Impact on pharmacovigilance related activities

01 Background

02 What is GDPR?

06 Impact on pharmacovigilance related activities

10 The approach towards compliance
   - Pseudonymization and encryption of personal data
   - Data minimization and purpose limitation
   - Data security
   - Data protection impact assessment tools
   - Demonstration of compliance
   - Data protection by design and by default
   - Tools for accommodating data subject’s request
   - Data protection organization:
     - Contracts
     - Training

18 Conclusion
Background

Non-compliance with data protection law, An Example:
The emergence of big data promises to have a significant impact on healthcare. With the availability of large amounts of patient data, new treatments and technologies are being built for diagnosis, prognosis, and treatment of various diseases.

“Streams” is an app developed by DeepMind, a London-based Google’s Artificial Intelligence company, in collaboration with London’s Royal Free hospital. The app is built for the detection of early signs of acute kidney disease and does so by immediately alerting clinicians when a patient’s health deteriorates. As part of the clinical trial, Royal Free Hospital transferred the data of 1.6 million patients to DeepMind. In July 2017 the UK’s Information Commission Office (ICO) ruled that the transfer of 1.6 million patient records failed to comply with the Data Protection Act.

So what went wrong? The ICO had found that the patients were not adequately informed about the way their data would be used and there was a potential erosion of fundamental data privacy rights of the patients. The Data Protection Act 1998 in the UK is based on the European Union (EU) Data Protection Directive 1995 (Directive 95/46/EC) on the protection of EU citizens’ personal data. The directive regulates the processing of personal data and provides the right to the data subject to be informed when his/her data is being processed.

Although the right to data privacy laws existed in the European Union (EU) from a long time, there were several inconsistencies with regard to the enforcement of these laws across the member states. Also, there were some uncertainties with regard to the legal implications of violating these laws. These and other factors resulted in the decision to reform the existing Data Protection Directive that was adopted over 20 years ago. Consequently, the new General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council) was developed. The GDPR was adopted by the European Parliament and the European Council on 27th April 2016 and is effective from 25th May 2018.
What is GDPR?

The General Data Protection Regulation (GDPR) is a legislative document consisting of 99 articles and 173 recitals and is based on seven key principles. The regulation applies to organizations that control or process personal data of EU residents with or without a physical presence in the EU.

**GDPR principles:**

**Article 5 of GDPR** provides the basic principles that drive the data protection legislation, according to which:

- The personal data should be processed lawfully, fairly and in a transparent manner
- Data collected for specified, explicit and legitimate purposes is not further processed in a manner that is incompatible with those purposes
- The personal data collected would be adequate, relevant and limited to what is necessary
- The personal data collected and processed would be kept accurate, where necessary it would be rectified or erased
- The personal data would be kept no longer than is necessary for the purposes for which the personal data are processed
- The personal data would be secured in an appropriate manner
- The controller would be responsible for demonstrating compliance with the regulation

In summary, GDPR includes key aspects surrounding personal data and personally identifiable information (PII). So, what is personal data? According to **Article 4 of GDPR regulation**, "personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Further, PHI (personal health information) is defined as ‘data concerning health’ and it means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
An overview of the selected components of GDPR that regulate the processing of such data are described below.

**Rights of data subjects:**
The GDPR provides significant authority to the data subjects on their personal data. The data subjects can now have a clear understanding of how the data is being processed, who is it being shared to and what measures are taken to protect his/her data. The data subjects have the right to access their personal information that is being processed, right to get rectified any inconsistencies, right to get their data erased/forgotten, right to restrict processing, right to data portability and right not to be subject to a decision based solely on automated processing (Chapter 3 GDPR).

**Controller and processor responsibilities:**
According to GDPR, the controller has the responsibility to apply appropriate technical and organizational measures and demonstrate that the personal data is being processed in compliance with GDPR through documentation and approved certification mechanisms. Similarly, the compliance of the “processor” contracted by the controller should also be demonstrated through documentation and approved certifications. Additionally, the other core “controller” responsibilities include, implementing data protection by design and by default, undertaking data security measures, and conducting data protection impact assessment (DPIA).

- **Data protection by design and default:** According to the principle of “data protection by design and by default”, the tools for processing personal data should incorporate the features that aid in compliance with data protection regulation. Rather than a post hoc measure, pseudonymization and data minimization should be incorporated into the processing systems prior to conducting processing operations.

- **In order to adhere to the principle of data minimization,** the controller should ensure that only data that is required for the purpose of processing is collected, the extent of processing and storage should be in accordance with the purpose of processing. The accessibility of the personal data should be limited to certain individuals rather than to an indefinite number of individuals.

- **Pseudonymization:** As per Article 4, “pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.”
Pseudonymization is an important technical measure that is required to be taken by the companies for processing of personal data and is mentioned in the GDPR in multiple provisions:

- It is a core basis of implementation of the GDPR requirement of “data protection by design and by default” (Article 25)
- Pseudonymization forms a crucial foundation for appropriate safeguards required for legalizing the processing of personal data (Article 6)
- It would be a component for the code of conduct for “processors” and “controllers” (Article 40)
- Pseudonymization, along with encryption of personal data, are the primary security measures for data privacy that the “controllers” or “processors” of personal data are expected to implement (Article 32)

**Processor responsibilities:** The processor should have all the technical and organizational measures in place for compliance with GDPR as applicable to the controller. The language and terms of the contract between the controller and processor should be in compliance with the regulation. The contract should include subject-matter and duration of the processing, nature, and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller (Article 28). The processor should only process the personal data of the data subjects under the instructions of the controller.

**Data Security:** GDPR provides a risk-based approach for instituting the security measures for personal data processing operations. The security measures that a controller is expected to take include:

- The pseudonymization/encryption of personal data
- The processing systems with the ability to ensure the ongoing confidentiality, integrity, availability, and resilience
- Disaster management
- A process for regularly testing, assessing and evaluating the effectiveness of security measures

**Data protection impact assessment:** Prior to conducting processing operations, the data controller is required to perform an impact assessment of processing on a data subject’s right to privacy. The assessments include risk assessment, risk evaluation and the measures taken to alleviate the risk of violation of the subject’s right to data privacy.
**Data Protection Officer (DPO):** The industries that conduct regular and systematic monitoring of data subjects and processing of large scale personal data, are required to appoint a Data Protection Officer (DPO) as per GDPR Article 37. For entities established outside the European Union, a representative in EU should be designated for data protection-related issues. The representative will be responsible for communication with the supervisory authorities and data subjects on issues related to processing and compliance with GDPR. The role of the DPO would be to assist the organizations to ensure compliance with GDPR, therefore the person should have sufficient expertise in data protection law. One of the means for demonstrating expertise of a DPO is certifications such as Certified Information Privacy Manager (CIPM), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) from organizations like International Association of Privacy Professionals. Apart from the specialized data protection team/DPO, the staff working on data collection and processing data should be trained on GDPR.

The core “Controller” responsibilities include implementing data protection by design and by default, undertaking data security measures, establishing a Data Protection Office and conducting data protection impact assessment (DPIA).

**Transfer of personal data:**

There are certain restrictions imposed on the transfer of the personal data from the EU to the international organizations. The controller can transfer the personal data to the countries or organizations outside the European Union (EU) where the European Commission (hereafter referred to as ‘Commission’) has decided that the country or organization could ensure an appropriate level of protection to the personal data of EU citizens. In the absence of adequacy decision by the Commission, transfer of the personal data can be conducted based on the presence of appropriate safeguards. Transfers are also allowed under certain situations such as explicit consent from the data subject, transfer due to the public interest, and to protect the vital interest of the data subject (Figure 1).

The enforcement of GDPR in the EU is having a cascading effect on the data privacy laws across other countries. For instance, Japan has made recent changes to the Act on Protection of Personal Information and includes topics similar to the EU-GDPR, such as consent for sensitive data, transfer of data, legitimate international transfer of personal information.

China’s cyber security and data protection law has been changed to include regulations related to collection and use of personal information, data breach, and data subject’s rights.
Impact on pharmacovigilance-related activities

In this paper, the authors would like to share the approach they have adopted to establish and express their understanding and interpretation of GDPR. ArisGlobal has studied the GDPR in its entirety, and the opinions expressed in this position paper are limited to the sections that ArisGlobal feels are relevant to pharmacovigilance (PV) industry and its stakeholders. The authors have attempted to understand and define the changes to ArisGlobal’s safety products in order to ensure compliance with the spirit of the GDPR regulations.

This paper should be read by marketing authorization holders (MAHs) in conjunction with their own interpretation of GDPR and its applicability to their processes. This is important to note, as every organization has its own policies, procedures and working practices.

The principles of GDPR aim towards building a sustainable approach for utilizing the personal data in pharmacovigilance to improve health outcomes. The data protection regulation aims to protect an individual’s sensitive data, resulting in greater public confidence in how their personal data is being utilized.

According to these requirements, the MAHs should collect as much information as possible on the suspected drug-related adverse events. Typically, the PV data may include information that identifies the patient and the reporter, and the personal information such as age, weight, height, ethnic origin and health status. The personal identification and contact details may also be collected if there is a follow-up to the adverse events required. All these data fall under the category of “personal data” according to GDPR Article 4. The life sciences industry and the clinical research organizations (CROs) therefore inherently fall under the governance of GDPR as they are either “controllers” or “processors” of the “personal data.”

Consent: The GDPR considers obtaining data subject’s “consent” before processing his/her data, as the fundamental basis of data protection law. An explicit consent is obtained from the participants in the clinical trials for conducting trial-related activities including processing of their personal data. However, no such consenting process exists for pharmacovigilance. In most of the cases, it might not be feasible to obtain a consent from the data subjects as they may not always be the reporters of the adverse events. GDPR provides special provisions in such cases. According to GDPR recital 33, “It is often not possible to fully identify the purpose of personal data processing for scientific research 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 recognized ethical standards for scientific research”.

Data subject’s rights: Although GDPR may provide some exceptions to obtaining a data subject’s consent for processing personal data for pharmacovigilance, the data subject, however, has the right to protection of his/her personal data submitted for pharmacovigilance purpose. The GDPR-specified subject rights and possible derogations are:

- **Right to access:** Although processing of personal data is allowed for pharmacovigilance, when requested the controllers should provide the relevant information regarding their personal data to the data subjects. Some of the important elements that should be provided to the subject are: purpose for collecting the data, the type of personal data that is being processed, the recipients of the personal data such as case processing vendors and regulatory authorities, the period of retention of personal data, other data subject rights, and existence of automated decision-making (Article 15).

- **Right to erasure:** According to Article 17, the data subjects have the right to have their personal data erased or forgotten. However, if the processing of the personal data is required for reasons of public interest in the area of public health such as pharmacovigilance, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes such as clinical trials, the right to erasure shall not apply.
• **Right to restriction of processing:** The data subject has the right to restrict the processing of his/her personal data for various reasons such as suspected inaccuracy of personal data. However, if the processing is required for the reasons of important public interest, such as pharmacovigilance or clinical trials, the data may be processed with the data subject’s consent (Article 18).

• **Right to data portability:** The data subject has the right to receive the personal data that is processed, in the commonly used, machine-readable format and has the right to transfer his/her data to another controller. The exception is made for tasks that are performed in public interest, such as post-marketing surveillance (Article 20).

• **Right to object:** The data subject has the right to object to the processing of personal data. When the data is processed for scientific or historical research purposes or statistical purposes, the data subject still has the right to object, however it is the controller’s responsibility to demonstrate the legitimacy of processing the data (Article 21).

• **Right to profiling:** Although further guidance on this provision is required from the European Data Protection Board, this right provides an individual not to be subject to a decision based on automated processing, including profiling that might result in any discriminatory effects on the individual. Further, Recital 71 mention’s that “Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.” Hence there needs to be further guidance on the implication of this provision on clinical trials and post-marketing surveillance (Article 22).

• In pharmacovigilance, the algorithms used for analysis and signal detection should include appropriate scientifically proven statistical methods in order to prevent any inaccuracies in decision making based on the automated processing.

Pharmacovigilance data entry into the database:

The adverse event reports that MAHs receive, include elements that are essential for pharmacovigilance as well as non-essential information. In accordance with the data minimization principle, after receipt of the pharmacovigilance data, the essential and non-essential elements should be sifted and only the essential elements should be retained. The data elements generally considered essential for pharmacovigilance are patient ID, date of birth, age at onset, ethnic origin, symptoms of an adverse event, duration of experiencing an adverse event, resolution/outcome, suspected drug, concomitant medication and medical history. The non-essential elements could include patient name, contact address, phone numbers, email address, hospital admission details and medical reports not related to the condition of interest. If the adverse event report is obtained from the HCP, the contact address may be required for conducting follow-up. The non-essential personal data should be anonymized or redacted.
Processing of pharmacovigilance data:

Based on the principle of data minimization and purpose limitation, the personal data provided for pharmacovigilance should not be processed for any other purpose. As mentioned above, the MAHs should only process and hold data that is required for pharmacovigilance. The duration for which the personal data will be stored should be conveyed to the subject. The MAHs cannot hold the personal data after the expiry of the data storage period. The duration of pharmacovigilance data storage is detailed in pharmacovigilance-implementing regulationix. According to this regulation, all pharmacovigilance-related documentation should be retained until the medicinal product is in the market and until 10 years after the product is withdrawn from the market.

Data transfer to international organizations:

In pharmacovigilance, the personal data of the EU citizens may be required to be transferred to international locations if the case processing or other PV tasks are outsourced. Alternately, it is possible that the PV data entered into the database may be accessed through locations outside the EU, or may be backed-up outside EU, or may be transferred to other regulatory authorities. If the international locations do not comply with the adequacy requirements of GDPR, such activities may result in GDPR violation. The MAHs should ensure that relevant systems are in place to avoid violation of GDPR regarding international data transfer.

Data security:

All appropriate security measures should be taken to protect the personal data collected for pharmacovigilance purposes. The personal data should be protected from unauthorized access and accidental data loss. The PV database systems should be validated and tested periodically and the system should restrict access to only a selected number of authorized staff. The PV database should be able to track all changes to personal data and should be able to create an audit trail of the same.

When outsourced to service providers for processing (called ‘processors’), the MAHs should ensure the security measures are GDPR compliant, even if they are located outside the EU.

Data Protection Officer:

As core activities of MAHs and CROs involve regular and systematic monitoring of data subjects and processing of large scale personal data, they are required to appoint a Data Protection Officer (DPO) as per GDPR Article 37. For the MAHs or CROs established outside the European Union, a representative in EU should be designated for data protection related issues.
The approach towards compliance

As a pharmacovigilance solutions provider, ArisGlobal supports compliance with the GDPR. The pharmacovigilance software providers and other enterprises can achieve compliance by incorporating appropriate changes at the level of product, process and people.

Pseudonymization and encryption of personal data:

Assessment of personal data:

As an initial step in securing personal data, the enterprises should conduct an audit for personal data discovery to map and understand the following:

- Categories of personal data processed (e.g., personally identifiable information (PII), health information, etc.)
- Types of personal data processing
- Purposes of personal data processing at a granular level
- Locations of personal data in the entire data lifecycle
- Parties involved in the processing of personal data
- Formats of personal data processed (e.g., digital or physical)
- Amount of data processed
- Automated processing of personal information

The enterprises can use data flow diagrams to understand the location of personal information and flow of such information. The diagrams should at least include the details of individuals, the formats and the time-points related to the collection / processing / storage of personal information.

Encryption of Personal Data Fields

Some of the current PV solutions may include certain optional features of data privacy, while others do not include such features. Optional implementation of Data Privacy features may lead to uncontrolled management of personal information of customers leading to an increased exposure and risk of GDPR noncompliance. For instance, personal identifiers may be visible in database audit tables if data privacy feature is not enabled. This may lead to personal data leakage. The MAHs should ensure that encryption of all relevant data fields that include personal information is set as default configuration.

The PV application should enable encryption of all fields that contain personally identifiable information (PII), including fields such as case history. The solution providers can include guidelines listing the fields which are covered / not covered in data privacy module and inform the users that they should not include personal information in the fields that are not covered in data protection module.
Generally, the safety information about a medicinal product is initially received in the form of unstructured narratives that may include personal information of data subject.

- Such documents should be redacted before undergoing a triaging process for inclusion in a PV database. The MAHs should establish a mechanism to ensure that all safety information is redacted appropriately. Applications that support the management of redacted copies of unstructured documents should be leveraged.

- Further appropriate safeguards should be in place for storing the original unredacted and unencrypted documents. After the initial purpose of triaging the safety events is fulfilled, the original document containing the personal information should be encrypted.

- The case data of individuals is included in the PV application in the XML format. The PV applications should ensure that the unencrypted XML files are either protected or removed from the application server archive folders.

- The libraries maintained in the central PV database of parents, investigators, medical practitioners of the patients which adverse events should be encrypted.

- ArisGlobal recommends the usage of more sophisticated algorithms for encryption such as AES 128 bit.

The data privacy module in ArisGlobal's LifeSphere Safety™ applications consider the PII to be encrypted. The MAHs should ensure that the PIIIs are not included in other locations such as narratives and in email communications, e.g., in the subject line of an email. The source documents and any other documents related to a case will also be encrypted in the database. For example, in LifeSphere Safety MultiVigilance™, ArisGlobal's safety and case management system, the storage of personal information of data subjects in libraries in the central database will be encrypted.

For MAH's that use LifeSphere Intake and Triage™, the IRT module of ArisGlobal, encryption is being introduced at the database level. This is to ensure IRT users, who should not have access to PII in the application, are restricted at the receipt level. This will ensure that in scenarios like duplicate search, follow-up, etc., data privacy is maintained.

In the communication module, the application ensures that the PII of the reporter will be accessible to the privileged users only.
Data Encryption Keys:
The encrypted customer data that is stored within the application database includes PII. If the associated encryption keys are stored within the same database, this may lead to higher probability of a compromise by a malicious individual who has gained unauthorized access to the database. Therefore, a separate key management system should be implemented that should be designed in a manner to fulfil the objective of denying access to the data encryption keys to the individuals having access to the customer data in the central database.

The usage of same encryption keys during development, staging and operations may lead to continued access to individuals who are not required to access the customer data post the fulfilment of their purposes. Further, the usage of older encryption formats may lead to increased risk to customer data breach due to weak security protocol.

ArisGlobal recommends that MAHs should ensure a key management process is developed so that the encryption key is appropriately backed up and exchanged with other parties in a secure manner. ArisGlobal is also making change in its LifeSphere Safety applications, to ensure that the encryption key is stored securely with a restricted access. The MAHs should ensure that access is restricted to privileged users.

Data minimization and purpose limitation

Exposure to personal data
The PV solution providers should limit their exposure to personal data from MAHs or any other data controllers or processors. The exposure to personal data may occur either during application development, testing, validation or production purposes or during trouble shooting. In order to prevent such exposure to personal data, solution providers should implement a process to identify the current exposure levels to personal data, the nature of personal data that is being received, and the purpose for which it is received. Further, they should evaluate the means by which such exposures to personal data can be limited when it is not required. A Privacy Impact Assessment (PIA) should be performed for every process to ensure that the personal information collected is for a requisite purpose.
Customer property management

The PV solution providing enterprises should update the existing Customer Property Management Process to include implementation of appropriate safeguards by the data controllers and processors prior to receiving personal information, e.g., encryption of hard disks containing personal information. Alternately, the PV solution providers can use a masking script for the personal information extracted from the cloud environment or to the personal information obtained directly from the customer in hard disks or through SSH File Transfer Protocol (SFTP). This script should redact the personal identifier fields such as name, mobile number, address, etc.

The PV solution providers should evaluate the purpose for which the Personal Information is collected, processed and retained and for instances where the defined and agreed purpose have been accomplished, the original customer data dump received directly from the customers or extracted from the cloud environment should be appropriately destroyed / disposed or anonymized if there is a need to retain the original copies.

Safety database access

The IT service team may have to access the safety database periodically if there are issues reported. In order to allow the traceability and the accountability of the personnel who could access the personal information in the database, it is recommended that unique named accounts IDs are used to log-into database. Alternately, if generic account IDs are used, a Generic Account Management Process should be established. Some of the recommendations for the process are:

- Identification of an owner for a particular generic account
- Need-based and duration-based access
- Managed account access requests
- A review mechanism to validate the generic account access requests raised

A periodic review of all user access accounts should be performed to validate authorized access to the customer instances.

The companies should institute a Personal Data Sharing Tracking Form for capturing the details of the individuals with whom the personal information from customer data is being shared. This form can be leveraged to maintain the list of individuals who are exposed to personal information.
Retention of files containing personal information of data subjects in an unencrypted format on the application server beyond purpose (input files in archived folders, reports on application server) may lead to increased probability of a personal data breach. Copies of documents are likely to be available on other locations such as the report server, distribution server, ESM folders, in addition to the archive folders. Therefore, access should be restricted to these locations.

For the MAHs on Cloud, ArisGlobal will ensure that the files/documents are access controlled and are periodically removed beyond their retention period from locations like report server, distribution server, ESM folders, archive folders, IRT/OST/CCM email inboxes and attachments in the communication module.

For MAHs using on-premise installations, it is the MAH’s responsibility to ensure that documents are access controlled and are periodically removed beyond their retention period in above mentioned locations.

**Data security**

**Real-time security management**

The MAHs should consider implementing a real-time security monitoring process for leveraging the logs of activities collected from systems. There should also be a real-time security operations center that enables reporting the security breaches and appropriate actions to be taken in a timely manner within the breach notification window of 72 hours.

**Security incident management**

The data breach plan and security incident management plan should identify personal data as confidential or restricted data and tampering of personal information as a privacy incident. The process for reporting and initial handling of data breaches should at least include:

- Definition of type of breaches to be reported by users (e.g., lost USB drives, lost mobile devices and alerts from anti-virus systems to the service desk or similar)
- The mechanism of recording a breach
- Determining a contact point for reporting a breach (e.g., the help desk, service management or similar)

In addition, the companies should consider using automated tools for detection of suspected personal data breaches.
The investigation of personal data breaches should include at least the following elements:

- Details on time, location and system or service breached
- Relevant information from application and system event logs and alerts
- Information from law enforcement, social media platforms and hacker websites
- DPIA for the affected system that describes whether personal data is processed

The MAHs should create or update a personal data breach notification procedure and should develop a process to determine the level of risk to the rights and freedom of natural persons in the event of a personal data breach.

**Data protection impact assessment tools**

Personal data privacy should be considered as an integral part of the Risk Assessment Procedures and MAHs should conduct periodic risk assessments related to data privacy. The risk assessment procedures related to data privacy can be a two-step process:

- Determining if the processing requires privacy impact assessment (PIA)
- Conducting privacy impact assessments (PIA):

The process for conducting a PIA may include:

- Determination of the scope of the PIA
- Review the criteria for processing personal data such as:
  - Data processing is necessary to achieve its intended purpose
  - It is proportionate to individuals’ rights and freedom
  - It is adequate, relevant and not excessive
  - It is compatible with the purpose for which the data has been collected
- Assess the risks of data privacy breach
- Evaluate measures that will address the risks
- When assessing the impact, factors such as: type and volume of personal data that will be processed (e.g., special categories, financial information, children’s data and name/address), nature of processing performed (e.g., storing, profiling, analyzing for medical research) and whether the processing may be perceived by data subjects or the media as intrusive or excessive, should be considered
- Subsequently, a risk mitigation plan should be developed and implemented if warranted
Demonstration of compliance

The PV applications should be able to produce audit logs for all activities involving personal data handling such as entry, modification or deletion of personal data. Additionally, activities such as executing a query or extraction / export of personal data from the application should be captured in a log. Absence of logs for activities like data export (such as reports) may lead to a reduced traceability.

All major actions like exporting data, generation of reports, downloading the source documents are captured in ArisGlobal applications’ audit trail. All the audit trail reports have an option to view the encrypted/decrypted data based on the user privileges. Logs like admin server logs or the server trace logs generally capture all the actions in a decrypted format and are used for purposes like trouble shooting. The ArisGlobal applications will have the data privacy fields excluded from these logs. The MAHs should ensure that the access to these reports is restricted to privileged users.

Data protection by design and by default

According to the principle of “data protection by design and by default,” the tools for processing personal data should incorporate the features that aid in compliance with data protection regulation. Rather than a post hoc measure, pseudonymization, encryption and data minimization and data security measures should be incorporated into the processing systems prior to conducting processing operations.

The PV solution providers should ensure that privacy measures are implemented at a design level within the application. They should ensure that the principles of data privacy are integrated into architecture and design. They should consider de-identification of personal identifiers of data subjects from the entire application environment unless explicitly required for a business purpose. Personal information of data subjects should not be used during application development and application testing phases unless absolutely required due to a justified business purpose. The companies should ensure implementation of a Privacy by Design document during application development and deployment. The implementation of “Privacy by Design” should be reviewed and validated periodically.

ArisGlobal provides an option to enable data privacy at the database level via configuration of the applications. Since, every MAH may have different processes for achieving data privacy, default encryption of all fields in the ArisGlobal’s applications could result in restricting MAHs from applying their own processes. Therefore, ArisGlobal has chosen not to provide data privacy as a ‘default-configuration’ in the database via the application. However, through the option of combining technical and organizational measures, MAHs will be able to achieve compliance with the GDPR provision of “data protection by design and default.”
Tools for accommodating data subject’s request

**Erasure of personal data:** The PV applications should allow complete erasure of personal information of an individual from the application environment based on a valid request from a data subject. Methods and systems should be developed for erasing personal data relating to a data subject from the identified locations.

MAHs should establish a process to act on the data subject’s request for erasure of personal information.

**Data portability:** The PV applications should allow identification and packaging of the collected personal information of an individual into structured, commonly used and machine-readable format on a valid request from the data subject. A data portability form should be developed that highlights the personal information and is able to uniquely identify the requester to ensure that the requests are made by a legitimate person.

MAHs should define a process to address the data subjects request on data portability. ArisGlobal’s applications support the extraction of required information in a structured machine-readable format. As this might vary based on a specific request, this will be a customized activity.

**Data protection organization:**

To ensure adequate governance with regard to implementation of GDPR, a Privacy Organization should be established within the MAH’s enterprise.

**Contracts**

If MAH’s take the services of other organizations for activities that involve processing of personal data, data privacy impact assessments should be performed. If any risks are identified appropriate safeguards should be provided. Legal instruments like Non-Disclosure Agreement, Data Processing Agreement, etc., should be included in the process and responsible staff should be appropriately trained on privacy requirements.

**Training**

All employees in the enterprise who will be involved in development of applications for handling the personal information and employees who will be handling the personal information should be trained adequately on GDPR.

ArisGlobal is ensuring that all of our personnel involved in development of applications will undergo training on GDPR.
Conclusion

According to the EU pharmacovigilance regulation (comprising of Directive 2010/84/EU and Regulation (EU) No 1235/2010) MAHs are required to collect and process data of all adverse events. However, since this data also includes personally identifiable information, the controllers and processors of the pharmacovigilance data fall under the governance of GDPR.

In order to be compliant with GDPR, the MAHs should incorporate the principles of data privacy such as purpose limitation, data minimization, confidentiality and accountability into their processes, systems and organization. Some of the key measures that a data controller should undertake in order to ensure compliance are pseudonymization/encryption of PII, data security, minimize access to safety database, institute a security incident management process, conduct impact assessments, and demonstrate compliance. All these and other measures should be incorporated into their PV systems by “design and by default.”

Overall, ArisGlobal is making the necessary changes in their LifeSphere Safety applications to support the implementation of the new EU GDPR. In order to be compliant with the regulation, MAHs should re-define their processes and incorporate data privacy enabled solutions into their pharmacovigilance activities.

Authors:

Dr. Vivek Ahuja, Vice President, Global Pharmacovigilance, ArisGlobal
Maithili Dokuparti, Senior Manager, Pharmacovigilance, ArisGlobal
Dr. Karna Shetty, Associate Director, Safety Business Unit
Mohan Kuman Adisesha, Director, Product Management, Safety Business Unit

1https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act
3http://www.eugdpr.org/
4https://iapp.org/
About ArisGlobal

ArisGlobal is a visionary technology company that’s transforming the way today’s most successful life sciences companies develop breakthroughs and bring new products to market. The ArisGlobal LifeSphere® cognitive technology platform integrates machine-learning capabilities to automate the core functions of the product lifecycle. Designed with deep expertise and a long-term perspective that spans more than 30 years, our cognitive platform delivers actionable insights, boosts efficiency, ensures compliance, and lowers total cost of ownership through multi-tenancy.

Headquartered in the United States, ArisGlobal has regional offices in Europe, India and Japan. For more information, visit arisglobal.com or follow ArisGlobal on LinkedIn and Twitter.

© 2018 ArisGlobal LLC. All rights reserved. All trademarks are the property of their respective owners and are acknowledged as such.