DATA PROCESSING AND COMPLIANCE WITH EUROPEAN DATA PROTECTION LAWS

---

1. Data Processing and Compliance with European Data Protection Laws.

Each party represents and warrants that it understands its obligations under European Data Protection Laws and will comply with them. Exigyn and Client acknowledge and agree that for the purposes of the European Data Protection Laws, Client is the “controller” and Exigyn is the “processor” as defined in the GDPR with respect to any Personal Data that is processed by Exigyn in the provision of SaaS Services.

Client warrants that it shall:

(a) **(a)** Only disclose the Personal Data necessary for Exigyn to perform the SaaS Services;

(b) **(b)** Implement processes and procedures designed to prevent the upload of any Personal Data of patients or consumers to the Software;

(c) **(c)** Comply with all European Data Protection Laws and regulations, including the GDPR, in relation to the Processing of any Personal Data;

(d) **(d)** If applicable, ensure that appropriate consents and notices are in place to enable lawful transfer of Personal Data to Exigyn; and

(e) **(e)** Not transfer or provide access to Personal Data from inside the European Economic Area or the United Kingdom to Exigyn outside the European Economic Area or the United Kingdom unless appropriate safeguards have been put in place in compliance with European Data Protection Laws.

Exigyn warrants that it shall, in the performance of the SaaS Services:

(f) **(a)** Process data only on documented instructions from Client unless required to Process such Personal Data by applicable law to which Exigyn is subject; in such a case, Exigyn shall inform the Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

(g) **(b)** Not process or otherwise have access to Personal Data in the course of providing the services, unless explicitly instructed in writing by Client;

(h) **(c)** Ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(i) **(d)** Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk;

(j) **(e)** Taking into account the nature of the Processing, assist the Client by appropriate technical and organizational measures, insofar as this is possible, in fulfilling its obligations to respond to requests for exercising the data subject's rights under the European Data Protection Laws;

(k) **(f)** Without undue delay notify the Client about any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data belonging to the Client;

(l) **(g)** Delete or return all Personal Data to Client after the end of the provision of services, and delete existing copies unless the law requires storage of the Personal Data;

(m) **(h)** Make available to Client all information necessary to demonstrate compliance with the obligations laid down in this section; and

(n) **(i)** Permit the Client (or another auditor mandated by the Client and subject to appropriate confidentiality restrictions) at any time upon thirty (30) days' written notice to have access to the appropriate part of Exigyn's premises, systems, equipment, and other materials and data Processing facilities to enable the Client to inspect or audit the same for the purposes of monitoring compliance with Exigyn's obligations under this section. Any such inspection shall be carried out during normal business hours and shall be limited to one (1) inspection per calendar year.

Notwithstanding anything in the Agreement or other document, the parties acknowledge and agree that Exigyn's provision of access to Personal Data is not part of and explicitly excluded from the exchange of consideration, or any other thing of value, between the parties.

For the purposes of this section:

"European Data Protection Laws" means (a) the General Data Protection Regulation 2016/679 (the "GDPR"); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018 ("DPA"), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (together with the DPA, the "UK GDPR"), and the Privacy and Electronic Communications Regulations 2003; and (d) any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data, in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

“Data Subject”, “Personal Data”, “Process”, “Processed” or “Processing” shall have the meaning given in the relevant European Data Protection Laws.