GDPR Requirements Analysis Quick Reference Guide

DCAM™ Framework Mapping

The 48 GDPR Data Management requirement statements were mapped to the DCAM™ Framework at either the 2 digit Capability or 3 digit Sub Capability level. The mapping resulted in 172 pairings across 27 unique capabilities. The GDPR Requirement Count total is for the number of GDPR requirements that aligned to each item. This allows a quick reference and focus on the capabilities that are required for the Data Management function to support GDPR compliance.

This analysis can be used by the CDO as the basis for a GDPR compliance checklist for the required support from the Data Management function. While not a direct correlation to criticality, those capabilities with higher GDPR requirement alignment counts might infer prioritization if you are building your capability or working to close gaps in your existing capabilities.

Table: DCAM Framework Mapping Summary

Capability Category	DCAM™ Capability / Sub Capability	GDPR Req Ct
Data Content	4.2.1. Authorized data domains have been identified and inventoried	11
	4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use	11
	4.2.5. Data classifications are defined and assigned	12
	4.4.3. Data requirements are captured and prioritized	11
	5.1. Identify the data	12
	5.2. Define the data	12
	5.3. Govern the data	12
	8.2. A Data control environment supports the data management lifecycle (Lineage & Data Flow)	11
Governance Alignment	4.7. Cross-organizational enterprise data governance is aligned (1)	12
	6.3. Data storage management strategy defined and governed	2
	8.3. Control environment ensures the discipline of data management is operating collaboratively with cross-organizational Control Functions	5
	4.6.2. Data storage governance is established	3
	4.6.3. Data distribution governance is established	3
Data Management Policy	4.3. Policy and standards are written and approved	12
	4.5.2. Policy and standards are enforceable and auditable	7
Technology Architecture	6.1. Technology architecture is defined and governed	9
	6.2. Data technology tool stack is identified and governed	9
Data Management Program	3.5.1. Internal communication plans have been created, channels established, plans published and approved	1
	3.5.2. Communication plans with regulators bodies are created and approved	2
	3.6.2. Issue identification, prioritization, escalation and conflict resolution are defined and operational	4
	4.4.4. Escalation procedures are developed and documented	1
	4.5.1. Project review and approval processes are established	1
	4.5.4. Formal training programs have been designed and implemented	1
Data Quality	7.1. Data Quality program is established	2
	7.2. Quality of existing stores of data are identified and assessed	2
	7.3.The data quality roles and responsibilities have been communicated	2
Summary Review	8.1. A data control environment is established and operational	2

Supporting Documents

General Data Protection Regulation (GDPR): The Role of Data Management - a report of the EDM Council GDPR Best Practice Work Group

https://c.ymcdn.com/sites/edmcouncil.site-ym.com/resource/resmgr/featured_documents/REG_GDPR_WG_BP_v1.10.4.pdf

EDMC GDPR Requirements Detailed Analysis - the full GDPR requirements analysis with data and Data Management Impacts, requirements, and DCAM™ Capability Framework alignment.

https://c.ymcdn.com/sites/edmcouncil.site-ym.com/resource/resmgr/featured_documents/REG_GDPR_Reqmt_Detail_v2.0.pdf

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Data Subject Rights						
Transparency and Information Rights	Article 12(1) & (7) Article 13 Article 14 Article 23 Recital: 39, 58 – 62, 78, 100	To ensure that personal data are processed fairly, data controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data.	Privacy notices. Obligation to provide precise transparent explanation of the data collected prior to the processing of the data. Data from a third party - how notices are provided.	Data Governance: policy for and approval of in-scope data inclusive of data captured without visibility to the data subject Data Content: identify location and source (data flow and/or lineage); metadata to record location, source, transformation; business logic to identify in-scope data subjects; data element to flag in-scope data subjects Data Collaboration: management of the customer / employee data (and other in-scope data) - alignment with other ecosystem policies (privacy, compliance, etc.)	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.5.2. Policy and standards are enforceable and auditable 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 8.2. A Data control environment supports the data management lifecycle 8.3. Control environment ensures that the discipline of data management is operating collaboratively with cross-organizational Control Functions.	Policy Implications: Data Management Policy Data Elements (DEs) in Scope - Existing Design Guidelines: Master Data Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Business logic Policy Implications: Ecosystem
Right of Access	Article 12(1) – (6) Article 15 Article 23 Recital: 63, 64, 65	Data subjects have the right to obtain a copy of their personal data. Additionally, data subjects are entitled to a range of information relating to the data (such as their other rights and applicable retention periods.)	In Europe there is an existing right to contact data controller and ask for their data to be provided - slightly modified with a one month turnaround time - request can be made free of charge (repetitive requests may be charged-repetition is undefined) and may result in mass campaigns requesting data - can get a two month extension if the request is complex or high volume - obligation to inform consumer of delay	Data Content: new data fields to record the process and execution of the data request by data subject Data Collaboration: data provisioning process; format of information delivered to data subject with secure delivery	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 6.2. Data technology tool stack is identified and governed	Data Elements (DEs) in scope - Additions Design Guidelines: Data Provisioning Format

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Rectification, Erasure and Restriction of Processing	Article 4 (2) - (3) Article 12(1) - (6) Article 16 Article 17 Article 18 Article 19 Article 21 Article 23 Recital: 65, 66, 67, 69, 70, 71	Data subjects have the right to have their personal data corrected where it is inaccurate or incomplete. Additionally, in certain circumstances, the data subject can require the data controller to erase or restrict data and processing respectively.	Other data subject rights - overlapping rights - individuals can take measures to correct data or restrict processing - right to be forgotten relatively restricted - request to stop direct marketing	Data Governance: data retention policy and plan Data Content: identify location and source (data flow and/or lineage); metadata to record location and source; controls and process processing pause Data Collaboration: data provisioning process; 3rd party data sharing agreement with erasure requirement; 3rd party notification of erasure request; execution of data erasure for data subject request and/or retention policy	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.5.2. Policy and standards are enforceable and auditable 4.6.2. Data storage governance is established 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 6.2. Data technology tool stack is identified and governed 6.3. Data storage management strategy defined and governed 8.2. A Data control environment supports the data management lifecycle	Policy Implications: Data Retention Policy Design Guidelines: Pause Control and Process Policy Implications: Ecosystem Data Elements (DEs) in Scope - Existing Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Design Guidelines: Data Erasure
Profiling & Automated Individual Decisions	Article 4 (4) Article 12(1) - (5) Article 22 Article 23 Recital: 15, 24, 60, 63, 71, 72, 73, 91	Data subjects have the right not to be subject to profiling that results in decisions that significantly affect them without the ability to ask for a human review of that decision. This right is subject to limited exemptions, such as where the explicit consent of the data subject has been obtained. The data subject will be able to require that the data controller applies “human intervention” to such processing.	Additional rights if automated processing is being undertaken, algorithms that make decisions without human intervention - in notice the auto processing must be flagged - individual can request a human to review the decision - definitions of profiling is a bit sticky if this generates new data it must be captured and communicated	Data Content: identify location and source (data flow and/or lineage), source, and business rules for auto processing; metadata to record location, source and auto processing rules; controls and process for human intervention; data elements to record transaction including human intervention action and date	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.4.3. Data requirements are captured and prioritized 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 6.2. Data technology tool stack is identified and governed 8.2. A Data control environment supports the data management lifecycle	Data Flow or Lineage guideline Data Elements (DEs) in scope - Additions Metadata Model Additions Design Guidelines: Human Intervention Policy Implications: Ecosystem

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Data Portability	Article 12(1) - (6) Article 20 Article 23 Recital: 68, 73, 156	The right to data portability permits the data subject to receive from the data controller a copy of his or her personal data in a commonly used machine-readable format, and to transfer their personal data from one data controller to another or have the data transmitted directly between data controllers.	Facilitate data liquidity allowing individuals to take their data set to another provider - overlaps with right to access - commonly used machine readable format - data subject can instruct direct provision between entities Types of data a portability request covers: Data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.) Observed data provided by the data subject by virtue of the use of the service or the device. They may for example include a person's search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device. Article 29 working party guidance further states: "In contrast, inferred data and derived data are created by the data controller on the basis of the data 'provided by the data subject'". – these data types would not be in scope of the portability request.	Data Governance: policy for and approval of in-scope data (is all the in-scope data related to customer Master Data? if yes, impacts the governance process) Data Content: identify location and source (data flow and/or lineage); metadata to record location and source; business logic to identify in-scope data subjects; data element to flag in-scope data subjects Data Collaboration: management of the customer Master Data; data provisioning process to 3rd party (format, secure, etc.)	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.5.2. Policy and standards are enforceable and auditable 4.6.3. Data distribution governance is established 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 6.2. Data technology tool stack is identified and governed 8.2. A Data control environment supports the data management lifecycle	Data Elements (DEs) in Scope - Existing Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Design Guidelines: 3rd Party Provisioning Data Provisioning Format

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Data Handling Rights						
Purpose Limitation & Data Minimisation	Article 5(1) Article 25 (2) Recital: 15, 26, 32, 38, 40, 45, 47, 50, 51, 52, 53, 57, 78, 156	Purpose limitation and data minimisation are fundamental principles of data protection. Essentially, they stipulate that personal data should be collected only for specified and legitimate purposes, and that the data are used only in line with those purposes.	How is data handled internally in the organization - much is not new - even where quite mature privacy programs in place there is still lack of clarity Specified, explicit, and legitimate use of data - need to control the use of data to those purposes - only collect what is required	Data Governance: policy for and approval of in-scope data (is all the in-scope data related to customer Master Data? if yes, impacts the governance process) Data Content: identify location and source (data flow and/or lineage); metadata to record location, source, defined purpose of data, access control; business logic to identify in-scope data subjects; data element to flag in-scope data subjects Data Collaboration: management of the customer Master Data; data provisioning process; execution of data retention policy	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.5.2. Policy and standards are enforceable and auditable 4.6.2. Data storage governance is established 4.6.3. Data distribution governance is established 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 6.2. Data technology tool stack is identified and governed 8.2. A Data control environment supports the data management lifecycle	Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Business Logic Policy Implications: Ecosystem Purpose of Processing Standard Categories Policy Implications: Data Retention Policy

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Data Quality & Proportionality	Article 5(1) Recital: 59, 50, 57, 65, 156	Data quality and accuracy is a core principle of data protection. It requires that data controllers hold accurate personal data on data subjects. To this end, any inaccurate data should be corrected without delay.	Two separate elements - 1) straightforward requirements for personal data to be accurate, complete and current; 2) deleting personal data once no longer required	Data Quality: rules, measurement, reporting, issue management, root cause analysis, remediation of in-scope data Data Content: identify location and source (data flow and/or lineage); metadata to record location, source, and deletion trigger; business logic to identify in-scope data subjects; data element to flag in-scope data subjects; individual data element retention schedule (physical and electronic) (legal/regulatory and business process perspective) Data Collaboration: execution of data retention policy	3.6.2. Issue identification, prioritization, escalation and conflict resolution are defined and operational 4.2.1. Authorized data domains have been identified and inventoried 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.4.4. Escalation procedures are developed and documented 4.6.2. Data storage governance is established 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.2. Data technology tool stack is identified and governed 6.3. Data storage management strategy defined and governed 7.1. Data Quality program is established 7.2. Quality of existing stores of data are identified and assessed 7.3.The data quality roles and responsibilities have been communicated 8.2. A Data control environment supports the data management lifecycle	Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Business Logic Policy Implications: Ecosystem DQ Rules Unique to GDPR Policy Implications: Data Retention Policy

Thematic Area Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Legal Basis for Processing Personal Data	Articles 6 Article 7 Recital: 4, 8, 10, 16, 17, 19, 21, 40-48, 73, 109	Having a legal basis for the processing of personal data is a basic principle of data protection. The most frequently used legal bases for processing personal data are the data subject's consent, the data controller's legitimate interests, or necessity in the context of a contract with the data subject.	You have to be clear in your basis of processing - different basis for processing data - consent, legitimate interest; vital interest The defined Legal Basis for processing are defined in 6(1)(a), 6(1)(b), 6(1)(c), 6(1)(d), 6(1)(e), and 6(1)(f)	Data Content: identify location and source (data flow and/or lineage); metadata to record location, source, basis of processing, and controls to confine the processing basis; business logic to identify in-scope data subjects; data element to flag in-scope data subjects, processing purpose and consent evidence Data Collaboration: execution of the controls to confine the processing basis	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 6.2. Data technology tool stack is identified and governed 8.2. A Data control environment supports the data management lifecycle	Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Business Logic Design guidelines for legal basis for processing
Sensitive Data (Special Categories of Data)	Article 9 Article 10 Recital: 10, 32, 38, 50, 51, 52, 53, 54	Certain sensitive categories of personal data are generally not allowed to be processed unless a specified exemption applied. The most frequently used exemptions are processing based on the data subject's explicit consent, or necessary for employment.	Special categories - human rights angles In terms of the basis of processing - in vast majority of instances explicit consent is required - what is difference between unambiguous and explicit - explicit is a higher level - very clear and in writing or similar evidence - any data related to a living individual - data that can be used to discriminate Conditions for special categories of data are defined in 9(2)(a), 9(2)(b), 9(2)(c), 9(2)(d), 9(2)(e), 9(2)(f), 9(2)(g), 9(2)(h), 9(2)(i), and 9(2)(j)	Data Content: identify location and source (data flow and/or lineage); metadata to record location, source, sensitive data flag, basis of processing, and consent; business logic to identify in-scope data subjects; data element to flag in-scope data subjects, condition for special category, basis for processing, evidence of consent	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 6.2. Data technology tool stack is identified and governed 8.2. A Data control environment supports the data management lifecycle	Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Business Logic Policy Implications: Ecosystem

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Controller - Processor Relationship	Article 28 Recital: 48, 74, 78 – 82, 95	Where outsourcing personal data to a service provider (whether to a third party or an affiliate within the company group), the Business responsible for the data must use only data processors that provide sufficient guarantees to secure the personal data.	The entity that is in charge is the Data Controller - the processor is acting on behalf of the Controller Controller determines the purposes and use of data - notice -- consent - etc. Obligations on the data processors to maintain security and sometimes in breach processes	Data Governance: establish appropriate data management policies Data Content: identify location and source (data flow and/or lineage); metadata to record location, source, and controls to secure data; business logic to identify in-scope data subjects; data element to flag in-scope data subjects Data Collaboration: (Primary accountability with the reporting control function) engagement with the in-scope data supply chain for breach identification; support root cause analysis of breach and remediation	3.6.2. Issue identification, prioritization, escalation and conflict resolution are defined and operational 4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.5.2. Policy and standards are enforceable and auditable 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 7.1. Data Quality program is established 7.2. Quality of existing stores of data are identified and assessed 7.3.The data quality roles and responsibilities have been communicated 8.2. A Data control environment supports the data management lifecycle 8.3. Control environment ensures the discipline of data management is operating collaboratively with cross-organizational Control Functions	Policy Implications: Data Management Policy Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Business Logic Policy Implications: Ecosystem

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
International Data Transfers (Cross Border)	Article 44 Article 49 Recital: 101 – 116, 168	Before transferring personal data to an entity located in a jurisdiction not deemed to have adequate data protection, the Business needs to ensure either recognised adequate safeguards are in place (e.g., model contracts, BCRs) or a derogation applies (e.g., the explicit consent of the data subject has been obtained).	This has not been substantially changed by GDPR - EU looks at the privacy regime as the 'gold standard" - if you move data outside their regime it must be covered by contract with receiving entity, approval by regulator of receiving jurisdiction, other mechanism including consent	Data Governance: establish appropriate data management policies Data Content: identify location and source (data flow and/or lineage); metadata to record location, source, consent, and controls for cross border movement; business logic to identify in-scope data subjects; data element to flag in-scope data subjects Data Collaboration: engagement with the in-scope data supply chain; execute controls for cross border movement; cross border provisioning process including secure delivery, contract and data delivery agreement	4.2.1. Authorized data domains have been identified and inventoried 4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.5.2. Policy and standards are enforceable and auditable 4.6.3. Data distribution governance is established 4.7. Cross-organizational enterprise data governance is aligned (1) 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 6.2. Data technology tool stack is identified and governed 8.2. A Data control environment supports the data management lifecycle 8.3. Control environment ensures the discipline of data management is operating collaboratively with cross-organizational Control Functions	Policy Implications: Data Management Policy Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Business Logic Policy Implications: Ecosystem
Training						
Training Programme	Article 39 Recital: 81	Periodic general and role-based training should be provided to all employees handling personal data.	Operational in nature - less regulatory - underlying sense of accountability - this tends to be already baked into processes of financial service organizations	Data Collaboration: education of supply chain business and technical data stewards; evidence of training Data Governance: education fo audit to GDPR requirements	3.5.1. Internal communication plans have been created, channels established, plans published and approved 4.5.2. Policy and standards are enforceable and auditable 4.5.4. Formal training programs have been designed and implemented	Education content outline

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Accountability and Governance						
DPOs, Compliance & Mutual Assistance	Article 37 Article 39 Recital: 77	Under the GDPR, the role of Data Protection Officers has been formalised. This means that, in certain circumstances, companies will need to appoint a Data Protection Officer with a specified role.	Requirement to appoint a Data Protection Officer - attributes, job protection, level of independence with reporting lines to SR Mgmt	N/A	N/A	N/A
Records of Processing Activities	Article 30 Recital: 82	Companies must record certain details on their personal data processing activities. This obligation applies to both data controllers and data processors.	Effectively every Data Controller and Processor must have a written record to cover (a list of items) that must be provided to regulator on request	Data Collaboration: provisioning of metadata, lineage, consent evidence	8.1. A data control environment is established and operational	N/A

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Security						
Security of Processing	Article 32 Recital: 78, 79, 81, 83, 84	The GDPR requires all companies to institute appropriate technical and organisational measures to protect the personal data they handle.	Underlying security requirement is not very different from Data Protection Directive of 1995 - discussion around pseudo anonymization - of data - not changing how data should be handled - if data is anonymized - then it is no longer personal data - if not, it is personal data	Data Governance: establish appropriate data management policies; approve the data targeted for anonymization - alignment to Security policy Data Content: identify location and source (data flow and/or lineage); metadata to record location, source, anonymization, and controls for anonymization and access; business logic to identify in-scope data subjects; data element to flag in-scope data subjects Data Collaboration: execute the anonymization process	8.1. A data control environment is established and operational	Policy Implications: Data Management Policy Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Business Logic Design Guidelines: Anonymization Policy Implications: Ecosystem
Breach Notifications to Data Protection Authorities	Article 33 Recital: 85, 87, 88	Data controllers will be required to notify a Data Protection Authority of personal data breaches in certain instances. Similarly, a data processor is obliged to notify the data controller in the event of a personal data breach.	Requirement that you notify appropriate authority within 72 hours - clock starts ticking from point of awareness	Data Collaboration: engagement with the in-scope data supply chain for breach identification; alignment with the escalation policy of the organization	3.5.2. Communication plans with regulators bodies are created and approved 3.6.2. Issue identification, prioritization, escalation and conflict resolution are defined and operational 4.3. Policy and standards are written and approved 4.7. Cross-organizational enterprise data governance is aligned (1) 8.3. Control environment ensures the discipline of data management is operating collaboratively with cross-organizational Control Functions	N/A

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Breach Notifications to Data Subjects	Article 34 Article 23 Recital: 86	Data controllers may be required to notify data subjects in the event of a breach of personal data in certain instances.	Risk based - if there is risk to the individual then you must notify the data subject	Data Content: identify location and source (data flow and/or lineage); metadata to record location, source; business logic to identify in-scope data subjects; data element to flag in-scope data subjects Data Collaboration: engagement with the in-scope data supply chain for breach identification; alignment with the escalation policy of the organization	3.5.2. Communication plans with regulators bodies are created and approved 3.6.2. Issue identification, prioritization, escalation and conflict resolution are defined and operational 4.3. Policy and standards are written and approved 4.7. Cross-organizational enterprise data governance is aligned (1) 8.3. Control environment ensures the discipline of data management is operating collaboratively with cross-organizational Control Functions	Design Guidelines: Data Flow and/or Lineage Data Elements (DEs) in scope - Additions Metadata Model Additions Business Logic Policy Implications: Ecosystem
Change Management						
Data Protection by Design & Default	Article 25 Recital: 78, 108	Companies are required to implement data protection by design (e.g., when creating new products, services or other data processing activities) and by default (e.g., data minimisation).	Principals - evidence in the CM processes and SDLC that these privacy principles are inherent in the default build	Data Content: metadata and lineage/data flow maintenance Data Collaboration: engagement with the in-scope data supply chain (internal and external) to participate in change that impacts the data	4.2.4. Unique and precise data identification schemes and methodologies have been defined, applied and are in use 4.2.5. Data classifications are defined and assigned 4.3. Policy and standards are written and approved 4.4.3. Data requirements are captured and prioritized 4.5.1. Project review and approval processes are established 5.1. Identify the data 5.2. Define the data 5.3. Govern the data 6.1. Technology architecture is defined and governed 8.2. A Data control environment supports the data management lifecycle	N/A

Thematic Area / Component	GDPR Reference	Description	Work Group Commentary	DM Capability Description	DCAM V1.2.2 Alignment	DM Specific Guidance
Data Protection Impact Assessment (DPIA)	Article 35 Recital: 84, 90-95	Where certain processing of personal data (particularly using new technologies) is planned, data controllers will need to carry out a Data Privacy Impact Assessment ("DPIA"). DPIAs must include certain specific information as set out in the GDPR.	Important distinction - privacy impact assessment processes exist - where there is no data processing - there is an assessment of the privacy risk - if the data controller thinks there is new high risk processes - then must review and possibly notify the regulator	N/A	N/A	N/A
Prior Consultation	Article 36 Recital: 96	Depending on the outcome of the DPIA, data controllers may need to consult the relevant supervisory authority on the planned data processing activities.	Process to engage the relevant DPA if DPIA determines high risk	N/A	N/A	N/A
Audit						
Audit Programme	N/A – industry practices only	To provide enhanced assurance concerning privacy and data protection controls, companies should establish a robust internal audit programme to provide periodic independent review.	Driven by accountability principle in GDPR but not specifically required	N/A	N/A	N/A

(1) 4.7. Cross-organizational enterprise data governance - has four defined Sub Capabilities. Due tox differences between governance and policy structures across organizations a review of each Sub Capability is recommended to determine, which policy categories align to this GDPR requirement.