RxLogix Corporation -

Effective Date:	20-Nov-2019
Document Number:	POL-001
Version:	2.0

Confidentiality

This document contains proprietary information. Unauthorized copying or disclosure is prohibited.

RxLogix firmly believes in maintaining the highest principles of professional ethics and adheres to the confidentiality agreements of the respective parties. RxLogix has demonstrated the ability to develop quality solutions while maintaining full confidentiality.

Revision History

Version	Author	Date	Description of Change
1.0	Jayashree P K Acharya	25-Mar-2019	Initial document
2.0	Jayashree P K Acharya	24-Oct-2019	Updated the document to reflect sections on implementation approaches

Template: RxL-TMP-SOP-001, Version 7.0; Effective 01-Aug-2019

Table of Contents

1.0 PURPOSE

RxLogix is a global pharmacovigilance solutions company specializing in innovative software and expert consulting services. In our pursuit to satisfy our Customers we provide business and technology innovations in the space of Pharmacovigilance and Risk Management. These solutions help increase the compliance, productivity and quality for the entire Drug Safety value chain. As part of providing these value-added software and cloud-based solutions, we understand that ensuring patient safety while advancing medical and scientific research is vital to life sciences companies.

The objective of this position paper is to explain the approach and controls put forth by RxLogix corporation to honour the expectations of the EU General Data Protection Regulation (GDPR henceforth).

2.0 SCOPE

RxLogix works on a Proven business model of providing multiple services to their Customers, extending from Product Implementation of their developed Products, System Integrators with proven Industry best Pharmacovigilance solutions, Hosted solutions and other services as part of ‘Managed Services’.

As part of these solutions that we provide, we assume the role of ‘Data Processor’ as means of processing that set of personal data entered by end user organizations using our Software Solutions which may or may not contain personal data or on sets of personal data, whether or not by automated means, and store these data as part of our hosted solutions. The scope of work undertaken with each End User Organisation is in accordance with a mutually signed off Contract.

RxLogix does not by any means engage in interacting with data subjects nor engage in collection, eliciting, organization, structuring, adaptation or alteration, retrieval, consultation, use, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction any such data.

RxLogix has introduced various measures as part of the Product Design and Service offering, to comply with the needs laid out by this Regulation. The detailed elaboration of the approaches are described in the Quality Management System, mutually agreed Contracts and other enforceable approaches.

These controls implemented by RxLogix to adhere the expectations of this regulation span across following levels:

- Organization
- Product
- Process
- Personnel
- Cloud Infrastructure Management

3.0 What is GDPR

The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). This provides directions on export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and is designed to:

- Harmonize data privacy laws across EU
- Protect and empower all EU citizens data privacy
- Regularise the approach towards data privacy across region.

3.1 Context of GDPR

The economic and social integration resulting from the functioning of the international market has led to a substantial increase in exchange of personal data from countries of origin. The exchange of personal data between public and private corporations, including individuals, associations and Multinational organizations across the Globe has increased.

Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life and should further facilitate the free flow of personal data within and between third countries and international organisations, while ensuring a high level of the protection of personal data.

These developments required a strong and more coherent data protection framework in the European Union, backed by strong enforcement, given the importance of creating the trust that would allow the digital economy to develop across the international market. These challenges led to the emergence of a strong regulation such as GDPR.

4.0 GDPR principles

Article 5 of GDPR has put forth the following principles relating to processing of personal data to drive the Data Protection regulation

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’)

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’)

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)(Right to erasure)

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and

organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’)

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’)

7. The controller shall be responsible for, and be able to demonstrate compliance with this regulation

5.0 GENERAL

5.1 Definitions

For the purposes of this Regulation, and the context of services provided by RxLogix, the following definitions are considered. Refer - Art. 4

Term / Abbreviation	Definition
Personal data	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
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
restriction of processing	means the marking of stored personal data with the aim of limiting their processing in the future
Profiling	means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements
Data controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

Term / Abbreviation	Definition
Data Processor	processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Consent of the data subject	means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
cross-border processing	1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or 2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

5.2 References

Document ID	Document Title
GDL-001	Glossary
QM-001	Quality Manual
SOP-008	Hosting
SOP-022	Document Management Plan
SOP-029	Business Continuity Plan
SOP-030	Disaster Recovery Plan
SOP-032	Record Retention
SOP-036	Antivirus Management
SOP-037	Access Authorization Authentication
SOP-041	Mobile Device Management
SOP-042	Operating System Hardening for Hosted Servers
SOP-043	Patch Management for Hosted Servers
SOP-044	Vulnerability Management for Hosted Servers
GDL-002	Customer Property
GDL-003	Security Incident Management
GDL-004	Open Source Software Adoption

5.3 External References

Document Title
https://eur-lex.europa.eu/eli/reg/2016/679/oj
CELEX_32016R0679_EN_TXT.pdf
https://gdpr-info.eu/
https://www.oracle.com/in/applications/gdpr/

6.0 Overview of GDPR Chapters (selected) in context of services provided by RxLogix

6.1 Chapter 3 Rights of the data subject

This regulation provides significant authority to the data subjects on their personal data. Article 12-23 provides the rights to data subjects, as below

- Transparent information, communication and modalities for the exercise of the rights of the data subject
- Information to be provided where personal data are collected from the data subject
- Information to be provided where personal data have not been obtained from the data subject
- Right of access by the data subject
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restriction of processing
- Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Right to data portability
- Right to object
- Right to object and automated individual decision-making

6.2 Responsibility of the Data Controller

Considering the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of data subjects, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. The measures shall be reviewed and updated where necessary.

6.2.1 Data protection by design and by default

The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects in proportionate to the amount of personal data collected (data minimization).

The controller shall apply the measures of pseudonymization as part of Article 4 .The application of pseudonymization to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.

6.2.2 Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. Article 33

6.3 Data Processor Responsibilities

The Data Processor, in this case RxLogix corporation will implement all controls to ensure compliance to this regulation.

6.3.1 Data Processing Agreements

RxLogix shall carry out processing activities on behalf of Data Controllers as agreed with them individually in accordance with Contracts and Agreements mutually signed. These agreements will be signed between both parties assuring implementation of sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. These agreements shall detail set out the activities and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The reviews of such contracts shall be in accordance with SOP 15- Contract Review. Article 28

The specific site for hosting the Customer environments and any other customer requirements will be mutually agreed between RxLogix and its customers via the contract.

6.3.2 Subcontracting notification

RxLogix shall not engage another processor without prior specific or general notification of the controller. As part of hosting solutions, RxLogix will partner with approved Hosting solution providers, post a detailed evaluation. In the case of general written authorization, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. Such subcontractors shall go through a detailed assessment as governed by the SOP 26- Vendor Procurement. RxLogix shall be accountable to the quality of the deliverables of its outsourced vendors, in case the vendor fails to fulfil its data protection obligations. Article 28

6.3.3 Data Transfers

RxLogix being a global organization shall process personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Chapter 5

The place of hosting and operational details of staff location shall be written and agreed in the Contract.

RxLogix has a detailed guideline on GDL 002 - Customer Property. The guideline defines an approach to identify, verify, protect, safeguard both data , documents or other proprietary as received from Customers of RxLogix.

6.3.4 Sign Confidentiality Agreements

RxLogix shall ensure all its employees and subcontractors are bound by Non-Disclosure Agreement on principles of Confidentiality, Integrity and Accountability. RxLogix, has identified ‘professional etiquette’ as a no compromise parameter as part of its selection process and continues to encourage this as a discipline throughout the employee lifecycle. RxLogix reserves the right to enforce the principles of NDA in case of any inappropriate actions, in an event if occurred by its employees.

6.3.5 Data Security

RxLogix shall implement appropriate technical and organization controls as laid out in Article 32

- **Encryption of personal data** - This is done in a two pronged approach – Design level at the Product feature level and of that while hosting. All Personal data shall be encrypted at rest and transit using proven algorithms.
- Ensure ongoing **confidentiality, integrity, availability** and resilience of processing systems and services (SOP031- Information Security and Administration)
- Conduct periodic **Disaster recovery tests** and adequate **Back up Management** to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (SOP029- Business Continuity Plan and SOP – 30-Disaster Recovery Plan).RxLogix shall have a periodic process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. (SOP029- Business Continuity Plan and SOP – 30-Disaster Recovery Plan)
- RxLogix has an approved Business Continuity plan to ensure key services are available at an event of Disaster and ensure continued availability of services.
- All security incidents shall be reported to si@rxlogix.com and a systematic evaluation approach is defined to report, manage and handle any such incidents at RxLogix upon the occurrence of the incident, including data breaches.
- As part of key technical measures to enable trace inappropriate access to RxLogix developed applications, cookies are enabled to only capture Session ID to trace the session management details. Other necessary controls to capture User management shall be in built in the application to have a robust Audit trail management. Application time stamp for audit log entries shall synchronize with other applications and systems.
- Secure Design and Coding practices shall be implemented as part of the Software Development Lifecycle practices.

- Data flow diagrams demonstrate the flow of data from the origin and the lifecycle throughout the application.

- RxLogix shall deploy, configure and implement the required monitoring tools and reporting intended to detect real time performance and capacity utilization of applications and servers to allow notification before failure occurs and proactive remediation.

- RxLogix shall deploy a stringent Endpoint security program to manage antivirus and handle malicious code.

- Other security measures such as Password management, User Management, User authentication, Access management, Periodic reviews of Access, Secure session management.

- RxLogix shall ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service.

- RxLogix shall implement a systematic assessment of changes by documenting, assessing the impact, roll out planning and implement changes that are identified.

- Structured Risk management approaches shall be planned RxLogix to ensure risks are being managed, addressed and controlled at acceptable levels.

6.3.6 Data Compliance

RxLogix shall cooperate with its Customers (Data Controllers)

- For the fulfilment of the controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III;

- Assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

- At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

- Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

6.3.7 Communication of a personal data breach to the data subject

In an event of a data breach likely to result in a high risk to the rights and freedoms of natural persons, RxLogix shall inform the impacted customers of RxLogix immediately from the time the organization becomes aware of the situation.

6.3.8 Data protection impact assessment

Where processing activities involve new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller and RxLogix shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

6.3.9 Appointment of Data Privacy Officer

RxLogix shall designate a data protection officer in any case who:

- Will be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

- Will perform the tasks referred to in article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

- Does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

The data protection officer shall have at least the following tasks:

1. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

2. To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

3. To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

4. To cooperate with the supervisory authority;

5. To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

6.3.10 **Transfers of personal data**

Any Data transfers shall be performed by RxLogix with consent from the Controller and tracked via the Customer Property management guideline – GDL002.

REVISION HISTORY

Version 01 Effective on 22-Apr-2019

None

Version 02 Effective on 22-Nov-2019

Updated the document to reflect the implementation attributes

DOCUMENT ELECTRONIC SIGNATURES

DOCUMENT APPROVAL WORKFLOW

Author Approval

Jayashree Acharya Director Jayashree.Acharya@rxlogix.com	I am the author of this document. *Signed 8:23:12 PM UTC 04-Nov-2019*

Required Workflow Steps for this Category

Jayashree Acharya Director Jayashree.Acharya@rxlogix.com	*RxLOGIX / Author* I am the author of this document. *Signed 8:23:51 PM UTC 04-Nov-2019*
Sanjeev Singh Director sanjeev.singh@rxlogix.com	*RxLOGIX / Approver* I have reviewed and approve this document. *Signed 10:28:20 AM UTC 13-Nov-2019*
Amit Kumar Director Amit.kumar@rxlogix.com	*RxLOGIX / Approver* I have reviewed and approve this document. *Signed 8:43:59 AM UTC 22-Nov-2019*