The GDPR Roadmap : Building an implementation plan

Area of Control	Things to consider for building a GDPR implementation plan	GDPR Articles
Roles and Responsibilities	Make sure you fully understand the various roles and responsibilities required to ensure successful GDPR compliance. Clearly define and distribute new responsibilities to specific roles. Be flexible to amending these responsibilities if an employee's role changes. Assign responsibilities appropriately and provide sufficient coverage through annual attestation and competency reviews. Put all pertinent policies, procedures and links to training resources in one place to provide easier employee access. Ensure sufficient data privacy coverage by developing and implementing a policy and procedure workflow to regularly review responsibilities. Create reports and document evidence of compliance against obligations based on those reports. Consider a tool that allows you to manage and mitigate risk by putting controls in place to assign responsibilities and track obligations.	5, 24, 25, 26, 27 (Controller) 28 (Processor) 37, 38, 39 (DPO)
Integrity and Confidentiality	Develop and document best practices to identify and reduce risks around data processing. Distribute these best practices to your workforce. Ensure the compliance of third party data processors by providing access to the same policies and procedures as internal employees. This also provides you with reportable attestation against policies. Make sure you have tools and policies in place to ensure security capabilities that will enforce data access controls.	5, 6, 7, 8, 9, 35, 40, 41, 47
Data protection by design and by default	Consider a risk management tool that allows you to specify and define measures, risks and controls to ensure that data is protected. Distribute and gather attestation for these policies and procedures and use to verify the effectiveness of these controls. Validate the effectiveness of your data security design by using the audit and assessment capabilities of a risk management solution.	25
Data Breach Procedures	Build and distribute defined data breach policies and procedures and include a link to the appropriate response plan.	32, 33, 34

	Review and manage data breach policies and procedures on a defined schedule. Audit internal and third party data processors to ensure appropriate procedures to respond to data breaches. Consider a risk management tool that could manage a potential breach, determine its impact and rectify the problem.	
Data Security	Define, control and update security policies and procedures and validate employees' understanding through an auditable testing method. Consider sending regular knowledge assessments to ensure that employees are complying with policies and procedures. If using a risk management tool, ensure that security policies can be linked back to the controls established within the tool to provide visibility of the effectiveness of controls defined against risks. Ensure that data is only accessible for those that require access for data processing.	25, 32, 35, 36, 47
Data Minimization	Define data collection procedures and distribute to employees. Flag unrequired documents for review, approval and deletion, and implement retention policies to remove data. Consider a tool that allows you to define and categorize data with appropriate metadata and enable you to use versioning to reduce data duplication.	5, 25, 47, 89
Purpose Limitation	Allow employees to simply and quickly access standard operating procedures that cover how data can be used. Ensure employees only reference the latest version of the procedure. Consider a content management solution that allows you to limit data access to certain business processes and situations only where consent is given. Develop and enforce a structure for how documents are handled throughout any business process. Using a risk management tool, regularly evaluate and ensure how and why data is used. Distribute regular knowledge assessments to confirm employee and third parties comply with data processing regulations. If an incident occurs, consider a risk management tool to report, track and monitor the issue and provide feedback to minimize the chance of it recurring.	25, 28, 47

Consent	Document and store details of consent given by the data subject. Maintain and distribute policies and procedures on how to obtain and manage consent and how to handle data if consent is withdrawn. Consider a risk management solution to assess and audit correct data usage and flag areas that require rectification.	6, 7, 8, 13, 14, 17
Transparency and Traceability	Document and distribute procedures detailing exactly how data is used and allow easy access to internal staff and third party data processors. Consider a content management solution that provides audit capabilities to report on activities performed by employees during the data lifecycle. Report how data is accessed and managed for additional audit capabilities, data analysis and compliance oversight. This oversight supports assessments that can track back to original regulatory obligations.	12, 30
Data Accuracy	Ensure the latest version of the information is available as required. Employ a system or method where new versions can be added and a full history of the information lifecycle can be stored. Ensure data is valid, accurate and appropriate for processing. Use a tool or develop a system that notifies data processors when information is due to expire and drives escalation as the expiry date approaches. Develop procedures that support sharing of new information by internal employees or third party data handlers.	5, 16, 18
Storage Limitation	Create and share procedures around how and when to remove data. Consider a content management tool that supports the creation of retention policies that can be used to automatically remove information based on defined classifications.	5, 6, 17, 23, 47