Arkivum

Get Prepared for GDPR
in Life Sciences

Prepared by Arkivum

Arkivum

How to prepare for GDPR compliance: Life Sciences

The EU General Data Protection Regulation (GDPR) represents a sea change in data protection, and nowhere more so than in Life Sciences. In a matter of months, individuals such as patients and clinical trial subjects will enjoy a raft of new rights concerning the personal data you hold about them.

Coming fully into effect in May 2018, the General Data Protection Regulation (GDPR) centers on the rights of individuals, giving them much more control over their personal data. Punitive penalties of €20million or 4% of global turnover make compliance business-critical.

> In a sector that processes large volumes of personal data, the guiding GDPR principle of data minimization – holding only data that is needed for specified purposed and that has been subjected to consent – is challenging. GDPR redefines consent as something that must be freely given and explicit, and the individual must be informed of all proposed uses at the point of consent.

Consent is just one of the extensive rights that GDPR gives to what it terms Data Subjects. And the regulation is equally prescriptive about the obligations this places on data owners and processors. The accountability of the data owner for what is a stringent regulation means that life sciences need to carry out due diligence now and put an appropriate data management programme in place. Many life sciences organizations may also act as processors, of clinical trial data for example, and will need to pay attention to the detail of the regulation, even if the Data Controller is ultimately accountable.

Crucially, GDPR has even higher standards around the processing of sensitive personal data. The key categories here, for the life sciences, are health-related and genetic data. This paper includes guidance in this critical area.

If yours is one of the 45% of organizations without a structured process in place to comply with GDPR then read on for clear guidance through the complexities of this far-reaching data protection regulation.

The GDPR Essentials You Need to Know

GDPR at a Glance

The EU General Data Protection Regulation (GDPR), which comes into force in May 2018, tightens security around data that can be used to identify an individual person. Institutions will now have a "duty of care", requiring them to protect personal information from loss, alteration or unauthorized processing.

Whether you are just starting to think about GDPR or have an action plan in progress, here are the headline areas your organization needs to address:

Data Rights: GDPR gives individuals, or Data Subjects, unprecedented rights over their personal data. We give more detail on this in a separate section below.

Customer consent: Customers must be fully informed of every use of their personal data, and give their explicit consent freely on that basis.

Privacy by design: Organizations need to design GDPR compliance into all new products, services, systems and processes.

Data breach notification: GDPR gives organizations just 72 hours, once aware, to notify supervisory authorities that they have been subject to personal data breach.

Data Protection Officers*:* Organizations that monitor personal data regularly, and on a large scale, will need to appoint a Data Protection Officer.

Data location: Organizations will need to be able to locate the processing of personal data at all times, and follow stricter rules about data held or transferred outside the EU.

Impact outside the EU: The impact of GDPR extends beyond the EU, applying to EU governments and businesses that process the personal data of any citizen in the world, and any organization in the world that processes the personal data of EU citizens.

GDPR and Brexit: The UK has now cleared up any uncertainty around the impact of Brexit on GDPR, by committing to updating its data protection laws in line with the EU regulation.

Prohibited data categories: The processing of data in the following categories will be strictly controlled – children, genetic data, biometrics and health.

Life Sciences organizations should be aware of a small number of exceptions to the GDPR prohibited data categories. These can include situations where processing:

- Has been given explicit consent by the individual, and is for specified and lawful purposes.
- Is in the 'vital interests' of the individual.
- Is necessary for preventive or occupational medicine or for public health.

We recommend that organizations take specialist advice on any of the above scenarios when carrying out clinical trials or managing patient identifiable data.

The Rights of the Data Subject under GDPR

GDPR gives Data Subjects – synonymous with individuals such as your customers and other stakeholders – an array of rights concerning personal data that can be used to identify them, either:

- **Directly** – such as date of breach, identification numbers and location information, or
- **Indirectly** – including achievements, beliefs and ethnicity.

Under GDPR, your customers and stakeholders will have the following rights over any personal data you hold about them:

- ***Right to access:*** The Data Subject will have the right to know if you are processing their personal data, for what purpose, and precisely what data you are processing.
- ***Right to rectification:*** You must rectify and inaccurate personal data as quickly as possible on request.
- ***Right to portability:*** Individuals can obtain their personal data and have it transferred to another organization free of charge.
- ***Right to object:*** Individuals can object to specific processing of personal data, such as profiling for direct marketing.
- ***Right to erasure (or the right to be forgotten):*** Individuals can ask you to delete personal data that has outlived its agreed purpose.

How to Prepare for GDPR

In this section we will look at the responsibilities of the Data Controller and Data Processor – two roles defined by GDPR with important responsibilities for safeguarding personal data. We will then explore how GDPR maps into the data management lifecycle. Finally, we will take a brief look at Arkivum long-term data management modules and how they can help you comply with GDPR.

What is a Data Controller?

The Data Controller is the organization that is responsible for the personal data, determining its purpose and processing. The Data Controller may outsource processing to a Data Processor, but will remain liable for the personal data under its care. If your organization has a direct functional relationship with the Data Subject that goes beyond simply processing its data, then it is a Data Controller.

To be GDPR compliant, the Data Controller must:

- Put organizational measures in place to comply with GDPR, such as data protection policies and codes of conduct.
- Store and provide access only to the personal data that is required for stated purposes.
- Make sure systems handling personal data have all the capabilities needed to protect personal data.
- Ensure any Data Processors employed have technical and organizational mechanisms in place to manage compliance.
- Keep detailed records of all processing activities.
- Safeguard confidentiality, integrity, availability and resilience of data processing by working with the Data Processor to put in place data security mechanisms to:
    - Pseudonymize and encrypt personal data
    - Restore access to personal data in a timely manner following downtime
    - Assess and test data security arrangements on a regular basis.
- Restrict handling of personal data to authorized processors.
- Notify both the GDPR supervisory authority and the Data Subject of a personal data breach within 72 hours of becoming aware of it.
- Carry out an impact assessment where personal data is at risk - for example when introducing new technologies - and consult the GDPR supervisory authority on any high risks identified.
- Appoint a Data Protection Officer, if required.
- Cooperate with the GDPR supervisory authority on request.
- Manage any conflicts and overlaps between GDPR and MiFID II. Inform the Data Processor of any additional requirements.

What is a Data Processor?

The Data Processor can be an organization, person or automated mechanism that processes data under the instructions of the Data Controller, and takes adequate measures to protect any personal data.

To be GDPR compliant, the Data Processor must:

- Work with the Data Controller to put in place the security mechanisms needed to protect personal data.
- Process personal data only within the remit of a legally-binding contract, and according to documented instructions of the Data Controller.
- Delete or return personal data to the Data Controller at the end of the contractual relationship, unless retention is required under EU or national law.
- Be able to demonstrate full operational compliance with GDPR at all times.
- Make sure all authorized persons are legally bound to confidentiality.
- Obtain authorization from the Data Controller if planning to engage another processor.

- Keep detailed records of all processing.
- Notify the Data Controller of a personal data breach as soon as possible and give support as required.
- Consult the Data Protection Officer, where one is appointed, on all issues concerning the protection of personal data.
- Assist the Data Controller in responding to requests for exercising data subjects' rights.

Addressing GDPR in Your Long-Term Data Lifecycle Management

Long-Term Data Lifecycle Management is a set of policies and processes for overseeing all data - not just the personal data covered by GDPR - from creation and initial storage, through to its performance and integrity in usage, up to the point where it becomes obsolete.

If your organization has yet to embed long-term data lifecycle management processes and policies, Arkivum can advise you on implementing practices that will form a robust foundation layer for your GDPR project, making the needs of Data Subjects, Data Controllers and Data Processors much easier to manage.

For organizations that are already following good practice in data lifecycle management, this section sets out the preparation and activities necessary to manage GDPR compliance at every stage.

Following this step-by-step process will help you to know your data, minimize risk, and embed best practice in data governance – three crucial elements to data management under GDPR:

Step 1: Prepare

Most organizations hold data in disparate systems, not all of which are under their direct control. This makes planning a key stage within the lifecycle. We recommend carrying out an audit to understand, identify, locate and categorize all personal data across the organization. The results should give you a heat map of risk areas where personal data is concentrated, and this is where your efforts should be focused.

Step 2: Assess Personal Data

Organizations should then put rules in place to determine the relevancy of all Personally Identifiable Information (PII). This will help ensure that only necessary personal data is stored, and later erased once it has outlived its purpose. All instances of personal data consent should be recorded in a reportable form.

Step 3: Produce Policies for Risk Minimization and Retention Policies

Data Controllers need to put policies and procedures in place to protect personal data from loss, alteration or unauthorized processing. These should be disseminated to all Data Processors, and should cover criteria for both the retention and deletion of personal data.

Step 4: Pseudonymize Personal Data

Where possible, personal data should be stored in a dedicated location, separate from core archive content. That core data then refers to the personal data only through metadata. This makes the personal data non-identifiable in the archive. This is what we do at Arkivum when managing our clients' data, with access permissions to reinforce the separation. It reduces risk and makes it easier to limit personal identification to specific needs for defined periods of time, to comply with GDPR.

Step 5: Data Governance

Good data governance involves putting technical measures in place to demonstrate that your organization can mitigate the risks involved in processing personal data. This includes full control over storage locations, data classifications and audit logs.

Step 6: Security

As we have seen, data security is central to GDPR compliance, with the regulation stipulating specific measures such as encryption. So at this stage you need to make sure you have the security infrastructure in place to support these requirements. Arkivum provides a security solution that is compliant with the international data security standard, ISO 27001. Data is encrypted both in transit and at rest, with only the Data Controller holding the key. We make data locations clearly visible on a single dashboard, and our audit trails track all data-related activity.

Step 7: Supporting the Rights of the Data Subject

To support the array of privacy rights that the GDPR introduces, organizations need to be able to respond to requests for information from Data Subjects and put robust data access controls in place.

At Arkivum, we believe that a single repository where data can be searched and retrieved makes these Data Subject requests much easier for Data Controllers. Our GDPR-compliant infrastructure includes stringent access control rights, a comprehensive record-keeping solution, demonstrable file deletion and a packaging and extraction tool for subsets of personal data.

How Arkivum TRUST Supports GDPR Compliance

Arkivum TRUST gives life sciences organizations an end-to-end secure digital safeguarding and preservation archival solution that supports GDPR compliance on a module-by-module basis.

Arkivum Compliance Module (ACM)

The ACM provides flexible record management capabilities such as retention management, secure removal of data, evidence-ready data exports, comprehensive audit trails, chain of custody, data encryption and data sovereignty.

How will ACM help you comply with GDPR?

The ACM ensures that both Data Controllers and Data Processors adhere to all regulatory requirements, including GDPR. Its data erasure capabilities will help your organization comply with the Data Subject's right to be forgotten, and more proactively, to remove any data that is no longer required for its original stated purpose.

Arkivum Integration Module (AIM)

The AIM is a scalable and automated ingestion solution that provides quick and seamless connectivity, with out-of-the-box integration connectors, flexible APIs and drag-and-drop options.

How will AIM help you comply with GDPR?

By providing visibility across multiple systems, the AIM makes it easier for both Data Controllers and Data Processors to safeguard GDPR compliance efficiency across multiple systems.

Arkivum Safeguarding Module (ASM)

The ASM is a secure, cloud-based managed service that guarantees 100% data integrity, ensuring the highest standards of data protection at every stage of the data management lifecycle. The ASM performs validation and integrity checks on data created, and ensures that the records are encrypted. It also provides a full audit trail for all ingested records, and manages the day-to-day operations of the archive, including access control, in line with OAIS standard processes.

How will ASM help you comply with GDPR?

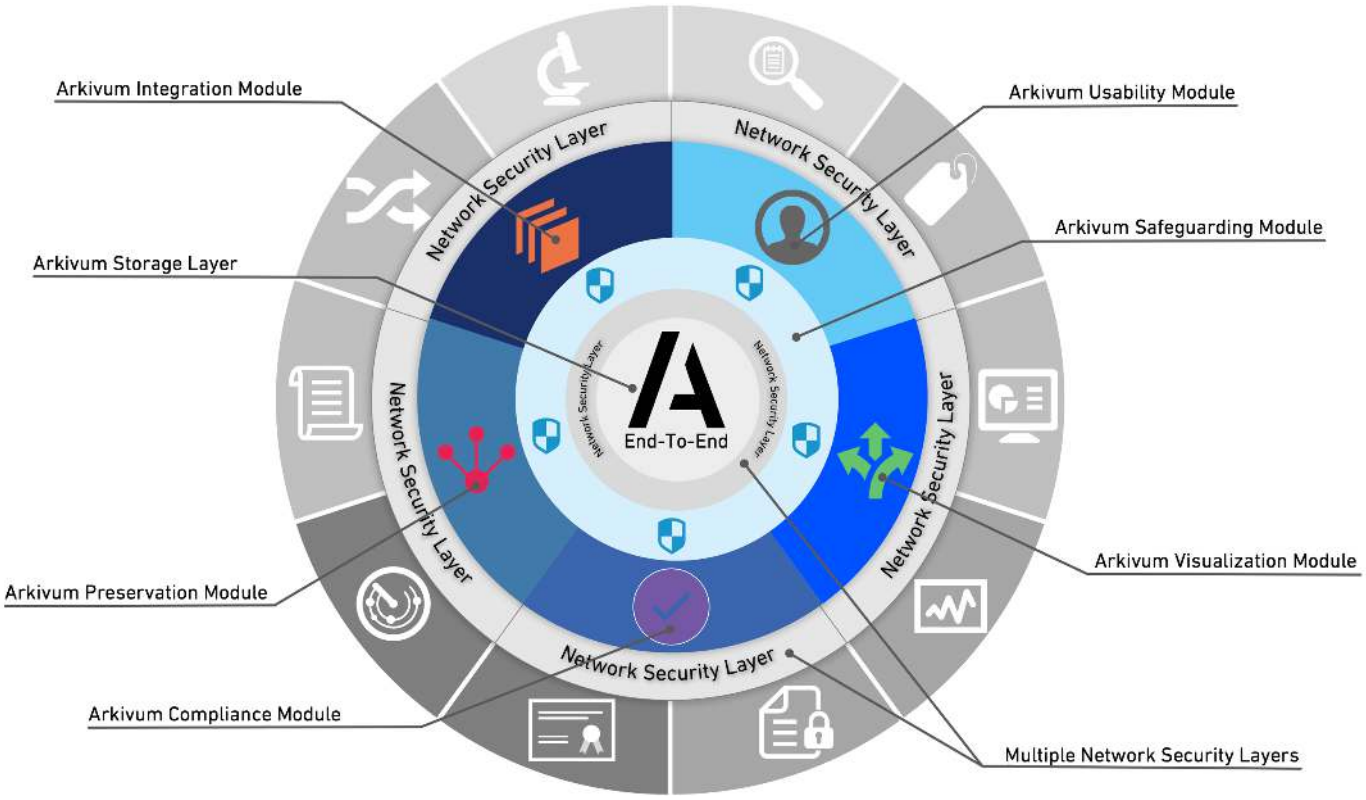
The ASM is central to GDPR compliance, keeping data secure with key capabilities such as encryption, separating off any personal information as required, and controlling the location of data at all times.

Arkivum Usability Module (AUM)

AUM improves user access to archive content, by extracting and enriching the metadata to make the content both searchable and shareable.

How will AUM help you comply with GDPR?

With permission-based restrictions, AUM can control access to and sharing of personally identifiable information. And in support of any GDPR-related investigations, AUM can perform a trusted export of data to prove the authenticity of the records in their original state, should this be required as evidence.



www.arkivum.com
hello@arkivum.com
@Arkivum