is ongoing	
Consequences of this enforcement of this right	Controller can store data but not process it	
	Processing can be done only with the data subject's consent; or	
	Processing can be done for establishment exercise or defense of legal claims; or	
	Processing can be done for protecting rights of another natural or legal person ;or	
	It can be done in public interest of Union or Member State.	
Obligations of controller under Art 18	The controller must inform the data subject before the restrictions are lifted.	
Obligations of controller under Art 19	Inform each recipient of personal data about the restriction.	
	This obligation need not be performed if it is impossible to do so or it involved disproportionate effort.	
	Inform data subject about the recipients when requested by the data subject.	

4.10.6 Right to data portability

This right empowers the data subject to receive personal data from one controller and transfer it to another. This gives the data subject more control over his or her own data. The controller cannot hinder this right when the following conditions are met.

Sub-topics in the section	GDPR	DPD
Given in article	20	
Conditions for data transmission	The data must have been provided to the controller by data subject himself; and	
	Processing is based on: Consent; or For performance of contract; and is carried out by automated means	
	Data transfer must be technically feasible	
Format of personal data	It should be in a: Structured Commonly-used Machine readable format	
Time and cost for data transfer	Given in Art 12(3) Should be free of charge Information to be provided within one month. Further extension by two months permissible under certain circumstances.	
Circumstance under which this Right cannot be exercised	When the exercise of the Right prejudices rights and freedom of another individual	
	When processing is	

	necessarily carried out in public interest	
	When processing is necessarily done in exercise of official authority vested in controller	
	When this Right adversely affects the "Right to be forgotten"	

4.10.7 Right to Object

Both DPD and GDPR confer upon the data subject the right to object to processing on a number of grounds. The GDPR strengthens this right . Under GDPR, there is a visible shift from the data subject to the controller as far as the burden of showing " compelling legitimate grounds" is concerned. Under the DPD, when processing is undertaken in public interest or in exercise of official authority or in legitimate interests of third party or controller, the data subject not only has to show existence of compelling legitimate grounds but also that objection is justified. On the other hand, GDPR spares the data subject from this exercise and instead places the onus on the controller of demonstrating that "compelling legitimate grounds" exist such that these grounds override the interests, rights and freedom of the data subject.

GDPR also provides a new ground for objecting to processing. The data subject can object to processing when it is for scientific or historical research or statistical purpose unless such processing is necessary in public interest.

Under the GDPR the data subject must be informed of this right "clearly and separately" and "at the time of first communication with data subject" when processing is done in public interest/exercise of official authority/legitimate interest of third party or controller or for direct marketing purpose. This right can be exercised by automated means in case of information society service.

The DPD also provides that the data subject must be informed of this right if the controller anticipates processing for direct marketing or disclosure of data to third party. It specifically states that this right is to be offered "free of charge". Additionally, it places responsibility upon the Member States to ensure that data subjects are aware of this right.

Sub-topics in the section	**GDPR**	**DPD**

Given in Article	21	14
Conditions under which the right can be exercised during processing	When performance of task is carried out in public interest or in exercise of official authority vested in controller. (Art 6(1)(e)) Exception: If controller demonstrates processing is for compelling legitimate grounds which override interests of data subject For establishment, exercise or defense of legal claims.	Grounds are same but the data subject also has to show existence of compelling legitimate grounds. Processing will cease if objection is justified. Exceptions: Unless provided by national legislation the data subject can object on this ground.
	For legitimate interests of controller or third party (Art 6(1)(f)) Exception: 1. If controller demonstrates processing is for compelling legitimate grounds that override interests of data subject. 2. For establishment, exercise or defense of legal claims.	Same as above

	When data is processed for scientific/historical research/ statistical purpose under Art 89(1) Exception: If processing is necessary for public interest	
	When personal data is used for marketing purpose. Can object at anytime. No exceptions	Same

4.10.8 Rights in relation to automated individual decision making including profiling

This Article empowers the data subject to challenge automated decisions under certain conditions. This is to protect individuals from decisions taken without human intervention.

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	22	15
This right can be exercised when decisions are based:		
	Only on automated processing Including profiling; and	Same
	Produce legal effects or have similarly significant effects on data subject	Same

Conditions under which this right will not be guaranteed		
	For entering into or performance of contract;	Same
	If Member State or Union law authorizes the decision provided it lays down suitable measures for safeguarding data subject's rights, freedoms and legitimate interests; Or	Same
	When decision is based on data subject's explicit consent.	
Controller's obligation	Enforce measures to safeguard rights and freedom and interests	
	Ensure data subject can obtain human intervention, express his point of view, challenge decisions	
Automated decision making will not apply when:	"Special categories of personal data" are to be processed However, if the data subject gives his explicit consent or such processing serves substantial public interest then the restriction can be waived.	

	Concerns a child	

4.11 Security and Accountability

4.11.1 Data protection by design and default

This is another new concept under GDPR. It is a general obligation on the controller to incorporate effective data protection in internal policies and implementation measures. Measures include: minimization of processing, pseudonymisation, transparency while processing, allowing data subjects to monitor data processing etc. The implementation of organizational and technical measures is essential to demonstrate compliance with Regulation.

Sub-topics in the section	**GDPR**	**DPD**
Article	25	
Responsibility of controller when determining means of processing and at the time of processing	Implementation of appropriate technical and organizational measures for data protection	
	Ensure that by default only personal data necessary for purpose of processing is processed	
Means of demonstrating compliance with this Article	Approved certification mechanism may be used. Data minimization Transparency etc.	

4.11.2 Security of personal data

Security of processing is mentioned in the GDPR under Article 32. The controller and processor must implement technical and organizational measures to ensure data security. These may include pseudonymisation, encryption, ensuring confidentiality, restoring availability and access to personal data, regularly testing etc. Compliance with the code may be demonstrated by adherence to Code of conduct and certification mechanism. Further, all processing which is done by a natural person acting under authority of controller or processor can be done only under instructions from the controller.

4.11.3 Notification of personal data breach

This Article provides the procedure for communicating the personal data breach to supervisory authority. If the breach is not likely to result in risk to rights and freedoms of natural persons, then the controller is not required to notify the supervisory authority.

Sub-topics in the section	GDPR	DPD
Given in Article	33	
Responsibility of controller	Report personal data breach to supervisory authority after being aware of it	
Time limit for reporting data breach	Must be reported no later than 72 hours	
In case of delay in reporting	Reasons to be stated	
Responsibility of processor	Notify the controller after being aware of breach	
Description of notification	Describe nature of personal data	
	Name contact details of data protection officer	
	Likely consequences of personal data breach	
	Measures to be taken or proposed to be taken by controller to address the breach or mitigate its possible effect	
When information cannot be provided at same time	Provide it in phases without further undue delay	
For verification of compliance	Controller has to document any personal data breach. It must contain Facts , effects and remedial action taken	

4.11.4 Communication of personal data breach to the data subject

Not only is the supervisory authority to be notified, but data subjects are also to be informed about personal data breaches without undue delay under certain conditions.

Sub-topics in the section	GDPR	DPD
Given in Article	34	
Conditions under which controller is to communicate the breach to data subject	When breach is likely to cause high risk to rights and freedoms of natural persons	
Nature of communication	Must be in a clear and plain language. Must describe the nature of breach. Must Contain at least: Name contact details of data protection officer Likely consequences of personal data breach Measures to be taken or proposed to be taken by controller to address the breach or mitigate its possible effect	
Condition under which communication will not be required	If controller has implemented appropriate technical and organizational measures and these were applied to the affected data. E.g.: encryption	
	Subsequent measures have been taken by controller to ensure there is no high risk	

	If communication involves disproportionate effort. Public communication or similar measures can be undertaken under such circumstances.	
Role of supervisory authority	In case of likelihood of high risk, the authority may require the controller to communicate the breach if the controller has not already done so.	

4.11.5 Data protection impact assessment

This is also known as Privacy Impact Assessment. While DPD provides general obligation to notify the processing to supervisory authorities, the GDPR, taking into account the need for more protection of personal data, has replaced the notification process by different set of mechanisms.

To serve the above purpose, the data protection impact assessment (DPIA) has been provided under this Article.

Sub-topics in the section	**GDPR**	**DPD**
Given in Article	35	
When to carry out assessment	When new technology is used; and Processing is likely to result in high risk to rights and freedoms of natural persons	
	Automated processing including profiling involving systematic and extensive evaluation of personal aspects of natural persons; and When decisions based on such processing produce legal effects	

	Large scale processing of special categories of data or personal data relating to criminal convictions and offences	
	Large scale systematic monitoring of publicly accessible area	
Type of information contained in assessment	Description of processing operations and purpose	
	Assessment of necessity and proportionality of processing operations	
	Assessment of risks to individuals	
	Measures to address risks and demonstration of compliance with Regulation	
Sub-topics in the section	**GDPR**	**DPD**
Topic	Prior Consultation	
Given in Article	36	
When should controller consult supervisory authority	Prior to processing; and DPIA indicates high risk; and In absence of risk mitigation measures by controller	

Data protection officer

GDPR mandates that a person with expert knowledge of data protection law and practice is appointed for helping the controller or processor to comply with the data protections laws. A single data protection officer (DPO) may be appointed by a group of undertakings or where controller or processor is a public authority or body.The DPO must be accessible from each establishment.

Sub Topics in the Section	GDPR	DPD
Article	37	

Situations in which DPO must be appointed	When processing is carried out by public authority or body. Note: Courts acting in judicial capacity are excluded.	
	Core activity involves processing which requires regular and systematic monitoring of data subjects on large scale; or	
	Core activity involves processing of large scale special categories of data and criminal convictions and offences	

Position of Data Protection Officer

The DPO must directly report to the highest management level of the controller or processor. Data subjects may contact the DPO in case of problems related to processing and exercise of rights.

Sub Topics in the Section	GDPR	DPD
Article	38	
Responsibility of controller and processor	Ensure DPO is involved properly and in timely manner	
	Provide DPO with support, resources and access to personal data and processing operations	
	Not dismiss or penalize DPO for performing his task.	
	Ensure independence of working and not give	

	instruction to DPO	

Tasks of Data Protection officer

The DPO must be involved in all matters concerning data protection. He is expected to act independently and advice the controllers and processors to facilitate the establishment's compliance with Regulations.

Sub Topics in the Section	GDPR	DPD
Article	39	
Tasks	Inform and advise the controller or processor and employees over data protection laws	
	Monitor compliance with data protection laws. Includes assigning responsibilities, awareness- raising, staff training and audits	
	Advice and monitor performance	
	Cooperate with supervisory authority	
	Act as point of contact for supervisory authority for processing, prior consultation and consultation on other matter	

4.11.6 European Data Protection Board

For consistent application of the Regulation, the GDPR envisages a Board that would replace the Working Party on Protection of Individuals With Regard to Processing of Personal Data established under the DPD. This Regulation confers legal personality on the Board.

Sub Topics in the Section	GDPR	DPD
Article	68	
Represented by	Chair	

Composition of the Board	Head of one supervisory authority of each Member State and European Data Protection Supervisor or of their representatives. Joint representative can be appointed where Member State has more than one supervisory authority.	
Role of Commission	Right to participate in activities and meetings of the Board without voting rights. Commission to designate a representative for this.	
Functions of the Board	Consistent application of Regulation	
	Advise Commission of level of protection in third countries or international organizations	
	Promote cooperation of supervisory authorities	
	Board is to act independently	

4.11.7 Supervisory Authority

GDPR lays down detailed provisions on supervisory authorities, defining their functions, independence, appointment of members, establishment rules, competence, competence of lead supervisory authority, tasks, powers and activity reports. Such elaborate provisions are absent in DPD.

Sub-topics in this section	GDPR	DPD
Given in Article	Chapter VI, Article 51 -	28

	59	

4.12 Processor

The Article spells out the obligations of a processor and conditions under which other processors can be involved.

Sub Topics in the Section	GDPR	DPD
Article	28	
What kind of processors can be used by controller	● Those which provide sufficient guarantees to implement appropriate technical and organizational measures ● Those which comply with Regulation and Rights	
Obligations of processor in case of addition or replacement of processor	● Not engage another processor without controller's authorization ● In case of general written authorization inform the controller	
Processing shall be governed by	Contract or legal act under Union or Member State law.	
Elements of Contract	● Is binding on processor ● Sets out subject matter and duration of processing ● Nature of processing ● Type of personal data ● Categories of data subjects ● Obligations and Rights of the controller	

Obligations of processor under contract or legal act	Processor shall process under instructions from controller unless permitted under law itself. Controller is to be informed in the latter case.	
	Ensures that persons authorized to process have committed themselves to confidentiality	
	Processor to undertake all data security measures (mentioned under Art 32)	
	Enforces conditions on engaging another processor	
	Assists the controller by appropriate technical and organizational measures	
	Assists controller in compliance with Art 32 to 36	
	Delete or return all personal data to controller at the choice of controller at the end of processing	
	Make information available to controller for demonstrating compliance with obligations. Contribute to audits, inspections etc. Inform the controller if it believes that an instruction infringes the	

	regulation or law.	
Conditions under which a processor can engage another processor	● Same data protection obligations will be applicable to other processor. ● If other processor fails to fulfill data protection obligations, initial processor shall remain fully liable to controller for such performance.	

4.13 Records of processing activities

The controller or processor must maintain records of processing activities to demonstrate compliance with the Regulation. They are obliged to cooperate with and make record available to the supervisory authority upon request. DPD does not contain similar obligations.

Sub Topics in the Section	GDPR	DPD
Article	30	
Obligation of controller or controller's representative	Maintain a record of processing activities	
Information to be contained in the record	Name and contact details of: ● Controller /joint controller / controller's representatives ● Data protection officer	
	Purpose of processing	
	Categories of data subjects and categories of personal data	
	Categories of recipients to whom data has been	

	or will be disclosed	
	Transfers of personal data to third party, identification of third party, documentation of suitable safeguards	
	Expected time duration for erasure of different categories of data	
	Technical and organizational security measures	
Obligation of processor	Maintain a record of processing activities carried out on behalf of controller	
Record maintained by processor shall contain information such as:	Name and contact details of: ● Processor /processor's representative ● Controller /controller's representative ● Data protection officer	
	Categories of processing	
	Data transfer to third party Identification of third party Documentation of safeguards	
	Technical and organizational security measures	
Form in which record is to be maintained	In writing and electronic form	
Conditions under which exemption will apply	● Organizations employing fewer than 250 employees are exempted;	

	● Processing should not cause risk to rights and freedoms of data subjects ● Processing should not be occasional ● Processing should not include special categories of data	

4.14 Code of Conduct

These mechanisms have been provided under GDPR to demonstrate compliance with the Regulation. This is important as the GDPR (under Art 83) provides that adherence to code of conduct shall be one of the factors taken into account for calculating administrative fines. This is not an obligatory provision.

Sub Topics in the Section	GDPR	DPD
Article	40	27
Who will encourage drawing up of code of conduct	● Member States ● Supervisory Authorities ● Commission. Specific needs of micro, small and medium enterprises to be taken into account.	● Member States ● Commissions Does not mention the rest
Who may prepare amend or extend code of conduct	Associations and other bodies representing categories of controller or processors	
Information contained in the code	Fair and transparent processing	
	Legitimate interests of controller	
	Collection of personal data	
	Pseudonymisation	

	Information to public and data subjects	
	Exercise of rights of data subject	
	Information provided to and protection of children and manner in which consent of holders of parental responsibility is obtained	
	Measures under: ● Data protection by design and default ● Controller responsibilities ● Security of processing	
	Notification of data breach to authorities and communication of same to data subjects	
	Data transfer to third party	
	Dispute resolution procedures between controllers and data subjects	
	Mechanisms for mandatory monitoring	
Mandatory monitoring	Code of conduct containing the above information enables mandatory monitoring of compliance by body accredited by supervisory authority. (Art 41)	

4.15 Certification

Like the code of conduct, Certification is a voluntary mechanism that demonstrates compliance with the Regulation. Establishment of data protection certification mechanism and data protection seals and marks shall be encouraged by Member States, supervisory authorities, Boards and Commission. As in case of code of conduct, specific needs of micro, small and

medium sized enterprise ought to be taken into account. DPD does not mention such mechanisms.

Sub Topics in the Section	GDPR	DPD
Article	42	
Who will issue the certificate	Certification bodies or competent supervisory authority on basis of approved criteria.	
Time period during which certification shall be issued	Maximum period of three years. Can be renewed under same conditions.	
Who accredits certification bodies	Competent Supervisory bodies or National accreditation body.	
When can accreditation be revoked	When conditions of accreditation are not or no longer met. OR Where actions taken by certification body infringe this Regulation.	
Who can revoke	Competent supervisory authority or national accreditation body	

4.16 Data Transfer

4.16.1 Transfers of personal data to third countries or international organizations

Chapter V lays down the conditions with which the data controller must comply in order to transfer data for the purpose of processing outside of the EU to third countries or international organizations. The chapter also stipulates conditions that must be complied with for onward transfers from the third country or international organization.

4.16.2 Transfer on the basis of an adequacy decision

Under GDPR, transfer of data can take place after the *Commission decides* whether the third country, territory, specified sector within that third country or international organization ensures adequate level of data protection. This is

called adequacy decision. A list of countries or international organizations which ensure adequate data protection shall be published in the Official Journal of the European Union and on the website by the Commission. Once data transfer conditions are found to be compliant with the Regulation, no specific authorization would be required for data transfer from the supervisory authorities. The commission would decide this by means of an "Implementing Act" specifying a mechanism for periodic review, its territorial and sectoral application and identification of supervisory authorities. Decisions of Commission taken under Art 25(6) of DPD shall remain in force. DPD also provides parameters for the same.

Sub-topics in this section	GDPR	DPD
Given in article	45	25
Conditions apply when transfers take place to	Third country or international organization	International organization not mentioned.
Functions of the commission	Take adequacy decisions	Same
	Review the decision periodically every four years	
	Monitor developments on ongoing basis	
	Repeal, amend or suspend decision	
		Inform Member States if third country doesn't ensure adequate level of protection. Similarly, member state has to inform the Commission.
Functions of Member State		Inform Commission if third country doesn't ensure adequate level of protection.
		Take measures to comply with Commission's decisions
		Prevent data transfer if Commission finds

		absence of adequate level of protection.
Factors, with respect to third country or international organization, to be considered while deciding adequacy of safeguards	Rule of law, human rights, fundamental freedoms, access of public authorities to personal data, data protection rules, rules for onward transfer of personal data to third country or international organization etc.	Circumstances surrounding data transfer operations: nature of data; purpose and duration of processing operation; rule of law, professional rules and security measures in third country; country of origin and final destination; professional rules and security measures;
	Functioning of independent supervisory authorities, their powers of enforcing compliance with data protection rules and powers to assist and advise data subject to exercise their rights.	
	International commitments entered into. Obligations under legally binding conventions.	Same
When adequate level of protection no longer ensues	The Commission, to the extent necessary: repeal, amend or suspend the decision. This is to be done by the means of an implementing act. No retroactive effect to take place	The member state will have to suspend data transfer if Commission finds absence of adequate level of protection.
	Commission to enter into consultation with	Same

	the third country or international organization to remedy the situation	

4.16.3 Transfers subject to appropriate safeguards

This article provides for a situation when the Commission takes no decision. (Mentioned above under **Transfer on the basis of an adequacy decision**). In this case, the controller or processor can transfer data to third country or international organization subject to certain conditions. Specific authorization from supervisory authorities is not required in this context. Procedure for the same has been mentioned.

Sub-topics in this section	GDPR	DPD
Given in article	46	
When can data transfer take place	When *appropriate safeguards* are provided by the controller or processor; AND On condition that data subject enjoys enforceable rights and effective legal remedies for data safety.	
Conditions to be fulfilled for providing *appropriate safeguards* without specific authorization from supervisory authority	Existence of legally binding and enforceable instrument between public bodies or authorities	
	Existence of Binding Corporate Rules	
	Adoption of Standard Protection Clauses adopted by the Commission	
	Adoption of Standard data protection clauses by supervisory authorities and	

	approved by Commission.	
	Approved code of conduct along with binding and enforceable commitments of controller or processor in third country to apply appropriate safeguards and data subject's rights OR Approved certification mechanism along with binding and enforceable commitments of controller or processor in third country to apply appropriate safeguards and data subject's rights.	
Conditions to be fulfilled for providing appropriate safeguards subject to authorization from competent authority	Existence of contractual clauses between: Controller or Processor and Controller, Processor or recipient of personal data (third party)	
	Provisions inserted in administrative arrangements between public authorities or bodies. Provisions to contain enforceable and effective data subject rights.	
	Consistency mechanism to be applied by supervisory authority	
Unless amended, replaced or repealed, authorization to transfer given under DPD will remain valid when:	Third country doesn't ensure adequate level of protection but controller adduces adequate safeguards;	

	or Commission decides that standard contractual clauses offer sufficient safeguards	

4.16.4 Binding Corporate Rules

These are agreements that govern transfers between organizations within a corporate group

Sub-topics in this section	GDPR	DPD
Given in Article	47	
Elements of Binding Corporate Rules	Legally binding	
	Apply to and are enforced by every member of group of undertakings or group of enterprises engaged in joint economic activity. Includes employees	
	Expressly confer enforceable rights on data subject over processing of personal data	
What do they specify	Structure and contact details of group of undertakings	
	Data transfers or set of transfers including categories of personal data , type of processing, type of data subjects affected, identification of third countries	
	Legally binding nature	
	Application of general	

	data protection principles	
	Rights of data subjects Means to exercise those right	
	How the information on BCR is provided to data subjects	
	Tasks of data protection officer etc.	
	Complaint procedure	
	Mechanisms within the group of undertakings, group of enterprises for ensuring verification of compliance with BCR. Eg. Data protection audits Results of verification to be available to person in charge of monitoring compliance with BCR and to board of undertaking or Group of enterprises. Should be available upon request to competent supervisory authority	
	Mechanism for reporting and recording changes to rules and reporting changes to supervisory authority	
	Cooperation mechanism with supervisory authority	
	Data protection training to personnel having access to personal data	
Role of Commission	May specify format and procedures for	

	exchange of information between controllers, processors and supervisory authorities for BCR	

4.16.5 Transfers or disclosures not authorized by Union law

This Article lays down enforceability of decisions given by judicial and administrative authorities in third countries with regard to transfer or disclosure of personal data.

Sub-topics in this section	GDPR	DPD
Given in Article	48	
Article concerns	Transfer of personal data under judgments of courts, tribunals, decision of administrative authorities in third countries.	
When can data be transferred or disclosed	International agreement between requesting third country and member state or union. E.g.: mutual legal assistance treaty	

4.16.6 Derogations for specific situations

This Article comes into play in the absence of adequacy decision or appropriate safeguards or of binding corporate rules. Conditions for data transfer to a third country or international organization under such situations have been laid down.

Sub-topics in this section	GDPR	DPD
Given in Article	49	26

Conditions under which data transfer can take place	On obtaining Explicit consent of data subject after being informed of possible risks	On obtaining unambiguous consent of data subject to the proposed transfer
	Transfer is necessary for conclusion or performance of contract. The contract should be in the interest of data subject. The contract is between the controller and another natural or legal person.	Contractual conditions are same. DPD also includes implementation of pre contractual measures taken upon data subject's request.
	Transfer is necessary in public interest	Same
	Is necessary for establishment, exercise or defense of legal claims	Same
	To protect vital interest of data subject or of other persons where data subject is physically or legally incapable of giving consent	Includes vital interest of data subject but doesn't include "other person". Condition for consent is also not included.
	Transfer made from register under Union or Member State law to provide information to public and is open to consultation by public or person demonstrating legitimate interest.	Same
Conditions for transfer when even the above specific situations are not applicable	Transfer is not repetitive	
	Concerns limited number of data subjects	
	Necessary for compelling legitimate	

	interests pursued by controller	
	Legitimate interests are not overridden by interests or rights and freedoms of data subject	
	Controller has provided suitable safeguards after assessing all circumstances surrounding data transfer	
	Controller to inform supervisory authority about the transfer	
	Controller to inform data subject of transfer and compelling legitimate interests pursued	
		Member may authorize transfer personal data to third country where controller adduces adequate safeguards for protection of privacy and fundamental rights and freedoms of individuals

4.17 International cooperation for protection of personal data

This Article lays down certain steps to be taken by Commissions and supervisory authorities for protection of personal data.

Sub-topics in this section	GDPR	DPD
Given in Article	50	

Steps will include	Development of international cooperation mechanisms to facilitate enforcement of legislation for protection of personal data	
	Provide international mutual assistance in enforcement of legislation for protection of personal data	
	Engage relevant stakeholders for furthering international cooperation	
	Promote exchange and documentation of personal data protection legislation and practice	

4.18 Remedies, Liability and Compensation

4.18.1 Right to lodge complaint with a supervisory authority

This article gives the data subject the right to seek remedy against unlawful processing of data. GDPR strengthens this right as compared to the one provided under DPD.

Sub-topics in this section	GDPR	DPD
Given in Article	77	28(4)
Right given	Right to lodge complaint	Under GDPR the data subject has been conferred the "right" specifically. This is not so in DPD. DPD merely obliges the supervisory authority to hear claims concerning rights and freedoms.
Who can lodge complaint	Data subject	Any person or association representing

		that person
Complaint to be lodged before	Supervisory authority in the Member State of habitual residence, place of work or place of infringement	Supervisory authority
When can the complaint be lodged	When processing of personal data relating to data subject allegedly infringes on Regulation	When rights and freedom are to be protected while processing. When national legislative measures to restrict scope of Regulations is adopted and processing is alleged to be unlawful.
Accountability	Complainant to be informed by Supervisory authority on progress and outcome of complaint and judicial remedy to be taken up	Complainant to be informed on outcome of claim or if check on unlawfulness has taken place

4.18.2 Right to an effective judicial remedy against supervisory authority

The concerned Article seeks to make supervisory authorities accountable by bringing proceedings against the authority before the courts. GDPR gives a specific right to the individual. DPD under Article 28(3) merely provides for appeal against decisions of supervisory authority in the courts.

Sub-topics in this section	GDPR	DPD
Given in Article	78 (1)	
Who has the right	Every natural or legal person	
When can the right be exercised	Against legally binding decision of supervisory authorities concerning the complainant	

Sub-topics in this section	GDPR	DPD
Given in Article	78(2)	

Who has the right	Data subject	
When can the right be exercised	When the competent supervisory authority doesn't handle the complaint Or Doesn't inform data subject about progress / outcome of complaint within 3 months	

The jurisdiction of court will extend to the territory of the Member State in which the supervisory authority is established (GDPR Art 78(3)). The supervisory authority is required to forward proceedings to the court if the decision was preceded by the Board's decision in the consistency mechanism. (GDPR 78(4))

4.18.3 Right to effective judicial remedy against a controller or processor

The data subject has been conferred with the right to approach the courts under certain circumstance. The GDPR confers the specific right while DPD provides for judicial remedy without using the word "right".

Sub-topics in this section	GDPR	DPD
Given in	Art 79	Recital 55
Right can be exercised when:	1. Data has been processed; and 2. Processing Results in infringement of rights; and 3. Infringement is due to non compliance of Regulation	Similar provisions provided under DPD: When controller fails to respect the rights of data subjects and national legislation provides a judicial remedy. Processors are not mentioned.
Jurisdiction of the courts	Proceedings can be brought before the courts of Member States wherein: 1. Controller or	

	processor has an establishment Or 2. Data Subject has habitual residence	
Right cannot be exercised when	1. The controller or processor is a public authority of Member State And 2. Is exercising its public powers	

4.18.4 Right to compensation and liability

GDPR enables a person who has suffered damages to claim compensation as a specific right. DPD merely entitles the person to receive compensation. Although Liability provisions under GDPR and DPD are similar, the liability under GDPR is stricter as compared to DPD. This is because DPD exempts the processor from liability but GDPR does not. For example, DPD imposes liability on controllers only.

Sub-topics in this section	GDPR	DPD
Given in Article	82	23
Who can claim compensation	Any person who has suffered material or non material damage	Similar provisions. But DPD doesn't mention "material or non-material damage" specifically.
Right arises due to	Infringement of Regulation	Same
Right granted	Right to receive compensation	Same
Compensation has to be given by	Controller or processor	Compensation can be claimed only from controller
Liability of controller arises when	Damage is caused by processing due to infringement of	Same

	regulation	
Liability of processor arises when	1. Processor has not complied with directions given to it under Regulation OR 2. Processor has acted outside or contrary to lawful instructions of controller	
Exemptions to controller or processor from liability	If there is proof that they are not responsible	Exemption for controller is same
Liability when more than one controller or processor cause damage	Each controller or processor to be held liable for entire damage	

4.19 General conditions for imposing administrative fines

GDPR makes provision for imposition of *administrative fines* by supervisory authorities in case of infringement of Regulation. Such fines should be effective, proportionate and dissuasive. In case of minor infringement, "reprimand may be issued instead of a fine"[1]. Means of enforcing accountability of supervisory authority have been provided. If Member state law does not provide for administrative fines, then the fine can be initiated by the supervisory authority and imposed by courts. However, by 25 May 2018, Member States have to adopt laws that comply with this Article.

Sub-topics in this section	GDPR	DPD
Given in Article	83	
Who can impose fines	Supervisory Authority	
Fines to be issued against	Controllers or Processors	
Parameters to be taken into account while determining administrative fines	Nature, gravity and duration of infringement and Nature scope or purpose of processing and	

[1] Recital 148 , GDPR

	Number of data subjects affected and Level of damage suffered	
	Intentional or negligent character of infringement	
	Action taken by controller or processor to mitigate damage suffered by data subjects	
	Degree of responsibility of con controller or processor. Technical and organizational measures implemented to be taken into account.	
	Relevant previous infringement	
	Degree of cooperation with supervisory authority	
	Categories of personal data affected	
	Manner in which supervisory authorities came to know of the infringement and Extent to which the controller or processor notified the infringement	
	Whether corrective orders of supervisory authority under Art 58(2) have been issue before and complied with	
	Adherence to approved code of conduct under Art 40 or approved certification mechanisms under Art 42	
	Other aggravating or	

	mitigating factors like financial benefits gained losses avoided etc.	
If infringement is intentional or due to negligence of processor or controller	Total amount of administrative fine to not exceed amount specified for gravest infringement	
Means checking power of supervisory authority to impose fines	Procedural safeguards under Member State or Union law. Including judicial remedy and due process	

Article 83 splits the amount of administrative fines according to obligations infringed by controllers, processors or undertakings. The first set of infringements may lead to imposition of fines up to 10,000,000 EUR or 2% of total worldwide turnover.

Sub-topics in this section	GDPR	DPD
Article	83(4)	
Fine imposed	Up to 10,000,000 EUR or in case of undertaking, 2% of total worldwide turnover of preceding financial year, whichever is higher	
Infringement of these provisions will cause imposition of fine (Provisions infringed)	Obligations of controller and processor under:	
	Art 8 Conditions applicable to child's consent in relation to information society services	
	Art 11 Processing which does not require identification	
	Art 25 to 39	

	General obligations , Security of personal data , Data Protection impact assessment and prior consultation	
	Art 42 Certification	
	Art 43 Certification bodies	
	Obligations of certification body under: Art 42 Art 43	
	Obligations of monitoring body under: Art 41(4)	

Second set of infringements may cause the authority to impose higher fines up to 20,000,000 EUR or 4% of total worldwide turnover.

Sub-topics in this section	GDPR	DPD
Article	83(5)	
Fine imposed	Up to 20,000,000 EUR or in case of undertaking, 4% of total worldwide turnover of preceding financial year, whichever is higher	
Infringement of provisions that will cause imposition of fine (Provisions infringed)	Basic principles for processing and conditions for consent under:	
	Art 5 Principles relating to processing of personal	

	data	
	Art 6 Lawfulness of processing	
	Art 7 Conditions for consent	
	Art 9 Processing of special categories of personal data	
	Data subject's rights under: Art 12 to 22	
	Transfer of personal data to third country or international organization under: Art 44 to 49	
	Obligations under Member State law adopted under Chapter IX	
	Non Compliance with supervisory authority's powers under provisions of Art 58:	
	Imposition of temporary or definitive limitation including ban on processing (Art 58 (2)(f))	
	Suspension of data flows to third countries or international organization (Art 58(2) (j))	
	Provide access to premises or data processing equipment and means (Art 58 (1) (f))	

4.20 Penalties

Article 84 makes provision for penalties in case of infringement of Regulation. The penalties must be effective, proportionate and dissuasive.

Sub-topics in this section	GDPR	DPD
Given in Article	84	
When will penalty be imposed	In case of infringements that are not subject to administrative fines	
Who imposes them	Member State	
Responsibility of Member State	To lay down the law and ensure implementation. To notify to the Commission, the law adopted, by 25 May 2018	
