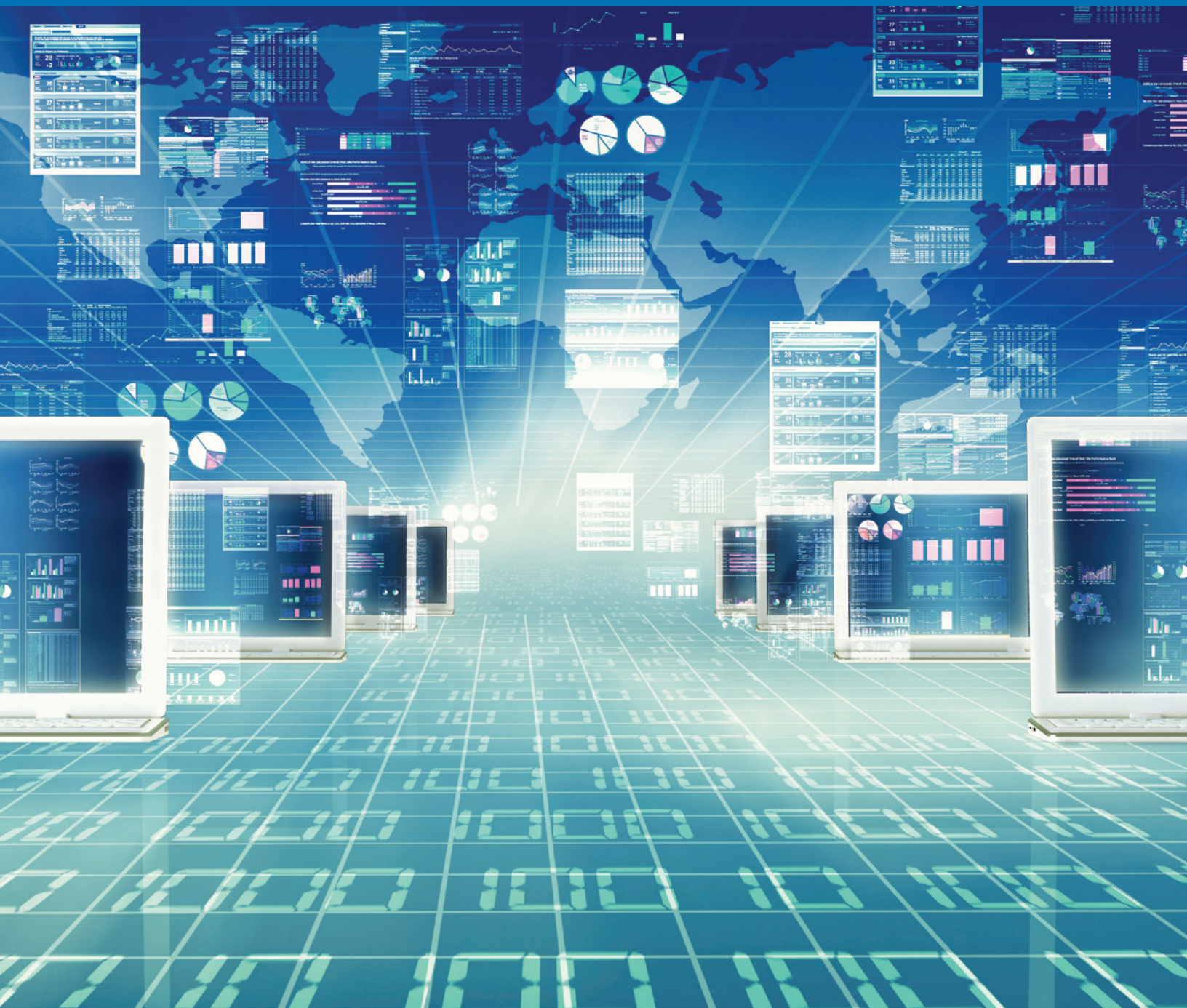
MetricStream
M7
GRC FOR HIGH PERFORMERS

Decoding GDPR Roles and Responsibilities

Requirements for Data Processors, Data Controllers, and Data Protection Officers



The EU General Data Protection Regulation (GDPR) is poised to do for data protection and security what the Sarbanes-Oxley Act (SOX) did for corporate governance in the early 2000s – the implications are that significant. While the new regulation may be EU-specific, its reach and impact are global. Enterprises across countries that collect, store, or process the personal data of EU citizens—be it that of customers, employees, patients, policy holders, beneficiaries, contractors, third parties, volunteers, or visitors — will need to demonstrate compliance with GDPR. Government agencies will also be impacted by the regulation.

It doesn't end there. While GDPR may seem like an "IT" issue, it will require multiple business units to participate actively in compliance – particularly Human Resources, Sales and Marketing, Finance, Procurement, and Legal. What's more, for the first time in the EU, data processors, including third parties, vendors, and suppliers will have direct obligations and responsibilities to protect and secure the data that they process.

In short, the scope of the new regulation is immense. And the repercussions for non-compliance are also expected to be huge – up to 4% of an enterprise's annual global turnover or €20 million, whichever is greater. To put that in context, UK-based telecom company, TalkTalk was fined a record £400,000 by the UK Information Commissioner's Office (ICO) in 2016 for security failings that allowed cyber attackers to access customer data. Under GDPR, those fines could have shot up to more than £50 million.*

$124 million (€106 million)

That's how much Equifax could have been fined under GDPR for its recent data breach affecting 143 million customers.

** https://www.theregister.co.uk/2017/04/28/ico_fines_post_gdpr_analysis/*

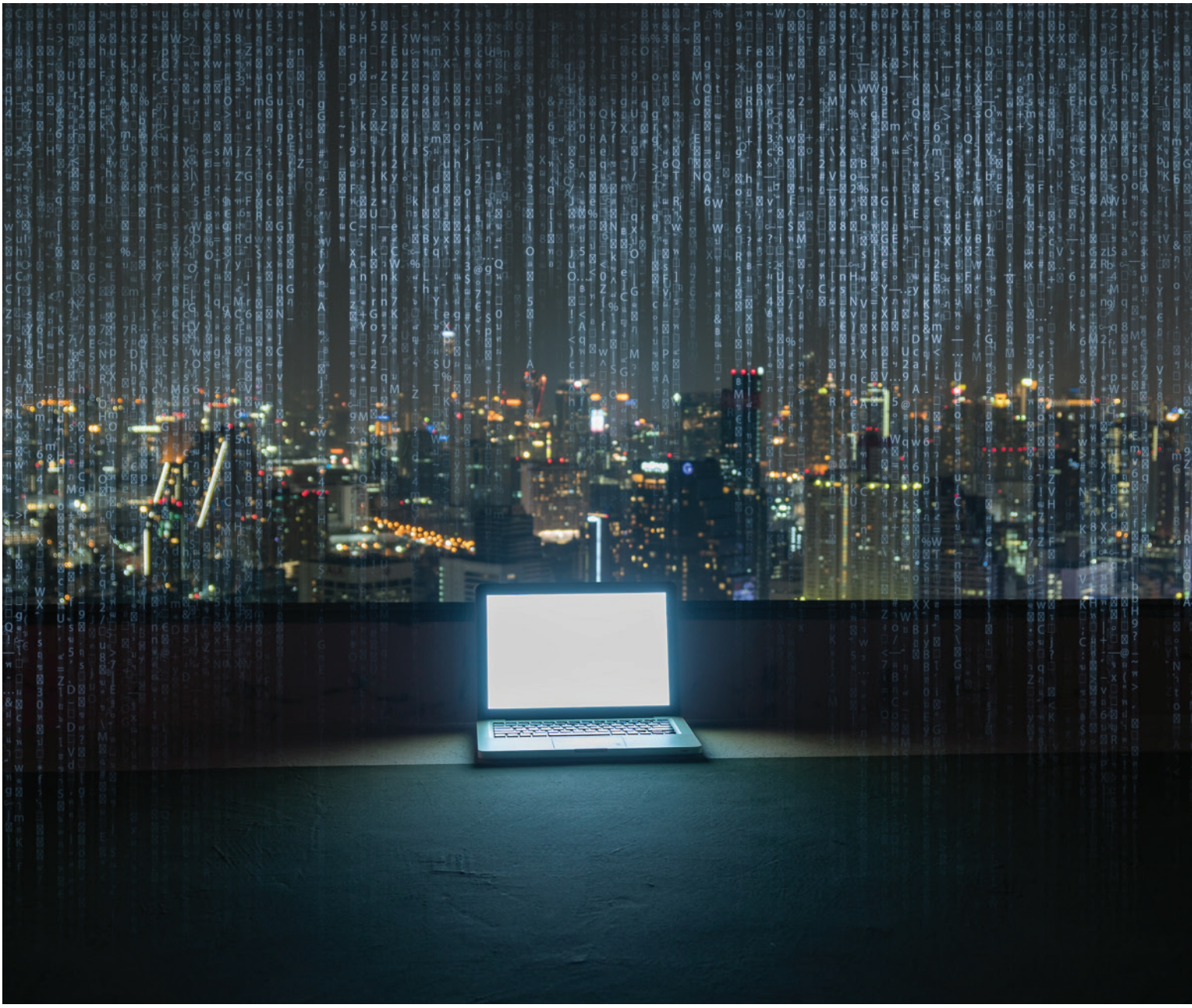
So What Do Enterprises and Government Agencies Need to Do?

GDPR outlines clear roles and responsibilities for the entities involved in the collection, storage, and processing of personal data. It divides these entities into data controllers and/or data processors, and also introduces the role of a Data Protection Officer (DPO) who must report directly to the CEO.

In the following pages of this document, we define each of these entities and their core compliance requirements. We also map each requirement to the MetricStream M7 GDPR Solution, demonstrating how technology can help data controllers, processors, and DPOs fulfill their compliance requirements successfully.

Who is a Data Controller?

Article 4 of GDPR defines a data controller as "a natural or legal person, public authority, agency, or other body which alone or jointly with others *determines the purposes and means of processing personal data."* A data controller could either be an organization (e.g. bank, retailer) or an individual (e.g. general practitioner) that collects and processes information about customers, patients, etc. Under GDPR, the data controller is responsible for ensuring that data is processed in compliance with the principles of lawfulness, fairness, transparency, data minimization, accuracy, storage limitation, integrity, and confidentiality.



GDPR Compliance Checklist for Data Controllers

GDPR Article	Summary of Requirements	How the MetricStream M7 GDPR Solution Can Help
		Policy and Document Management
Art. 9 Processing of special categories of personal data	Prohibit the processing of certain classes of data (e.g. genetic/ biometric details), unless under certain conditions (e.g. the data subject has provided explicit consent to process the given data)	Streamlines the creation and distribution of policies on how certain classes of data can and cannot be processed
Art. 13 Information to be provided where personal data are collected from the data subject	When personal data is collected, provide data subjects with relevant details such as the purpose of processing the data, recipients of the data, and period for which the data will be stored	Provides a central repository to maintain policies on how data will be processed and secured. These policies can be shared with data subjects when their personal data is collected
Art. 14 Information to be provided where personal data have not been obtained from the data subject	When personal data has not been collected, provide data subjects with relevant details such as the purpose of processing the data, recipients of the data, and period for which the data will be stored	Provides a central repository to maintain policies on how data will be processed and secured. These policies can be shared with data subjects.
Art. 22, Section 3 Automated individual decision-making, including profiling	Implement measures to safeguard the data subject's rights to contest decisions that were based on automated data processing, including profiling	Helps create and maintain policies to give data subjects inputs on data processing, and to govern decisions based on automated data processing
Art. 24, Section 2 Responsibility of the controller	Establish appropriate data protection policies	Supports the data protection policy management lifecycle, right from policy creation, to distribution, and attestation. Helps map policies to GDPR requirements to identify and close gaps
Art. 47, Section 2 Binding corporate rules	Create binding corporate rules to regulate the international transfers of personal data. Have these rules approved by the supervisory authority.	Enables the creation of binding corporate rules with clearly defined review and approval workflows involving the supervisory authority
Art. 33, Section 5 Notification of a personal data breach to the supervisory authority	Document any personal data breaches	Enables users to record, store, and track personal data breaches, including the details of the breach, effects, and remedial action taken. Allows notifications to be triggered to the supervisory authority
		IT Risk Management
Art. 46 Transfers subject to appropriate safeguards	Conduct assessments, and implement appropriate safeguards before transferring personal data to a third country or international organization	Delivers an in-built IT risk assessment framework to identify, assess, and monitor the risks to data security before transferring data to a third country or international organization.
		IT Compliance
Art. 24, Section 3 Responsibility of the controller	Adhere to codes of conduct or certification mechanisms to demonstrate compliance with data protection requirements	Enables detailed control tests and self-assessments to monitor compliance with codes of conduct. Integrates with the industry-leading Unified Compliance Framework (UCF) to capture control content and testing procedures
Art. 25, Sections 1 & 2 Data protection by design and by default	Implement technical and organizational measures to minimize the collection and processing of data	Helps establish and document controls for data minimization and protection. Integrates with UCF to provide a comprehensive library of GDPR compliance controls. Harmonizes controls, minimizing redundancies

Art. 25, Section 3 Data protection by design and by default	Demonstrate compliance with data minimization and protection principles	Supports surveys, assessments, and certifications to evaluate compliance with data minimization/ protection requirements
Art. 32, Section 1b Security of processing	Implement measures to ensure the confidentiality, integrity, availability, and resilience of processing systems and services	Helps implement controls for data security, confidentiality, integrity, etc. Links controls to risks, processes, and assets for a holistic view of compliance
Art. 32, Section 1d Security of processing	Ensure ongoing testing, assessment, and evaluation of the effectiveness of data security measures	Helps plan, manage, and conduct tests and assessments of data security controls based on pre-defined criteria and checklists
Art. 32, Section 3 Security of processing	Adhere to codes of conduct or certification mechanisms to demonstrate compliance with data security requirements	Enables detailed control tests and self-assessments to monitor compliance with codes of conduct around data security requirements
Art. 35 Data protection impact assessment	Conduct a Data Protection Impact Assessment (DPIA) when a data processing activity is likely to result in a high risk	Streamlines and automates DPIAs. Helps design and assign DPIA surveys, and automatically tabulates the results with configurable scoring algorithms
		Audit Management
Art. 35, Section 11 Data protection impact assessment	Perform reviews to assess if data is being processed in accordance with DPIAs	Helps plan and perform audits to evaluate compliance with data protection requirements, including DPIAs
Art. 47, Section 2j Binding corporate rules	Conduct data protection audits to verify compliance with binding corporate rules	Simplifies audit planning, scheduling, resource and task management, fieldwork, and reporting to validate compliance with binding corporate rules
		Case and Incident Management
Art. 12, Section 3 Transparent information, communication and modalities for the exercise of the rights of the data subject	Respond to requests for information from data subjects in a timely manner	Enables requests from data subjects to be managed efficiently through a streamlined, standardized process for request recording, action plan management, and resolution
Art. 15, Section 1f Right of access by the data subject	Respond to requests from data subjects on their right to access their data, and to lodge a complaint with the supervisory authority	
Art. 16 Right to rectification	Respond to requests from data subjects on their right to rectify any data that is inaccurate or incomplete	
Art. 17 Right to erasure	Respond to requests from data subjects on their right to be forgotten	
Art. 18 Right to restriction of processing	Respond to requests from data subjects on their right to restrict the processing of data under specific conditions	
Art. 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing	Notify data subjects on the actions taken to rectify or erase personal data, or restrict data processing	Supports a consistent, workflow-based approach to change, erase, or restrict data in coordination with data subjects
Art. 21 Right to object	Respond to objections from data subjects on the processing of personal data	Helps capture, track, investigate, and resolve objections or complaints from data subjects. Tracks each complaint in real time
Art. 22, Section 4 Automated individual decision-making, including profiling	Ensure that automated decision-making does not extend to special categories of personal data, unless suitable measures are in place to safeguard the data subject's rights	Create an exception-based workflow to manage special categories of personal data that cannot be subject to automated decision-making

Art. 33 Notification of a personal data breach to the supervisory authority	Notify the supervisory authority of a personal data breach within 72 hours of becoming aware of it	Helps log, track, investigate, and report data breaches and other incidents in a systematic, consistent manner
Art. 34 Communication of a personal data breach to the data subject	Notify data subjects of personal data breaches without undue delay	
Art. 36 Prior consultation	Consult the supervisory authority when a DPIA indicates that processing would result in a high risk	Captures high-risk data processing cases with comprehensive details, and supports communication with the supervisory authority; allows these cases to be logged anonymously if required
Art 38, Section 4 Position of the data protection officer	Ensure that DPOs can manage requests from data subjects with regard to data processing issues	Enables requests from data subjects to be managed efficiently through a streamlined, standardized process for request recording, action plan management, and resolution
		Third-Party Management
Art 28, Section 1 Processor	Onboard only those data processors that can ensure compliance with data protection requirements	Enables third-party due diligence and risk assessments to identify data processors that can and cannot comply with data protection requirements
Art 28, Section 3 Processor	Implement contracts to govern how data processors store and process data	Supports third-party onboarding and contract compliance management. Centrally maintains all contracts, links them to other documents, and provides automated reminders to update or renew contracts
		Business Continuity Management
Art. 32, Section 1c Security of processing	Restore the availability and access to personal data quickly in the event of a physical or technical incident	Helps plan and test crisis responses to possible physical or technical disruptions. Enables a systematic approach to log, track, investigate, and resolve incidents, as well as to implement recovery plans

Who is a Data Processor?

Article 4 of GDPR defines a data processor as "a natural or legal person, public authority, agency, or other body which *processes personal data on behalf of a controller.*" Data processors could include organizations such as payroll firms, cloud service vendors, and data analytics providers. While data processors report to data controllers, they are also directly accountable for data protection under GDPR. Incidentally, data processors can also be data controllers. For instance, a vendor conducting market research for another enterprise would be a data processor, but when managing the data of their own employees, they take on the role of a data controller.

GDPR Compliance Checklist for Data Processors

GDPR Article	Summary of Requirements	How the MetricStream M7 GDPR Solution Can Help
		Policy and Document Management
Art. 47, Section 2 Binding corporate rules	Create binding corporate rules to regulate the international transfers of personal data. Have these rules approved by the supervisory authority	Enables the creation of binding corporate rules with clearly defined review and approval workflows involving the supervisory authority

		IT Risk Management
Art. 46 Transfers subject to appropriate safeguards	Conduct assessments, and implement appropriate safeguards before transferring personal data to a third country or international organization	Delivers an in-built IT risk assessment framework to identify, assess, and monitor the risks to data security when transferring personal data to a third country or international organization.
		IT Compliance
Art. 28, Sections 3f and 3h Processor	Assist the controller in ensuring compliance with GDPR requirements, and managing audits	Helps document and establish controls to comply with GDPR requirements. Supports control tests, compliance self-assessments, and audits to monitor compliance
Art. 28, Section 5 Processor	Adhere to codes of conduct or certification mechanisms to demonstrate compliance with GDPR	Enables detailed control tests and self-assessments to monitor compliance with codes of conduct. Integrates with UCF to capture control content and testing procedures
Art. 32, Section 1b Security of processing	Implement measures to ensure the confidentiality, integrity, availability, and resilience of processing systems and services	Helps implement controls for data security, confidentiality, integrity, etc. Links controls to risks, processes, and assets for a holistic view of compliance
Art. 32, Section 1d Security of processing	Ensure ongoing testing, assessment, and evaluation of the effectiveness of data security measures	Helps plan, manage, and conduct tests and assessments of data security controls and measures based on pre-defined criteria and checklists
		Audit Management
Art. 47, Section 2j Binding corporate rules	Conduct data protection audits to verify compliance with binding corporate rules	Simplifies audit planning, scheduling, resource/ task management, fieldwork, and reporting to validate compliance with binding corporate rules
		Case and Incident Management
Art. 33, Section 2 Notification of a personal data breach to the supervisory authority	Notify the controller of a data breach without undue delay	Helps log, track, investigate, and report data breaches to data controllers in a systematic manner
Art 38, Section 4 Position of the data protection officer	Ensure that DPOs can manage requests from data subjects with regard to data processing issues	Enables requests from data subjects to be managed efficiently through a streamlined, standardized process for request recording, action plan management, and resolution
		Third-Party Management
Art. 28, Section 2 Processor	Ensure approval of the controller before engaging another processor	Helps implement a consistent, workflow based approach to reviewing, approving, and onboarding other processors in collaboration with the data controller
Art. 28, Section 4 Processor	Conduct effective due diligence on downstream processors to ensure that they can comply with data protection requirements	Enables third-party due diligence and risk assessments to identify downstream processors that can and cannot comply with data protection requirements
		Business Continuity Management
Art. 32, Section 1c Security of processing	Restore the availability and access to personal data quickly in the event of a physical or technical incident	Helps plan and test crisis responses to possible physical or technical disruptions. Enables a systematic approach to log, track, investigate, and resolve incidents, as well as to implement recovery plans

Who is a Data Protection Officer?

Under GDPR, data controllers and processors are required to appoint a Data Protection Officer (DPO) if: (a) processing is carried out by a public authority/ body, (b) the organization's core activities involve regular and systematic processing of data subjects on a large scale, or (c) the organization's core activities involve processing of special categories of data (e.g. criminal convictions). DPOs are responsible for ensuring that the strategy and implementation of data protection requirements are in compliance with GDPR. Even organizations that do not strictly meet the requirements for a DPO by title will still have someone who is fulfilling these responsibilities.

GDPR Compliance Checklist for DPOs

GDPR Article	Summary of Requirements	How the MetricStream M7 GDPR Solution Can Help
		IT Risk Management
Art. 39, Section 2 Tasks of the data protection officer	Be aware of the risks of data processing	Enables DPOs to assess, quantify, and monitor the risks of data processing. Provides a real-time risk view through powerful dashboards, reports, and analytics
		IT Compliance
Art. 47, Section 2h Binding corporate rules	Monitor compliance with binding corporate rules	Facilitates real-time monitoring of compliance through intuitive dashboards, reports, and risk heat maps
		Audit Management
Art. 39, Section 1b Tasks of the data protection officer	Monitor compliance with GDPR and data protection policies through activities such as audits	Enables regular, workflow driven audits to assess compliance with GDPR and data protection requirements.
		Regulatory Engagement Management
Art. 39, Sections 1d & 1e Tasks of the data protection officer	Manage relationships with the supervisory authority	Simplifies the process of managing various engagements with supervisory authorities, including meetings, investigations, and requests for information

Compliance Begins Now

GDPR may seem like yet another onerous regulation. Yet, in the wake of multiple data breaches—each worse than the last — the new regulation represents a step forward towards stricter accountability and enforcement. In fact, GDPR is increasingly being perceived as a benchmark for data protection laws worldwide, and it's only a matter of time before other countries impose similar regulations – perhaps with tougher restrictions and penalties.

Technology can play a key role in strengthening compliance, and to that end, the MetricStream M7 GDPR Solution provides a range of capabilities to align data protection and processing with GDPR compliance requirements. Enterprises also need well-defined compliance processes and policies, as well as cross-functional teams to manage and oversee compliance. Together, these elements can go a long way towards helping data controllers, processors, and other entities adhere to GDPR in a consistent manner, while also building credibility and trust around their data protection abilities.

MetricStream, the independent market leader in enterprise and cloud applications for Governance, Risk, Compliance (GRC) and Quality Management, makes GRC simple. MetricStream apps improve business performance by strengthening risk management, corporate governance, regulatory compliance, vendor governance, and quality management for hundreds of thousands of users in dozens of industries, including Financial Services, Healthcare, Life Sciences, Energy and Utilities, Food, Retail, CPG, Government, Hi-Tech and Manufacturing. MetricStream is headquartered in Palo Alto, California, with an operations and R&D center in Bangalore, India, and sales and operations support in 12 other cities globally. (www.metricstream.com)
Email: info@metricstream.com

US: +1-650-620-2955 UK: +44-203-318-8554 India: +91-(0)80-4049 6600 Australia: + 61 2-8036-3130