General Data Protection Regulation (GDPR): The Role of Data Management

Enterprise Data Management Council
Best Practice Program

May 2018

Prologue

About the EDM Council & Best Practice Program

The EDM Council is a global organization, with over 200 member organizations from the US, Canada, UK, Europe, South Africa, Japan, Asia, Singapore and Australia, with over 200 organizations and 7,000 data management professionals as members.

The EDM Council provides a venue for data professionals to interact, communicate, and collaborate on the challenges and advances in data management as a critical organizational function. The Council provides research, education and exposure to how data, as an asset, is being curated today, and a vision of how it must be managed in the future.

EDM Council members work collaboratively to define and publish best practice for effective Data Management. All Best Practice work is grounded in the ***WHAT*** - essential principles found in the Data Management Capabilities Assessment Model (DCAM™). The Best Practice Program objective is to develop the ***How*** - documenting the experiences of data management practitioners to support the development and refinement of standard Data Management processes and tools across the full range of capabilities.

The Council also conducts a biennial benchmarking study as a baseline for evaluating progress, publishes a glossary of data management concepts to support stakeholder communication and engages with global regulators to promote more effective public/private partnerships.

About the GDPR Work Group

Mid 2017 the Council held a GDPR webinar briefing for all members to level set basic understanding of the regulation. The forum was also an open invitation for representatives from member organizations to join a Work Group to develop a best practice recommendation for the role of data management in GDPR compliance.

A Work Group was formed that contains approximately 40 members representing all aspects of the industry (GSIBs, SIFIs, buy side, sell side, geographic, consultants, vendors). See appendix for a complete list of participating members.

The project objective was to assess actual member organization experience for development of best practice for the Data Management function to support compliance with GDPR.

Mark McQueen, EDMC Senior Advisor-Best Practice & Process Design, led the Work Group facilitation and serves as scribe of this report. Simon McDougall, Managing Director and global lead of the Privacy and Data Protection Practice for *Promontory Financial Group*, provided specific subject matter expertise on the GDPR legislation.

The first step was to level set an understanding of the GDPR legislation. With a grounding of the requirements of the legislation, the Work Group then went through a logical analysis of the requirements as follows:

- Implications for data and the Data Management function
- Identified data and Data Management function requirements
- Alignment of requirements to the DCAM™ Framework
- Identify Best Practice “Opportunities” to provide specific guidance to support compliance with the regulation

The following is a report of the findings of the Work Group. There will be an ongoing activity to collect best practice aligned to the identified areas for Best Practice Opportunities. As these are developed they will be updated in this report or related materials.

Table of Contents

Executive Summary

The GDPR requires any business that stores and manages personal data on behalf of people in the European Union (EU) (e.g. prospects, customers and/or employees) to handle this information in a transparent and structured manner. The biggest misconception about GDPR is that it is only a EU jurisdiction legislation and therefore only requires compliance by EU businesses. The reality is that **it applies globally to any organization offering goods or services into the European Union.**

Recognizing the global reach and impact of the GDPR, this work was designed to provide several practical deliverables to the EDM Council member organizations.

- Create a basic understanding of the regulation and the role of the Data Management function to support compliance.
- Identify requirements for data and the Data Management function.
- Align the requirements to the EDM Council DCAM™ Framework - providing a compliance roadmap specific to the Data Management function of an organization.
- Leverage member organization experience for development of best practice for the Data Management function to support compliance with GDPR.

The concepts and analysis presented in this paper and supporting materials are intended to communicate value to all organizational stakeholders impacted by GDPR (data management professionals, business executives, executive leadership, and regulatory compliance practitioners).

Key Observations

- GDPR is not a Data Management legislation, but, the Data Management control function will be needed to support the execution of the legislation - giving the business and the data subject (e.g. prospects, customers and/or employees) various obligations and rights around the management of personal data.
- Accountability for GDPR compliance is a Privacy activity. Most organizations already have a control function accountable for Privacy. How this is structured and the hierarchy of the organizations varies significantly across the industry. While there are some limited instances where the Privacy activity has been aligned to the Data Management function, that is not the norm.
- The Chief Data Officer (CDO) and the Data Management function provide support to the Privacy control function accountable for GDPR compliance and the business units who must manage privacy within their business process.
- If the DCAM™ Framework has been adopted and an effective operating level has been achieved, the foundation for supporting the data and Data Management requirements of GDPR compliance is largely in place. A challenge is the maturity and consistency of execution across the organization because the processes and data impacted by GDPR will exist in all areas of the organization that maintain personal data. The EDM Council will maintain an ongoing activity to collect best practice aligned to the identified areas for Best Practice Opportunities to enhance execution in the DCAM™ Framework.

GDPR Overview

Scope and Applicability

The European Union (EU) **General Data Protection Regulation (GDPR)** was introduced in response to the growth of global enterprise, technological developments, and the huge surge in the volume of data collected by organizations worldwide. It is also intended to harmonize data protection legislation across Member States, establishing a single set of EU laws regarding the processing of personal data. The GDPR is the first comprehensive overhaul of European Union data protection rules in 20 years. It repeals and replaces **EU Data Protection Directive 95/46/EC** and, in turn, the national transpositions of that directive at the EU Member State level. As an EU regulation, the GDPR will be **directly applicable in all 28 EU Member States** without the need for legislation at the Member State level. The GDPR entered into force on May 25, 2016, and will **go live on May 25, 2018**.

The GDPR confers significant powers on regulators to investigate and enforce compliance. Non-compliance could result in a fine of up to 20 million euros or 4% of an organization's total worldwide annual turnover (revenue), whichever is higher.

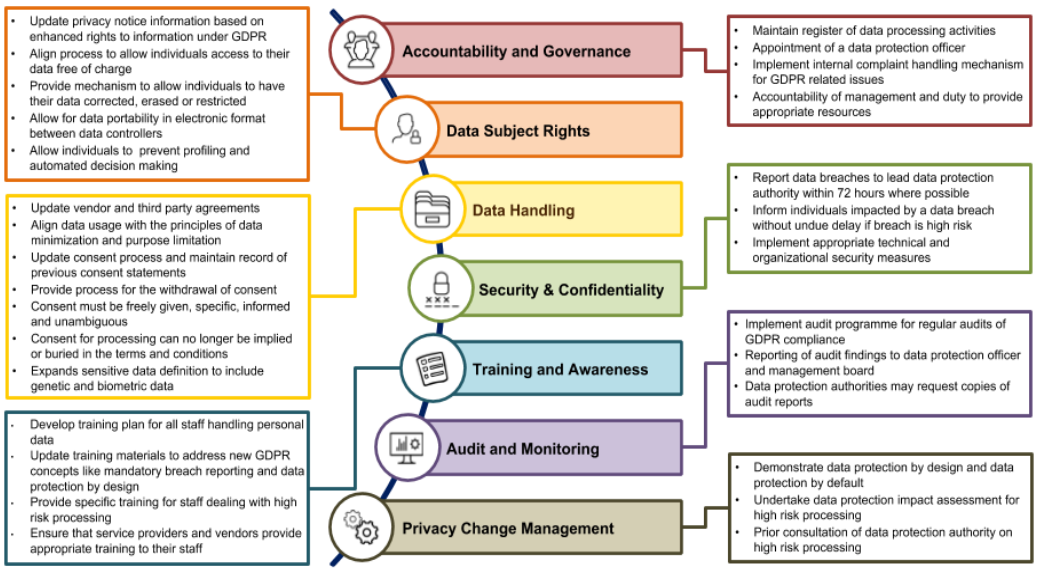
While the regulation is EU jurisdiction legislation **it applies globally to any organization offering goods or services into the European Union.** The GDPR requires any business that stores and manages personal data for people in the EU (e.g. prospects, customers and/or employees) to handle this information in a transparent and structured manner.

GDPR is not targeted to any one industry, however, the Financial Service Industry may be somewhat more prepared than other industries due to its history of dealing with financial services regulation. Nonetheless, GDPR goes beyond any prior Privacy legislation from any jurisdiction globally and is viewed by many as the threshold standard that will likely be formalized by other jurisdictions across the globe.

Background Reference: https://ec.europa.eu/info/law/law-topic/data-protection_en

Summary of Key Provisions

A high level summary of the key provisions of the GDPR are aligned to the seven thematic areas below. These areas are carried through the more detailed analysis of the regulation in this report.



Analysis Concepts

Design concepts were established from an understanding of the GDPR requirements and the implications for data and the Data Management function.

Customer Centric Business Value

While GDPR is a regulatory mandate, if executed effectively there is significant business value derived from the resulting customer concentricity and enhanced customer relationship. The GDPR regulation requires a process of interaction with a customer that delivers transparency, customer empowerment, efficient portability and data quality. These are all opportunities to deepen the relationship and develop trust providing a positive customer experience in order to drive profit and gain competitive advantage. Additionally, the availability of quality data will enable customer knowledge, cross sell and upsell, and opportunity to offer the right product at the right time in the customer lifecycle.

The Role of the CDO & Data Management Function

The CDO is NOT the GDPR “owner”, however, the CDO and the Data Management organization still play a significant role in satisfying the GDPR regulation. Data Management is a control function that will need to support the privacy control function accountable for GDPR compliance and the business units who must manage privacy within their business process. The foundation for supporting the data and Data Management requirements of GDPR compliance are in place if the DCAM™ Framework has been adopted and an appropriate maturity level has been achieved. The challenge is maturity and consistency of execution across the organization because the processes and data impacted by GDPR will exist in many areas across the organization.

Alignment to Organizational Ecosystem

GDPR requires all the lines of defense (1st, 2nd and 3rd), to work in concert to ensure the organization achieves the outcome of valuing and protecting customer privacy and data. The Data Management function must facilitate the collection of requirements from across a variety of ecosystem stakeholders (i.e. Privacy, Risk, Info Security, Data Retention, Technology, AML/KYC, etc.).

The Role of Technology

GDPR requires a strategic alignment between all data stakeholders, and Information Technology (IT) solutions must be a part of the overall solution. The "best efforts" requirement of GDPR requires that appropriate technical and organizational measures are applied.

A best practice approach may include technical automation to support data identification, lineage, metadata, etc. Also, beyond standard access controls more advanced tools may be applied for data to be encrypted, tokenized, anonymized, or pseudonymized at rest, in transit and in memory. These are technological solution to determine who is allowed to view the data and for what purposes.

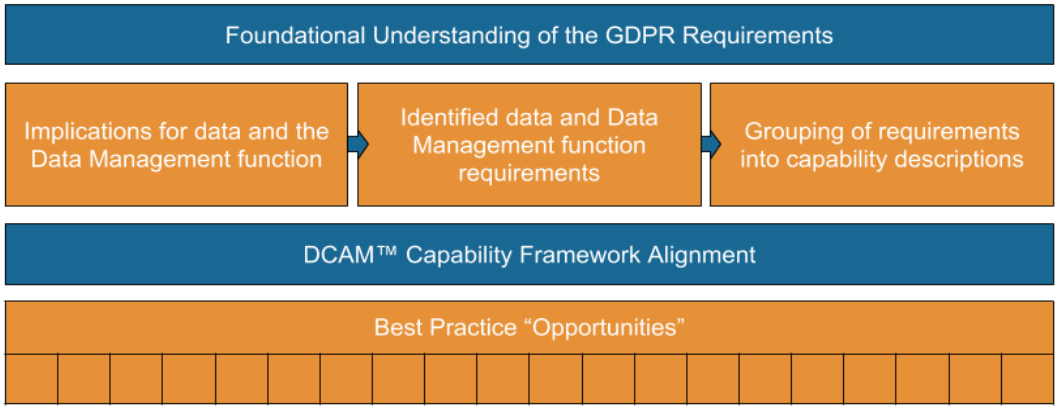
The Role of Master Data

The Work Group acknowledges the value of Customer Master data - if customer data is controlled in a single data domain across the organization the ability to achieve GDPR requirements are simplified and adds to the business case for the Customer Master. However, there are very few, if any, instances of mature Customer Master Data domains.

Approach to Analysis

The Work Group approach a logical analysis of the GDPR requirements for data and the Data Management function.

- Created a shared understanding of the regulatory requirements of GDPR
- Analyzed each requirement for implications for data or the Data Management function
- Interpreted the impacts into Data Management requirement statements
- Alignment of Data Management requirements to the DCAM™ Framework
- Identify Best Practice "Opportunities" to provide specific guidance to support compliance with the regulation



The Analysis

Key Terms

The following are key terms that are integral to understanding the GDPR regulation and thus are included here for reference. A complete glossary of terms is contained in the appendix.

TERM	DEFINITION
Data Subject	An identified or identifiable natural person – i.e., a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, etc.
Data Controller	Natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	Any natural or legal person, public authority, agency or other body that processes personal data on behalf of the Businesses.
Personal Data	Any information relating to a data subject.
Sensitive Personal Data	A subset of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life, sexual orientation, genetic data, biometric data in order to uniquely identify a person.

GDPR Requirements for Data and Data Management

The Work Group adopted the Table 1: Analysis Framework provided by *Promontory Financial Group*. The framework organizes the GDPR data protection requirements into seven Thematic Areas and 22 Components, as shown below. These 22 components are the basis for the detailed analysis conducted by the Work Group.

A walk through of each component was conducted resulting in identification of 32 implications for data and the Data Management function.

Data & Data Management Function Requirements

The 32 implications were then interpreted into a total of 48 Data Management requirement statements.

The Work Group adopted the hypothesis that the GDPR requirements impacting the Data Management function were *NOT* materially unique so the foundation provided by the EDM Council DCAM™ Framework would support GDPR compliance.

To validate the hypothesis the 48 defined Data Management requirements were successfully mapped to the Capabilities and Sub Capabilities defined in the DCAM™ Framework. An explanation of the mapping is presented in the next section.

The hypothesis was validated within the following parameters: If the DCAM™ Framework has been adopted and an effective operating level has been achieved, the foundation for supporting the data and Data Management requirements of GDPR compliance is largely in place. However, a challenge is the maturity and consistency of execution across the organization because the processes and data impacted by GDPR will exist in all areas of the organization that maintain personal data.

Table 1: Analysis Framework

Data Subject Rights	
1.1.	Transparency and Information Rights
1.2.	Right of Access
1.3.	Rectification, Erasure and Restriction of Processing
1.4.	Profiling & Automated Individual Decisions
1.5.	Data Portability
Data Handling	
2.1.	Purpose Limitation & Data minimization
2.2.	Data Quality & Proportionality
2.3.	Legal Basis for Processing Personal Data
2.4.	Special Categories of Data
2.5.	Controller - Processor Relationship
2.6.	Controller - Controller Relationship
2.7.	International Data Transfers
Training	
3.1.	Training Programme
Accountability & Governance	
4.1.	DPOs, Compliance & Mutual Assistance
4.2.	Records of Processing Activities
Security & Confidentiality	
5.1.	Security of Processing
5.2.	Breach Notifications to Data Protection Authorities
5.3.	Breach Notifications to Data Subjects
Change Management	
6.1.	Data Protection by Design and by Default
6.2.	Data Protection Impact Assessments
6.3.	Prior Consultation
Assurance and Monitoring	
7.1.	Audit Programme

Source: *Promontory Financial Group*

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

A summary and detailed version of the analysis are contained in two supporting documents.

GDPR Requirements Analysis Quick Reference Guide - a summary of the GDPR requirements aligned to the DCAM™ Framework.

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

Best Practice “Opportunities”

Best Practice Opportunities

While the DCAM™ Framework provides the Data Management foundation to support compliance to the GDPR, the Work Group did identify a set of additional focus areas where ongoing collaboration and knowledge share could produce further valuable best practice standards. The following is a listing of proposed areas for Best Practice Opportunities.

In the absence of these best practice standards it is recommended that organizations will need to independently define their approach to each of these focus areas. The list below is a guide for an organization to ensure their Data Management processes and tools consider an approach to these focus areas.

The EDM Council will maintain an ongoing effort to collect best practice executions from member organizations. As best practice emerges, it will be published as a follow-on to this report.

The table on the following page identifies the Focus Areas, provides a Description of the issue and lists the GDPR Components to which the issue is aligned. They are also presented in a ranked order (High, Medium and Low) per the collective opinion of the Work Group membership.

Focus Areas for Best Practice

#	Focus Area	Description GDPR Component Alignment
		High Priority
1	**Business Logic**	The objective is to define proposed standard business rules or logic that are required to define the scope and parameters of the following components to be considered by an organization. The actual interpretation of the requirements and resulting logic may vary between organizations. • Transparency and Information Rights • Purpose Limitation & Data Minimization • Data Quality and Proportionality • Legal Basis for Processing Personal Data • Sensitive Data (Special Categories of Data) • Controller - Processor Relationship • International Data Transfers (Cross Border) • Security of Processing • Breach Notifications to Data Subjects

#	Focus Area	Description GDPR Component Alignment
2	**Data Elements (DEs) in scope - Additions**	The objective is to identify the proposed data set to be considered in the execution processes. The processes to manage the GDPR component requirements will necessitate the creation of new data elements related to the activities in the process (Examples: Data Subject Request Flag, Request Date, Request Completion, Completion Date, etc.). Actual execution and data required may vary between organizations. ● Transparency and Information Rights ● Right of Access ● Rectification, Erasure and Restriction of Processing ● Profiling & Automated Individual Decisions ● Data Portability ● Purpose Limitation & Data Minimization ● Data Quality & Proportionality ● Legal Basis for Processing Personal Data ● Sensitive Data (Special Categories of Data) ● Controller - Processor Relationship ● International Data Transfers ● Security of Processing ● Breach Notifications to Data Subjects
3	**Design Guidelines: Data Flow and/or Lineage**	The objective is to define proposed design guidelines for the appropriate rigor of Data Flow or Lineage to execute the GDPR component requirements. The premise is that Data Flow is lighter rigor and is encompassed by the greater rigor included in Data Lineage. The proposal is to align the appropriate required rigor to the GDPR component requirements. ● Transparency and Information Rights ● Rectification, Erasure and Restriction of Processing ● Profiling & Automated Individual Decisions ● Data Portability ● Purpose Limitation & Data minimization ● Data Quality & Proportionality ● Legal Basis for Processing Personal Data ● Sensitive Data (Special Categories of Data) ● Controller - Processor Relationship ● International Data Transfers ● Security of Processing ● Breach Notifications to Data Subjects
4	**Design Guidelines: Legal Basis for Processing**	The objective is to define proposed design guidelines for identifying a standard set of legal basis for processing. The basis may vary across the range of products of an organization and specific business processes of an organization. ● Legal Basis for Processing Personal Data

#	Focus Area	Description GDPR Component Alignment
5	**Metadata Model Additions**	The objective is to identify a proposed standard set of new metadata fields that are needed to execute the GDPR component requirements (Examples: In scope for "X" flag", Erasure Flag, Automated Decision Flag, Special Categories of Data). ● Transparency and Information Rights ● Rectification, Erasure and Restriction of Processing ● Profiling & Automated Individual Decisions ● Data Portability ● Purpose Limitation & Data minimization ● Data Quality & Proportionality ● Sensitive Data (Special Categories of Data) ● Controller - Processor Relationship ● International Data Transfers ● Security of Processing ● Breach Notifications to Data Subjects
6	**Policy Implications: Data Retention Policy**	The objective is to propose standard language required in the Enterprise Data Management Policy related to achieving the execution of the GDPR related Data Retention policies. ● Rectification, Erasure and Restriction of Processing ● Purpose Limitation & Data minimization ● Data Quality & Proportionality
7	**Policy Implications: Ecosystem**	The objective is to propose standard language required in the Enterprise Data Management Policy to establish accountabilities and collaboration across the in-scope data ecosystem of the organization. ● Transparency and Information Rights ● Rectification, Erasure and Restriction of Processing ● Profiling & Automated Individual Decisions ● Purpose Limitation & Data minimization ● Data Quality & Proportionality ● Sensitive Data (Special Categories of Data) ● Controller - Processor Relationship ● International Data Transfers ● Security of Processing ● Breach Notifications to Data Subjects
	Medium Priority	
8	**Data Elements (DEs) in Scope - Existing**	The objective is to identify the possible data set in scope as defined by the specific criteria in the GDPR component requirements. Not all identified data will exist or have the same naming in every organization. ● Transparency and Information Rights ● Rectification, Erasure and Restriction of Processing ● Data Portability

#	Focus Area	Description GDPR Component Alignment
9	**Design Guidelines: 3rd Party Provisioning**	The objective is to define proposed design guidelines for the data management processes related to provisioning data to 3rd parties while executing the GDPR component requirements. The actual "3rd party provisioning process" would be incorporated into the various products and business processes of the organization. ● Data Portability
10	**Design Guidelines: Data Erasure**	The objective is to define proposed technical design guidelines for data erasure (incorporating the invocation of Right to be Forgotten). This is further complicated by the apparent tension between non-GDPR minimum records/data retention requirements and the "Right to be Forgotten". How can you do both? The best practice recommendation for this will need to address this tension in order to successfully meet the criteria. A best practice would be to allow for a data subject to reinstate their relationship with an organization. ● Rectification, Erasure and Restriction of Processing
11	**Design Guidelines: Data Provisioning Format**	The objective is to define proposed design guidelines for the standard format for provisioning data as defined in the GDPR component requirements. ● Right of Access ● Data Portability
12	**Education Content Outline**	The objective is to propose a curriculum outline for the data management related training required for GDPR compliance. This curriculum may be incorporated into an overall GDPR compliance training curriculum maintained by the GDPR accountable control function of the organization. ● Training Programme
13	**Policy Implications: Data Management Policy**	The objective is to propose standard language required in the Enterprise Data Management Policy related to GDPR component requirements compliance. These may all be in relation to the policy published by the control function accountable for GDPR compliance. ● Transparency and Information Rights ● Controller - Processor Relationship ● International Data Transfers ● Security of Processing ● Global Requirements

#	Focus Area	Description GDPR Component Alignment
		Low Priority
14	**Design Guidelines: Technical Access Controls**	The objective is to define proposed technical design guidelines to take technical and organizational measures to secure the data. A best practice approach is for data to be encrypted, tokenized, anonymized, or pseudonymized at rest, in transit and in memory. This cannot be done with policy alone, and it requires a technological solution to manage access to the data. The underlying process determines who is allowed to view the data and for what purposes and for tracking when access was granted and when it was blocked. ● Security of Processing
15	**Design Guidelines: Human Intervention**	The objective is to define proposed design guidelines for the appropriate data management requirements for executing the human intervention in automated decisioning requested by the data subject as defined in the GDPR component requirements. The actual "human intervention process" would be incorporated into the various products and business processes of the organization. ● Profiling & Automated Individual Decisions
16	**Design Guidelines: Master Data**	The objective is to define proposed design guidelines for the appropriate data management requirements for including all in-scope data in the related Master Data domain. This would only pertain to those organizations who have or are developing related Master Data. ● Transparency and Information Rights
17	**Design Guidelines: Pause Control and Process**	The objective is to define proposed design guidelines for the appropriate data management requirements for executing the "pause control process" as defined in the GDPR component requirements. The actual "pause and control process" would be incorporated into the various products and business processes of the organization. ● Rectification, Erasure and Restriction of Processing
18	**DQ Rules Unique to GDPR**	The objective is to define DQ rules that can be applied to in-scope data to measure quality or process compliance (Examples: Is there a data subject restriction applied to this data?). ● Data Quality & Proportionality
19	**Purpose of Processing Standard Categories**	The objective is to define a proposed standard set of categories for the "Purpose of Processing". The categories may vary across the range of products and specific business processes of an organization. ● Purpose Limitation & Data minimization

Appendix

GDPR Reference

Background Reference: https://ec.europa.eu/info/law/law-topic/data-protection_en

GDPR Requirements Analysis

GDPR Requirements Analysis Quick Reference Guide - a summary of the GDPR requirements aligned to the DCAM™ Framework.
https://c.ymcdn.com/sites/edmcouncil.site-ym.com/resource/resmgr/featured_documents/REG_GDPR_Reqmt_Anlsys_v1.0.pdf

EDMC GDPR Requirements Detailed Analysis - the full GDPR requirements analysis with data and Data Management Impacts, requirements, and DCAM™ Framework alignment.
https://c.ymcdn.com/sites/edmcouncil.site-ym.com/resource/resmgr/featured_documents/REG_GDPR_Reqmt_Detail_v2.0.pdf

Business Glossary

TERM	DEFINITION
Adequate jurisdictions	Jurisdictions that were deemed to provide an adequate level of protection to personal data by the European Commission. These include: Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.
Anonymisation	Process of turning data into a form that does not identify individuals and where identification is not likely to take place. (The process is irreversible so the data is likely removed from the GDPR scope.)
Customers	Current, former, and prospective individual consumers contracted to receive products or services.
Data controller	Natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	Any natural or legal person, public authority, agency or other body that processes personal data on behalf of the Businesses.
Data Protection Officer (DPO)	A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR).
Data subject	An identified or identifiable natural person – i.e., a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, etc.
Data Process Impact Assessment (DPIA)	A DPIA is an assessment of the impact of envisaged processing operations on the protection of personal data. Under the GDPR, a DPIA must be carried out where a type of processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons.

TERM	DEFINITION
Employees	Employees means current, former and prospective staff including full or part time workers, interim or casual workers, salaried workers, consultants, contractors or temporary workers whether employed directly or through an agency, interns and work experience students, senior management and executive officers and job applicants.
EU	Currently, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.
EU Data Protection Directive	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
GDPR	EU General Data Protection Regulation, or Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
Legitimate interest	Legitimate interest is one of a number of grounds that a data controller may rely on for the lawful processing of personal data. In order to rely on this ground, the legitimate interests of the data controller, or any third parties to whom the data are disclosed, must be balanced against the interests or fundamental rights of the data subject.
Personal data	Any information relating to a data subject.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual.
Pseudonymisation	Processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. (By design, pseudonymization is reversible and thus the data must remain in the GDPR scope.)
Sensitive personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life, sexual orientation, genetic data, biometric data in order to uniquely identify a person (formally referred to as "special categories of personal data" under the GDPR).
Standard data protection clauses	Contractual clauses approved by the European Commission, which can be included in controller-to-controller or controller-to-processor contracts in order to allow for the international transfers of personal data between the contractual parties.

Work Group Members

Allen, Diahn - T Rowe Price
Arzaga, Raymund - Scotiabank
Atkin, Mike - EDMC
Baig, Haroon - Barclays
Bersie, Bret - US Bank
Bholasing, Jeffrey - ING
Blaszkowsky, David - Financial Semantics Collaborative
Bottega, John - EDMC
Bruckman, Todd - AIG
Buoninfante, Christina - Mizuho
Cardoso, Karina - E&Y
Dinsmore, Chris - BBH
Dokuchaeva, Anastasia - ClauseMatch
Doyle, Martin - DQ Global
Giordano, Peter - Oppenheimer & Co.
Hankinson, Simon - Collibra
Inserro, Richard - PWC
Isaac, Gareth - Ortecha
Lancos, Peter - Exate Technology
Lawson, Andrew - Brickendon
Magora, Stephen - Credit Suisse
McDougall, Simon - Promontory Financial Group
McQueen, Mark - EDMC / FutureDATA
Miliffe, Christopher - E&Y
Naismith, Jonathan - Exate Technology
Rattan, Sonal - Exate Technology
Rende, Daniel - RBC
Rolles, Daniel - EXL Service
Ruston, Max - Charles Schwab
Sarkar, Agomoni
Singh, Ankita - Invesco
Snyder, Nathan - Brickendon
Sordo, Mauricio - ING
Spiegler, Yoni - Mizuho
St Clair, Micheline - RBC
Steenbeek, Irina - ABN AMRO
Stender, Werner - CapCO
Sukhia, Umang - AIG
Tanag, Marichelle - AIG
Thomas, Richard - Invesco
Timofeev, Paula - Wellington Management Co.
Van De Haar, Bert - ING
Wackwitz, Merel - ING

About the Author

Mark McQueen is the Senior Advisor, Best Practice and Process Management for the EDM Council. He joined the Council in 2016 and now leads the Best Practice Program to develop Data Management industry standard processes for executing the DCAM™ Framework. Mark has over 20 years with a Fortune 25 GSIB where he was the business Data Management Executive for the Wholesale Bank. In addition to Best Practice Program facilitation, he provides training and EDMC Advisory Services related to adoption and execution of the DCAM™ Framework in member organizations.

Mark is DCAM™ Foundations and Applied accredited, Six Sigma Black Belt Certified, and Strategic Foresight accredited - University of Houston.

Mark is Founder and Principal Consultant of FutureDATA Consulting.

mmcqueen@edmcouncil.org
+1 615.308.6465