Report By:

Scrut Automation Inc.

(Scrut Automation)

ASSESSMENT REPORT
Based on
General Data Protection Regulation- (EU) 2016/679
For
PharmaEdge Inc.
(PharmaEdge)

Scope of services	PharmaEdge is a Pharma Insights & Analytics provider leveraging AI to increase efficiency, accuracy and save cost.
Date(s) Assessment	August 14, 2025
Audit Criteria	Regulation (EU) 2016/679

August 14, 2025

PharmaEdge Inc.

We have examined the design and controls of PharmaEdge as on August 14, 2025, against the requirements of **General Data Protection Regulation (EU) 2016/679**.

The Company's management is responsible for the adequate design of these controls and compliance with the GDPR requirements. Our responsibility is to express an opinion on the design of these controls and the Company's compliance based on our examination.

Our examination included:

1. Interviewing Top Management, IT Administration Staff, HR Management Staff, General Administration Staff;
2. Reviewing IT Assets;
3. Obtaining an understanding of the design of the Company's controls over GDPR Principles;
4. Technical and Non- technical controls adopted and Reviewing Related policies and procedures;

Because of inherent limitations, controls may not prevent, detect or correct errors or fraud which may occur. Also, projections of any evaluation of adequate design to future periods are subject to the risk that controls may become inadequate because of change in conditions, or that the degree of compliance with the policies and procedures may deteriorate.

In our opinion, as of August 14, 2025 the Company in all material respects has adequately designed controls to meet GDPR requirements

This report is intended solely for the information and use of PharmaEdge and should not be used without prior authorization of PharmaEdge Inc.

1. GDPR Background

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1] Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of data subjects inside the EEA.

The GDPR was adopted on April 14, 2016, and became enforceable beginning May 25, 2018.The regulation applies if the data controller (an organisation that collects data from EU residents), or processor (an organisation that processes data on behalf of a data controller like **cloud service providers**), or the data subject (person) is based in the EU. Under certain circumstances, the regulation also applies to organisations based outside the EU if they collect or process personal data of individuals located inside the EU. The regulation does not apply to the processing of data by a person for a "purely personal or household activity and thus with no connection to a professional or commercial activity.

2. GDPR Definitions

S.No	Definitions
1	**'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;
2	'**processing'** means 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3	'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
4	**'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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
5	'**pseudonymisation'** 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;
6	**'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;
7	**'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
8	**'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients;
9	'**third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
10	'**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;
11	**'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
12	**'genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
13	**'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
14	**'data concerning health'** 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;

3. Introduction-

PharmaEdge Inc. (PharmaEdge)

PharmaEdge pioneers Life Sciences competitive intelligence by blending AI, machine learning, and deep therapy area expertise to disrupt traditional CI practices.

4. GDPR COMPLIANCE REPORT

S.No.	Domain	Control Title	Control Description	EU GDPR	Compliance Status	Testing Performed by Scrut
1.	Notice and Consent	Privacy Notice	PharmaEdge defines and documents a process to inform users with a Privacy Notice for collecting and processing their personal data.	Art. 12, 13	Compliant	Reviewed the existence and content of PharmaEdge's privacy policy at https://pharmaedge.ai/privacy-policy/ and determined that process to inform users with Privacy notice is maintained.
2.	Notice and Consent	Updated Privacy Notice	PharmaEdge timely notifies users about any changes to personal data processing.	Art. 13, 14	Compliant	Reviewed PharmaEdge's procedures for communicating updates to the privacy policy to relevant stakeholders, including employees.
3.	Notice and Consent	Cookie Policy	PharmaEdge displays a cookie consent banner for users to accept or decline the cookie policy.	Art. 7, 12	Compliant	Inspected PharmaEdge's cookie consent banner and verified that it aligns with GDPR requirements.
4.	Notice and Consent	Cookie - Banner	PharmaEdge obtains consent from data subjects for processing activities where consent is the legal basis.	Art. 7	Compliant	Conducted a walkthrough of PharmaEdge's application to verify that consent is obtained for relevant processing activities.
5.	Notice and Consent	Consent - Obtain	PharmaEdge maintains records of consent given by data subjects.	Art. 7	Compliant	Verified that PharmaEdge maintains records of consent, including the process for recording and managing consent logs.
6.	Notice and Consent	Consent - Record	PharmaEdge allows data subjects to withdraw their consent.	Art. 7	Compliant	Examined PharmaEdge's process for facilitating consent withdrawal by data subjects, including the mechanism for withdrawal and any limitations.
7.	Notice and Consent	Consent - Obtain and Withdrawal	PharmaEdge collects user data after receiving their consent.	Art. 8	Compliant	Confirmed that PharmaEdge processes data only on the instructions of the Data Controller.
8.	Notice and Consent	Parental Consent	PharmaEdge collects data after obtain verifiable parental consent for the processing of personal data of children below the legal age.	Art. 8	Not Applicable	Enquired with the DPO that PharmaEdge does not collect personal data of the children below the legal age.

S.No.	Domain	Control Title	Control Description	EU GDPR	Compliance Status	Testing Performed by Scrut
9.	Data Management	Personal Data Inventory	PharmaEdge has developed and maintains Personal Data Inventories for all processing activities carried out using the Product.	Art. 30	Compliant	We obtained and inspected the 'Data Asset inventory' maintained in the ROPA by PharmaEdge and noted that the policy document captured guidance on creating and maintaining a data inventory at PharmaEdge. Further, we obtained and inspected the Data Inventory document that is maintained and reviewed by the management. Upon inspection, we noted that the inventory captured the type of personal data, source of personal data, category of data and it's respective retention schedule at an organizational level.
10.	Data Management	Purpose Limitation	Personal data attributes processed by the Product are minimized to what is required for fulfilling the stated purpose.	Art. 5	Compliant	It was observed that PharmaEdge acts as a data processor for it's clients. The accountability of defining the purpose for the processing of the personal data and also the attributes to be included in product lies with the Client or Data Controller.
11.	Data Management	Data Minimization	PharmaEdge has implemented a process for granting and removing users' access to personal data.	Art. 5, 17, 18, 21	Compliant	As per the discussion with DPO and post walkthrough of the product, we observed that the product has the functionality to collect the personal data as per the requirement/fields defined by the client or data controller within the Customer Onboarding Form during the initial set up. Further, we observed and noted that the fields capturing the PII of the data subject within the Product can be customized by the client or data controller through the Admin Portal.
12.	Data Management	Retention Timelines	PharmaEdge identifies and defines timelines for retaining personal data processed by the Product as per the applicable legal and contractual requirements.	Art. 5	Compliant	As per the inspection of the Privacy Policy, it was observed that PharmaEdge has a defined retention policy and is governed contractually with the client and applicable laws. Personal Data from application is deleted as per the defined timelines and when the client requests deletion, otherwise the data is retained throughout the duration of the contracted service.
13.	Data Management	Insights-Data Aggregation	PharmaEdge ensures any insights generated from the personal data stored in the Product using third-party analytics engines are at an aggregated level.	Art. 32	Compliant	We found that PharmaEdge does not generate any insights from PII of the data subject(s) aligned processing activities. The insights generated are only with regards to the application performance and availability.
14.	Data Management	Anonymization	PharmaEdge anonymizes and de-identifies personal data attributes wherever possible.	Art. 15	Compliant	During the walkthrough it was observed that PharmaEdge anonymizes and de-identifies personal data.

S.No.	Domain	Control Title	Control Description	EU GDPR	Compliance Status	Testing Performed by Scrut
15.	Data Subject Rights	Access	PharmaEdge has mechanism in place to let the data subjects access their data.	Art. 15	Compliant	Right to access information about personal data found evident. Data subjects can write to siddharth.subramaniam@pharmaedge.ai .
16.	Data Management	Accuracy/ Update	PharmaEdge allow data subjects to update their data and keep it accurate.	Art. 5, 16, 19	Compliant	Right to update information about personal data found evident. Data subjects can write to siddharth.subramaniam@pharmaedge.ai to update their personal data to keep it accurate.
17.	Data Subject Rights	Deletion, Restriction of Processing, Notification Obligation, Data Portability, Objection to Processing, Automated Decision-Making, Nomination	PharmaEdge allow data subjects to delete their data, update their personal data to keep it accurate, update their restrict the processing of their data, to notify obligation regarding rectification or erasure of personal data or restriction of processing of personal data, right to data portability, right not to be subject to a decision based solely on automated processing.	Art. 17	Compliant	PharmaEdge has https://pharmaedge.ai/privacy-policy/ published on the website which has the below rights mentioned for the data subjects and data subjects can avail their rights by writing to siddharth.subramaniam@pharmaedge.ai - Right to be informed Right of access Right to rectification Right to be forgotten Right to restrict processing Right to data portability Right to object to processing Rights in relation to automated decision-making and profiling
18.	Accountability	Responsibility and Accountability	PharmaEdge documents the responsibilities of the privacy and security roles.	Art. 24	Compliant	Reviewed the document for Roles and Responsibilities for privacy and security roles and determined that privacy and security roles are established.
19.	Accountability	Data Protection Policy	PharmaEdge maintains a data protection policy that outlines its approach to protecting personal data and ensuring compliance with data protection laws.	Art. 24	Compliant	Examined PharmaEdge's data protection policy, including the scope of the policy, the responsibilities of personnel, and the procedures for data handling and processing.
20.	Accountability	Training and Awareness	PharmaEdge provides periodic training and awareness programs for employees on data protection and privacy requirements.	Art. 24	Compliant	Verified that PharmaEdge conducts regular training and awareness programs for employees on data protection and privacy requirements.
21.	Accountability	Monitoring and Review	PharmaEdge conducts regular monitoring and reviews of its data protection measures and policies to ensure ongoing compliance and effectiveness.	Art. 24	Compliant	Reviewed PharmaEdge's monitoring and review process for data protection measures, including the frequency of reviews, the assessment of effectiveness, and the implementation of any necessary changes.
22.	Security	Data Protection by Design	PharmaEdge implements data protection principles in the design and operation of its systems and processes.	Art. 25	Compliant	Assessed PharmaEdge's approach to data protection by design, including the integration of privacy considerations into the development and implementation of its systems and processes.

S.No.	Domain	Control Title	Control Description	EU GDPR	Compliance Status	Testing Performed by Scrut
23.	Security	Data Protection by Default	PharmaEdge ensures that, by default, only personal data necessary for each specific purpose of the processing is processed.	Art. 25	Compliant	Verified that PharmaEdge has implemented data protection by default, ensuring that only necessary personal data is processed for each specific purpose.
24.	Security	Representative	PharmaEdge appoints a representative in the EU for compliance with GDPR requirements when not established in the EU.	Art. 27	Not Applicable	PharmaEdge does not have clients in EU currently. Hence, they have not appointed an EU Representative to address all issues related to processing, for the purposes of ensuring compliance with this Regulation
25.	Security	Processor Contracts	PharmaEdge ensures that contracts with data processors include clauses requiring the processor to comply with data protection regulations.	Art. 28	Compliant	Examined PharmaEdge's contracts with data processors to verify the inclusion of clauses requiring compliance with data protection regulations.
26.	Disclosure	Data Processing Agreement	PharmaEdge executes Data Processing Agreements with all third parties that may have access to personal data processed by the application.	Art. 28	Compliant	Verified that PharmaEdge has executed Data Processing Agreements with all third parties that may have access to personal data processed by the application.
27.	Disclosure	Third Party Integration	PharmaEdge integrates with third-party service providers, such as analytics engines, in a manner that exposes only minimal requisite personal data attributes to these third parties.	Art. 28	Compliant	Assessed PharmaEdge's integration with third-party service providers, ensuring that only minimal necessary personal data is exposed to these third parties.
28.	DPO	Appointment of DPO	PharmaEdge appoints a Data Protection Officer (DPO) to oversee GDPR compliance.	Art. 29, Art. 37	Compliant	Confirmed that PharmaEdge has appointed a Data Protection Officer (DPO) to oversee GDPR compliance.
29.	DPO	Position and Role of DPO	PharmaEdge ensures that the DPO's position and role are properly defined and communicated.	Art. 29	Compliant	Verified that PharmaEdge has defined and communicated the DPO's position and role within the organization.
30.	DPO	Independence of DPO	PharmaEdge ensures that the DPO operates independently and reports directly to the highest management level.	Art. 29, Art. 38	Compliant	Confirmed that PharmaEdge's DPO operates independently and reports directly to the highest management level.
31.	DPO	Resources and Support for DPO	PharmaEdge provides adequate resources, training, and support for the DPO to carry out their tasks effectively.	Art. 29	Compliant	Verified that PharmaEdge provides adequate resources, training, and support for the DPO to carry out their tasks effectively.
32.	DPO	Expertise of DPO	PharmaEdge ensures that the DPO has the necessary expertise/professional competence in data protection law and practices.	Art. 29	Compliant	Confirmed that PharmaEdge's DPO has the necessary expertise and professional competence in data protection law and practices.
33.	Accountability	Records of Processing Activities	PharmaEdge maintains records of processing activities (ROPA), including the purposes of processing, categories of data subjects and personal data, and recipients of personal data.	Art. 30	Compliant	Verified that PharmaEdge maintains records of processing activities (ROPA), including the purposes of processing, categories of data subjects and personal data, and recipients of personal data.
34.	Security	Cooperation with Authorities	PharmaEdge cooperates with data protection authorities in the performance of their tasks, providing necessary information and access to data processing activities.	Art. 31	Compliant	Confirmed that PharmaEdge cooperates with data protection authorities and provides necessary information and access to data processing activities.

S.No.	Domain	Control Title	Control Description	EU GDPR	Compliance Status	Testing Performed by Scrut
35.	Security	Access Restriction	PharmaEdge restricts access to personal data processed by the Product only to authorized personnel.	Art. 32	Compliant	Verified that PharmaEdge restricts access to personal data processed by the Product only to authorized personnel.
36.	Security	Product - Version	PharmaEdge releases security updates of the Product in a timely manner, upon identification of vulnerabilities, bugs, or security enhancements.	Art. 32	Compliant	Confirmed that PharmaEdge releases security updates of the Product in a timely manner, upon identification of vulnerabilities, bugs, or security enhancements.
37.	Security	Backup	PharmaEdge backs up critical data residing in the Product (and its DBs) on a periodic basis.	Art. 32	Compliant	Verified that PharmaEdge backs up critical data residing in the Product (and its DBs) on a periodic basis.
38.	Security	Audit Logging	PharmaEdge enables audit logging on all systems and ensures the same can be extracted for all Products.	Art. 32	Compliant	Confirmed that PharmaEdge enables audit logging on all systems and ensures the same can be extracted for all Products.
39.	Security	Web Application Firewall	PharmaEdge has implemented a Web Application firewall to Protect the product from malicious attacks.	Art. 32	Compliant	Verified that PharmaEdge has implemented a Web Application firewall to Protect the product from malicious attacks.
40.	Security	Encryption at Rest	PharmaEdge protects personal data stored in the Product and its DBs with a secure level of encryption.	Art. 32	Compliant	Confirmed that PharmaEdge protects personal data stored in the Product and its DBs with a secure level of encryption.
41.	Security	Encryption in Transit	PharmaEdge protects all client-server communications with an appropriate level of encryption.	Art. 32	Compliant	Confirmed that PharmaEdge protects all client-server communications with an appropriate level of encryption, such as TLS or SSL.
42.	Security	Vulnerability Assessment	PharmaEdge subjects the Product to periodic Vulnerability Assessments. All critical vulnerabilities are patched without undue delay.	Art. 32	Compliant	Verified that PharmaEdge conducts periodic Vulnerability Assessment and Penetration Testing (VAPT) and addresses any critical vulnerabilities promptly.
43.	Security	Backend Integration	PharmaEdge protects the Product's integration with backend systems using secure APIs/Web services.	Art. 32	Compliant	Confirmed that PharmaEdge protects the Product's integration with backend systems using secure APIs/Web services and appropriate security measures.
44.	Security	Breach Notification to Customer	PharmaEdge notifies the relevant customer of a personal data breach within 48 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s).	Art. 33	Compliant	Verified that PharmaEdge has procedures in place to notify customers of personal data breaches within 48 hours of becoming aware of the breach.
45.	Security	Breach Notification to Data Subjects	PharmaEdge communicates a personal data breach to the affected data subjects without undue delay when the breach is likely to result in a high risk to their rights and freedoms.	Art. 34	Compliant	Confirmed that PharmaEdge has procedures in place to communicate personal data breaches to affected data subjects without undue delay when the breach is likely to result in a high risk to their rights and freedoms.
46.	Privacy in SDLC	Change Management	PharmaEdge ensures any proposed changes that may change how the Product processes personal data are subject to approvals from the Management prior to starting development-related activities.	Art. 35	Compliant	Verified that PharmaEdge has a change management process in place to assess and approve any proposed changes that may affect how the Product processes personal data.

S.No.	Domain	Control Title	Control Description	EU GDPR	Compliance Status	Testing Performed by Scrut
47	Privacy in SDLC	Risk Mitigation	PharmaEdge addresses and mitigates risks identified as part of the Privacy Assessments in a timely manner.	Art. 35	Compliant	Confirmed that PharmaEdge addresses and mitigates risks identified as part of the Privacy Assessments in a timely manner.
48	Privacy in SDLC	Segregation of environment	PharmaEdge ensures segregation of environments between the Product's development, test, and production environments. Access to the production environment is restricted to authorized personnel.	Art. 35	Compliant	Verified that PharmaEdge maintains segregation of environments between the Product's development, test, and production environments and that access to the production environment is restricted to authorized personnel.
49	Privacy in SDLC	Testing	PharmaEdge ensures testing is performed only in the Product's test environment and no production data is used for testing purposes.	Art. 35	Compliant	Confirmed that PharmaEdge performs testing only in the Product's test environment and no production data is used for testing purposes.
50	Accountability	Data Protection Impact Assessment	PharmaEdge subjects the Product to periodic DPIAs. All medium and high risks identified during the assessment are treated in a timely manner.	Art. 35	Compliant	Verified that PharmaEdge conducts periodic Data Protection Impact Assessments (DPIAs) and addresses any identified medium and high risks promptly.
51	Accountability	Prior Consultation	PharmaEdge consults the supervisory authority prior to processing PII, when a DPIA indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk, as per the Data Processing Guidelines.	Art. 36	Compliant	Confirmed that PharmaEdge consults the supervisory authority prior to processing PII when a DPIA indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk.
52	Accountability	DPO Accessibility	PharmaEdge makes the DPO easily accessible to data subjects and supervisory authorities.	Art. 37	Compliant	Verified that PharmaEdge makes the DPO easily accessible to data subjects and supervisory authorities.
53	International Transfers	Data Transfers Outside EU	PharmaEdge ensures that personal data transferred outside the EU is protected by appropriate safeguards, such as standard contractual clauses or binding corporate rules.	Art. 44, Art. 46	Compliant	Verified the DPA and determined that PharmaEdge ensures that personal data transferred outside the EU is protected by appropriate safeguards, such as standard contractual clauses or binding corporate rules.
54	International Transfers	Adequacy Decisions	PharmaEdge transfers personal data to jurisdictions outside the applicable jurisdiction only when the level of protection is adequate as per the governing law/regulation.	Art. 45	Compliant	Verified that PharmaEdge transfers personal data to jurisdictions outside the applicable jurisdiction only when the level of protection is adequate as per the governing law/regulation.
55	International Transfers	Codes of Conduct and Certifications	PharmaEdge adheres to approved codes of conduct and certifications as a mechanism to demonstrate compliance with GDPR when transferring data internationally.	Art. 40, Art. 42	Compliant	Verified that PharmaEdge adheres to approved codes of conduct and certifications as a mechanism to demonstrate compliance with GDPR when transferring data internationally.

AUDIT REPORT SUMMARY
PharmaEdge working as a Processor is found to have effectively implemented the requirements of GDPR. Required security policies and practices found to be documented and implemented. **PII being processed is non sensitive in nature and presently the required GDPR practices as controller are available and are well adopted by PharmaEdge**.