General Date Protection Regulation (GDPR) vs. ISO 15189

Article	GDPR REQUIREMENTS	ISO 15189:2012 REQUIREMENTS	ACTIONS	ADDITIONAL DOCUMENTATION TO ISO 15189
3	GDPR should be applied by any organization that processes data of EU data subjects.	4.1.1.3 Ethical Conduct Laboratory management shall ensure that staff treats human samples, tissues or remains **according to relevant legal requirements** and confidentiality of information is maintained. 5.10 Information System Management The system(s) used for the collection, processing, recording, reporting, storage or retrieval of examination data and information shall be in compliance with **national or international requirements** regarding data protection. The laboratory shall have a documented procedure to ensure that the **confidentiality** of patient information is maintained at all times.	Laboratory management shall have arrangements in place related to the privacy and protection of people's personal information, particularly sensitive computer data.	Not necessary
37-39	Appointment of a qualified data protection officer (DPO) (if required)	4.1.2.5 Responsibility, Authority and Interrelationships Laboratory management shall ensure that responsibilities, authorities and interrelationships are defined, documented within the laboratory organization. This shall include the **appointment of person(s)** responsible for each laboratory function and appointment of deputies for key managerial and technical personnel	DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data. The GDPR requirements would form the basis of a DPO role description.	Role Description of DPO if such a DPO is needed.

35	Obligation to carry out risk analysis and privacy risk impact assessments;	4.14.6 Risk Management The laboratory shall **evaluate the impact of work processes and potential failures** on examination results as they affect patient safety, and shall modify processes to reduce or eliminate the identified risks and document decisions and actions taken.	Privacy-related risks should be included in corporate risk registers alongside various other risks.	Analysis of the impact of processing personal date of natural persons.
5, 89	Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Personal data must be adequate, relevant and limited to those which are necessary; Where personal data are to be archived *e.g.* for research and statistical purposes, the privacy risks should be addressed through suitable controls such as pseudonymization and data minimization where feasible.	5.10.1 Laboratory Information Management The laboratory shall have access to the data and information needed to provide a service which **meets the needs and requirements** of the user. 5.4.3 Request Form Information **Information needed** for examination performance and result interpretation may include the patient's ancestry, family history, travel and exposure history, communicable diseases and other clinical relevant information. Financial information for billing purposes, financial audit, resource management and utilization reviews may also be collected. **The patient should be aware of the information collected and the purpose for which it is collected**.	Laboratory's processes plus apps, systems and networks must adequately secure personal information, requiring a comprehensive suite of technological, procedural, physical and other controls, starting with an assessment of the associated information risks.	Security policies that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
17	Storage limitation (data should be kept for no longer than is necessary); Right to erasure ("right to be forgotten") including withdrawal of consent;	4.5.1 Referral Laboratories and Consultants Requests and results of all samples referred are kept for a **pre-defined period**. 4.13 Control of Records The laboratory shall define the **time period** that various records pertaining to the quality management system are to be retained. The length of time that the records are retained may vary; however, reported results shall be	Data retention policies	Not necessary, if Data retention policies are implemented

		retrievable for as long as medically relevant or as required by regulation. NOTE 2 Legal liability concerns regarding certain types of procedures (e.g. histology examinations, genetic examinations, paediatric examinations) may require the retention of certain records for **much longer periods** than for other records.		
Recital 39	Integrity and confidentiality appropriate security of the personal data (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage);	4.13 Control of Records Facilities shall provide a suitable environment for storage of records **to prevent damage, deterioration, loss or unauthorized access** (see 5.2.6). NOTE 3 For some records, especially those stored electronically, the **safest storage** may be on secure media and an offsite location (see 5.9.4). 5.2.2 Laboratory and Office Facilities Medical information, patient samples, and laboratory resources are **safeguarded from unauthorized access**. 5.2.3 Storage Facilities Storage space and conditions shall be provided that ensure the **continuing integrity** of sample materials, documents, equipment, reagents, consumables, records, results and any other items that could affect the quality of examination results. 5.10.2 Authorities and Responsibilities The laboratory shall ensure that the **authorities and responsibilities** for the	Data transfer and data sharing agreements Data processing agreements Security policies	Security policies that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

		management of the information system are defined, including the maintenance and modification system(s) that may affect patient care. 5.9.1 Release of Results Results are legible, without mistakes in transcription, and reported to **persons authorized** to receive and use the information. Processes shall be established for ensuring that results distributed by telephone or electronic means reach only **authorized recipients.** Results provide orally shall be followed by a written report. There shall be a record of all oral results provided.		
33-34	Data breach notification requirements;	5.9 Release of Results The laboratory shall establish documented procedures for the release of examination results, including details of who may release results and **to whom** and processes for ensuring that results distributed by telephone or electronic means **reach only authorized recipients.** Results provide orally shall be followed by a written report. There shall be a record of all oral results provided.	Data breach notification procedure should include: Description of the nature of the breach; Identification of the number of the data subjects affected by the breach; Description of the likely consequences of the breach; Description of the measures taken or proposed to be taken to remedy the breach. Should be considered that there is a tight deadline of 72 hours for the notification.	Data breach protocols and Incident response plans, which have to be implemented anyway under ISO 15189.

7-9 Recital 161 Recital 33	Valid consent necessary (including process of children's data). Consent may be withdrawn easily at any time.	5.4.4.1 <u>Primary Sample Collection and Handling</u> All procedures carried out on a patient need the **informed consent** of the patient. 5.4.2 <u>Information for Patients and Users</u> The laboratory shall have information available for patients about the laboratory's policy on **protection of personal information**; The laboratory shall have information available for patients and users that includes an explanation of the clinical procedure to be performed to enable **informed consent**. Importance of provision of patient and family information, where relevant (e.g. for interpreting genetic examination results), shall be explained to the patient and user.	There is a requirement to request informed consent for processing (otherwise stop!) and to be able to demonstrate this. Procedures need to be in place for this and records demonstrating the consent must be protected and retained. For the purpose of consenting to the participation in scientific research activities in clinical trials the relevant provisions of Regulation (EU) No 526/2014 should apply. It is often not possible to fully identify the purpose of data processing for scientific purposes at the time of data collection. Therefore data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research Withdrawal of consent implies the capability to locate and remove the personal info, perhaps during its processing and maybe also from backups and archives.	Implemented consents Implemented Data retention policies