Maturity Level	Data Ethics	Privacy by Design	IT Architecture	Ease of Collaboration	Cost Management	IT Security	Data Governance	Insights, Automation & AI
0 – Non-Existent	No concept of the existence of Data Ethics or data usage guidelines.	No regard given to data subjects' legal "rights". Data is a utility to be used however suits.	No overarching infrastructure strategy.	No collaboration. All data and operations take place in isolated silos.	No defined IT budget, or established financial management policies or processes.	No implemented tools, roles and responsibilities, or documented policies, methods or processes.	No data governance practices, or recognition of their need.	No automation and no understanding of its potential value.
1 - Ad hoc	Basic awareness of Privacy laws and regulations but no understanding of how they affect the organisation.	Awareness of obligations but culture of "common sense" rather than adherence. Little / no security, privacy or compliance expertise.	IT architecture is planned and funded on a per project basis, not strategically.	Some platforms for sharing information amongst teams and individuals, but limited to systems such as email and file storage.	Some understanding and awareness of IT assets, capacity, and costs associated. IT budget is defined and managed.	Activities are unstaffed or co-ordinated. No formal security programme in place. Despite security issues, no controls exist	No data strategy and no business rules. Duplicated and inconsistent data. No responsibility for data management.	Minimal automation and/or data analysis, applied in isolation, based on single datasets and driven by non-experts.
2 - Opportunistic	Departmental initiatives to comply with regulations, but gaps common across the business.	Standards are being established. Measures applied to projects towards end of design cycle, usually to prevent previously-experienced issues.	Centralised IT architecture funding, but planning remains project- based and reactive, rather than anticipating demand strategically.	Some inter-departmental collaboration through cloud-based tools, but platforms were chosen by the teams / individuals, not the business.	IT spend is tightly tied to demand and strategic objectives and costs are reviewed against financial management targets.	Basic governance and risk management process and policies. Some controls in development, but little documentation.	Awareness of importance of data governance, but no one has responsibility. Data loss and duplication are recognised risks, but no measures exist to mediate it.	Automation and/or data analysis is deployed reactively by non-expert teams, sometimes across multiple datasets, but no organisation-wide plan.
3 - Systematic	Standardised frameworks and procedures in place across the entire organisation.	Security, compliance and data privacy responsibilities are all assigned, and individuals collaborate regularly with established processes.	IT architecture is planned for efficiency, both in resources and cost. Performance is measured against cost and governance processes are in place.	Controlled and standardised collaboration platforms in place, with central governance and usage guidelines.	Business can trace spend back to actual consumption by business unit and accurately forecast future demand.	Organisation-wide policies and processes in place, following recognised standards, regularly audited.	Data vision, strategy and quality metrics are emerging. Recovery Point and Time Objectives are understood and set in line with business needs.	Business analysts evaluate datasets to identify trends or make forecasts in line with a central plan. No machine learning or artificial intelligence in place as data not in fit state.
4 - Institutionalized	Business routinely considers data ethics and privacy against every data processing initiative, including those that do not use personal data.	Privacy by Design is understood and culture prevails throughout the organisation. Champions exist in all business units.	IT architecture planning is a core part of organisational strategy, and planned out to meet core objectives rather than project deliverables.	Tools have been chosen to match strategic direction, not just operational needs.	Automated some IT financial management and integrated with IT risk and supplier management processes. Billing is based on service charge-back.	Formal infosecurity committees and measurement processes, and some automation. Data relating to controlled processes is additionally protected.	Data management processes are formalised. Business rules are systemized. Disaster Recovery and Business Continuity is routinely re- assessed, and recovery actions are automated.	Data is organised so that machine learning / artificial intelligence can be applied. Automation has become the norm.
5 - Adaptive	Data ethics are first and foremost in every business process, and marketed externally to demonstrate the business' high standards.	Principles of Privacy by Design are consistently applied. Constructive challenge to innovation is commonplace. Regular review of privacy policies as regulations evolve.	Solutions are chosen and designed to serve the applications that need to be delivered today, with enough flexibility to support applications that the business may require in the future.	Platforms are unified, with little or no duplication of functionality and automation features heavily in many repetitive processes.	Automated service consumption tracking, integrated with charge-back capability.	Security processes are comprehensively implemented and subject to continuous improvement. Some responses to security threats are automated.	Data management fully aligned to corporate strategy. Disaster recovery and backup is fully automated.	Automated processes are smart. They are self-learning and self-healing, and adapting to changes in the processes, quality of data etc