IMS Health & Quintiles are now IQVIA™

IQVIA GDPR CHECKLIST

Summary of Activities

GDPR REQUIREMENT	IQVIA GDPR ACTION COMPLETED
Accountability Controllers must be responsible for demonstrating compliance with the data protection principles, including a detailed description of all processing carried out by and on behalf of a controller.	✓ Engaged more than 170 implementation leads focused on GDPR compliance across IQVIA business and operations. Leadership provided by the executive steering committee supported by a project manager and the Global Privacy Team ✓ Distributed and completed GDPR Readiness Questionnaires and Legal Basis Workbooks to create an extensive record of processing ✓ Determined that data processing agreements are suitable to serve as record of processing ✓ Released training on basic GDPR requirements ✓ Updated Information Governance framework, policies, and SOPs to further embed GDPR principles ✓ Appointed a Data Protection Officer (DPO) and established contact process ✓ Validated governance structure ✓ Confirmed corporate guidance on data retention is consistent with GDPR requirements
Data Protection Impact Assessments (DPIAs) Appropriate controls must be in place where processing activities are proposed that may result in a high degree of risk to the rights and freedoms of individuals.	✓ Provided available tools to consistently perform DPIAs as needed ✓ Implemented DPIA trigger questions to identify areas where additional controls are required
Processing Basis Controllers must have a clear and documented lawful basis for processing, including any further processing. If relying on consent, stringent requirements must be met for consent to be valid.	✓ Distributed and completed legal basis workbooks for controller activities ✓ Provided detailed checklist for verifiable consent ✓ Provided updated Informed Consent Form templates and guidance for clinical studies
Data Security Controllers and their processors must implement appropriate technical and organizational measures to ensure a level of data security appropriate to the risk.	✓ Validated requirements are incorporated into Integrated Information Security Framework policies and standards including: unauthorized access and use, correct storage, transmission and disposal ✓ Developed template data processing terms for incorporation into contracts with third-party service providers, communicating the necessity to adhere to our security standards and policies as well as GDPR requirements ✓ Provided training to Office of General Counsel to support review and execution of data processing terms with customer controllers

Breach Reporting GDPR requires controllers to (1) report data breaches to DPAs within 72 hours, unless it is unlikely to result in harm, and (2) notify individuals without undue delay if there is a high risk of harm. Controllers are required to document all breaches regardless of any notification obligations.	✓ Reinforced our existing policies and practices which were previously aligned with the GDPR requirements ✓ Established additional support and provided guidance and education to ensure that the organization is aware and able to respond within the required timelines
Data Subject Rights Controllers must comply with the exercise of data subject rights within a month (which may be extended by a further two months for complex or high-volume requests). Data subjects whose rights have been infringed have a right of judicial remedy against any processor responsible for the alleged breach.	✓ Provided guidance aligned to our existing policies on how to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their personal data ✓ Established centralized processing to ensure data subject requests are handled timely, consistently and in accordance with the regulation
Appointment of Processors/Sub-processors Controllers must only use processors that guarantee compliance with GDPR. Controllers are required to ensure there is a contract with each processor containing certain minimum provisions to meet GDPR requirements.	✓ IQVIA has a risk assessment and management process for the engagement of processors (i.e., vendors and service providers) which includes identifying, assessing, managing and monitoring risk from processors including cybersecurity controls ✓ Developed a data processing terms addendum for use with vendor processors/ sub-processors to ensure processor/sub-processor compliance with GDPR requirements ✓ Provided training to Office of General Counsel to support review and execution of data processing terms with customer controllers
Cross-Border Data Transfers GDPR requires certain conditions to be met for any transfer of data outside the European Union.	✓ For the transfer of data to non-EU countries that do not benefit from an EU Commission adequacy decision, IQVIA has approved data transfer mechanisms available: EU Commission-approved Standard Contractual Clauses (SCCs) and Privacy Shield certifications (for transfers to US only). ✓ Developed template SCCs for use with controllers where IQVIA is a processor utilizing non-EU-based sub-processors (i.e. IQVIA affiliates or third-party vendors)

IMS Health & Quintiles are now IQVIA™

CONTACT US
privacyofficer@iqvia.com
iqvia.com/about-us/privacy