Last Updated: April 17, 2024
Data Processing Addendum

This Data Processing Addendum ("DPA") forms an integral part of the Terms of Service provided by LexRing at www.lexring.com or any other agreement that regulates the use of LexRing's services ("Agreement"), agreed upon by you, the Customer (as identified in the Agreement) (referred to as "you," "your," or "Customer"), and LexRing spółka z ograniczoną odpowiedzialnością with its registered office in Warsaw, located at 18 Twarda Street, Spektrum Tower 19 floor, 00-105 Warsaw, Poland, ("LexRing," "us," "our"). This DPA outlines the mutual understanding concerning LexRing's handling of Personal Data exclusively on behalf of the Customer. The term "Parties" refers to both parties collectively, and "Party" refers to each individually.

Terms not defined in this document will carry the meanings attributed to them in the Agreement.

By utilizing the Services, the Customer consents to this DPA, affirming that you possess the necessary authority to commit the Customer to this DPA. Should you not agree to this DPA, lack the authority to bind the Customer or any other entity, please refrain from submitting Personal Data to us.

Should discrepancies arise between specific terms of this DPA and the Agreement's terms, the stipulations of this DPA will take precedence over the conflicting terms of the Agreement, strictly in relation to the handling of Personal Data.

1. DEFINITIONS
(a) An "Affiliate" is an entity that exercises control over, is controlled by, or is under shared control with the referenced entity. "Control" in this context means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity, whether through the ownership of voting securities, by contract, or otherwise, which includes owning more than 50% of the voting interests of the entity.
(b) "Authorized Affiliate" denotes any Affiliate of the Customer authorized under the Agreement to utilize the Services but which has not executed its own agreement with LexRing and is not considered a "Customer" as per the Agreement's definition.
(c) "CCPA" stands for the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., along with its implementing regulations, subject to amendments over time.
(d) Terms such as "Controller," "Member State," "Processor," "Processing," and "Supervisory Authority" retain their definitions as in the GDPR. Similarly, "Business," "Business Purpose," "Consumer," and "Service Provider" are as defined in the CCPA. For clarity, within this DPA, "Controller" also encompasses "Business," and "Processor" also means "Service Provider," where applicable under the CCPA. Likewise, the term for Processor's Sub-processor is extended to include the notion of Service Provider.
(e) "Data Protection Laws" encompasses all relevant and enforceable privacy and data protection statutes and regulations, including those from the European Union, the European Economic Area, Member States, Switzerland, the United Kingdom, Canada, Israel, and the United States, such as the GDPR, UK GDPR, and CCPA, as they apply to the Processing of Personal Data under this DPA and Agreement.
(f) "Data Subject" refers to the identifiable individual to whom the Personal Data pertains.
(g) "GDPR" signifies the Regulation (EU) 2016/679 of the European Parliament and of the Council from 27 April 2016 concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data.
(h) "Personal Data" or "Personal Information" includes any data that identifies, relates to, describes, can be associated with, or could reasonably be linked, directly or indirectly, with a specific natural person or Consumer, processed by LexRing solely on behalf of the Customer under this DPA and the Agreement.
(i) "Services" entails the LexRing cloud-based services including platforms, products, services, applications, APIs, tools, and any related or supplementary LexRing offerings (including Upgrades as defined in the Agreement), provided online and through mobile applications ("Platform"), and any other services rendered to the Customer by LexRing under the Agreement.
(j) "Security Documentation" refers to the periodically updated security documentation that delineates the technical and organizational measures implemented by LexRing relevant to the Processing of Personal Data under the Agreement and this DPA, accessible at www.lexring.com, or otherwise made reasonably available to the Customer by LexRing.

(k) "Sensitive Data" means Personal Data that falls under specific legal protection requiring distinct handling, such as "special categories of data," "sensitive data," or other terms of similar significance under applicable Data Protection Laws, which may encompass: (a) social security number, tax identification number, passport number, driver's license number, or similar identifiers (or parts thereof); (b) financial or credit information, including credit or debit card numbers; (c) details revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a person, health-related data, sexual orientation or sex life, or data regarding criminal convictions and offenses; (d) Personal Data about children; and/or (e) unhashed account passwords.
(l) "Standard Contractual Clauses" include (a) for transfers of Personal Data under the GDPR, the controller-to-processor Standard Contractual Clauses and processor-to-processor Standard Contractual Clauses as sanctioned by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, including all relevant Annexes, ("EU SCCs"); (b) for transfers under the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses of 21 March 2022 (version B.1.0) ("IDTA"), incorporated into the EU SCCs via Annex III ("UK Addendum"); and (c) for transfers subject to the Federal Act on Data Protection (revised as of 25 September 2020), the terms in Annex IV of the EU SCCs ("Switzerland Addendum").
(m) "Sub-processor" is any third party appointed to conduct specific Personal Data Processing activities following LexRing's instructions.
(n) "UK GDPR" represents the Data Protection Act 2018, in addition to the GDPR as it is part of the law of England, Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, amended by the Data Protection, Privacy, and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

2. RULES OF PROCESSING
2.1. Party Roles. The Parties acknowledge their roles in relation to the handling of Personal Data solely by LexRing on behalf of the Customer: (a) the Customer is the Data Controller, and (b) LexRing acts as the Data Processor. Within this context, "Data Controller" and "Data Processor" refer to the Customer and LexRing, respectively.

2.2. Customer Responsibilities. In utilizing the Services and directing the Data Processor, the Customer must adhere to Data Protection Laws, the Agreement, and this DPA. The Customer is responsible for ensuring it has all necessary legal grounds to gather, Process, and transfer the Personal Data to the Processor and to sanction the Processor's data handling activities on the Customer's behalf in line with the Agreement and this DPA, including achieving a Business Purpose.

2.3. Data Processor's Data Handling. The Data Processor is tasked with Processing Personal Data for specific purposes: (a) as outlined in the Agreement and this DPA; (b) as part of its Service provision; (c) in compliance with the Customer's legitimate and documented directives, provided these directives align with the Agreement and this DPA, and pertain to the Processing's execution manner; (d) to exchange Personal Data with, or receive Personal Data from, third parties as instructed by the Customer or as part of the Customer's Service usage (for example, through integrations between Services and third-party services configured by the Customer or on their behalf); (e) to anonymize Personal Data to become Anonymous Information (as defined in the Agreement); and (f) as necessitated by applicable laws to the Processor, or as mandated by a legally competent court or authority, ensuring the Processor informs the Customer of such legal obligations prior to Processing, unless prohibited by such laws or orders from making this disclosure.

The Processor will promptly inform the Customer if, in the Processor's reasonable judgement, a Customer instruction regarding Personal Data Processing breaches applicable Data Protection Laws, except where prohibited from notifying the Customer under such laws. It is explicitly stated that the Processor is not obliged to verify the legality of Customer instructions against Data Protection Laws.

2.4. Processing Details. The Processing's subject matter, as undertaken by the Processor, is to perform Services as per the Agreement and this DPA. Schedule 1 (Processing Details) of this DPA elaborates on the specifics, including Processing's duration, nature, purpose, Personal Data types, and Data Subject categories.

2.5. CCPA Compliance; Restrictions on Personal Information. The Processor acknowledges it does not process any Personal Information in exchange for any services or goods provided to the Customer

under the Agreement or this DPA. The Processor certifies its comprehension of CCPA guidelines, requirements, and definitions and commits to not selling or sharing (as defined within the CCPA) any Personal Information processed herein, without the Customer's prior written consent or directive, nor will it undertake actions that would classify any Personal Information transfer to or from the Processor under the Agreement or this DPA as "selling" or "sharing" under the CCPA. The Processor understands that the Customer shares Personal Information with the Processor solely for specified, limited purposes outlined in this DPA and the Agreement. The Processor is to process all Personal Information (a) for such specified, limited purpose(s) and (b) in compliance with relevant CCPA sections. The Processor shall not (i) retain, utilize, or disclose Personal Information beyond the direct business relationship scope between the Parties, as described in the Agreement, or for any purpose other than performing the Services or as otherwise allowed by the CCPA, the Agreement, and/or this DPA; nor (ii) merge Personal Information processed on behalf of other entities with the Customer's Personal Information, unless expressly permitted under the CCPA, its implementing regulations, the Agreement, and/or this DPA. Additionally, the Processor acknowledges the Customer's right to implement reasonable and appropriate measures to halt and remedy any unauthorized Personal Information use by the Processor. The Processor will alert the Customer if it determines it can no longer meet its CCPA obligations.

3. HANDLING DATA SUBJECT REQUESTS

Should the Data Processor receive a request from a Data Subject or Consumer seeking to exercise their rights under applicable Data Protection Laws, such as access, correction, Processing limitation, deletion, data portability, objection to Processing, avoidance of automated decision-making, opting out from the sale of Personal Information, or protection against discrimination ("Data Subject Request"), the Processor will either notify the Customer or direct the Data Subject or Consumer to the Customer. Considering the nature of the Processing, the Processor will, to a feasible and reasonable extent, support the Customer in fulfilling Data Subject Requests. The Processor may guide Data Subjects or Consumers to contact the Customer's Administrator for handling their request or to use available self-service options within the Platform.

4. CONFIDENTIALITY

The Data Processor will ensure that all personnel and contractors involved in the Processing of Personal Data are bound by confidentiality commitments or are under a legal obligation to maintain confidentiality.

5. USE OF SUB-PROCESSORS

5.1. Engaging Sub-processors

The Customer acknowledges and consents that (a) the Processor's Affiliates may serve as Sub-processors; and (b) both the Processor and its Affiliates are permitted to hire third-party Sub-processors to assist in delivering the Services.

5.2. Current Sub-processors and Updates

5.2.1. From the agreement's commencement, the Customer grants the Processor general authorization to engage Sub-processors. List of the sub-processors is provided upon request of the Customer.

5.3. Objections to New Sub-processors

Following a Sub-processor Notification, the Customer may object to the introduction of a new Sub-processor or replacement based on Personal Data protection concerns. Such objections must be communicated to the Processor promptly in writing at privacy@lexring.com, explaining the objection reasons. If the Customer does not object within this timeframe as described, the new Sub-processor's engagement is deemed approved by the Customer. If the Customer objects to a new Sub-processor reasonably, the Processor will strive to offer an alternative to the Service or suggest a viable adjustment to the Customer's Service setup to prevent Personal Data Processing by the disputed Sub-processor without significantly inconveniencing the Customer. If the Processor cannot offer such alternatives within thirty (30) days of receiving the objection, the Customer may terminate the Agreement and this DPA concerning the affected Services or Service components that require the contested Sub-processor, by notifying the Processor in writing. All due payments under the Agreement before the termination concerning the Processing in question shall be made to the Processor. Pending a resolution on the new Sub-processor, the Processor may temporarily halt Processing of the implicated Personal Data or suspend access to the relevant Services. The Customer shall have no additional claims against the Processor following the Agreement's or DPA's termination under these circumstances, including but not limited to refund requests.

5.4. Sub-processor Agreements
The Processor, or an Affiliate of the Processor, has executed a written contract with each existing Sub-processor and will do so with any new Sub-processor, incorporating data protection commitments that are the same or substantially similar to those set out in this DPA, especially regarding implementing suitable technical and organizational measures to ensure that Processing meets GDPR standards. Should a Sub-processor fail to meet its data protection duties regarding Personal Data Processing, the Processor remains accountable to the Customer for fulfilling the Sub-processor's obligations.

6. SECURITY MEASURES & AUDIT RIGHTS
6.1. Security Measures for Personal Data Protection. The Data Processor commits to maintaining suitable technical and organizational measures to safeguard Personal Data processed under this agreement (including protections against unauthorized or illegal Processing, and against accidental or illegal destruction, loss, alteration, damage, unauthorized disclosure of, or access to, Personal Data, ensuring Personal Data's confidentiality and integrity). Upon the Customer's reasonable request, and considering the nature of Processing and information accessible to the Data Processor, the Data Processor will assist the Customer, at the Customer's expense and following Section 11.1, in complying with GDPR Articles 32 to 36 obligations.

6.2. Audits and Inspections. Given a 14-day advance written request from the Customer, at reasonable intervals (not exceeding once per year) and under strict confidentiality agreements, the Data Processor will provide the Customer (who is not a competitor) or a third-party auditor (independent, reputable, and not a competitor or in conflict with the Data Processor, under confidentiality and non-compete agreements) necessary information to prove compliance with this DPA, and permit and support audits, including inspections, by them. The Data Processor can fulfill this obligation by responding to questionnaire-based audits or providing attestations, certifications, and summaries of audit reports from accredited third-party auditors that relate solely to the Data Processor's compliance with this DPA. Any information or documents related to audits or inspections, including outcomes, must be used by the Customer solely to assess the Data Processor's compliance with this DPA and not disclosed to any third parties without the Data Processor's written consent. The Customer must return any documents or records provided or created during an audit or inspection to the Data Processor upon request.

6.3. Audit Conduct. During any audit or inspection, the Customer (and its auditors) must avoid (or minimize) any damage, harm, or disruption to the Data Processor's operations, premises, equipment, personnel, and business.

6.4. Audit Rights. The audit rights specified in 6.2 are applicable only if the Agreement does not already grant the Customer audit rights that fulfill the Data Protection Laws' requirements (including, where applicable, GDPR or UK GDPR article 28(3)(h)). If the Standard Contractual Clauses apply, nothing in Section 6 modifies or affects the Standard Contractual Clauses or any rights of Supervisory Authorities or Data Subjects under those clauses.

7. MANAGEMENT AND NOTIFICATION OF DATA INCIDENTS
7.1. The Data Processor has internal security incident management policies and will notify the Customer promptly upon becoming aware of any accidental or illegal destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data processed on the Customer's behalf ("Data Incident"). The Data Processor will reasonably attempt to mitigate and remediate the cause of such Data Incidents, as long as these actions are within the Data Processor's control. This obligation does not extend to incidents caused by the Customer, its users, or Service users.

7.2. The Customer agrees not to publicly disclose, admit liability, or release any information regarding a Data Incident that identifies the Data Processor without the Data Processor's written consent unless legally required. If disclosure is legally mandated, the Customer will notify the Data Processor beforehand, allowing an opportunity to contest the disclosure, and will limit the disclosure to what is legally required.

8. RETURN AND DELETION OF PERSONAL DATA
After the Agreement ends and Services cease, the Data Processor will, based on the Customer's instructions via the Platform or written notice, either delete or return all Personal Data processed on the Customer's behalf, except where the Data Processor is legally allowed or required to retain some data.

9. INTERNATIONAL DATA TRANSFERS
9.1. Transfers from the EEA, Switzerland, and the United Kingdom to Adequate Protection Countries. Personal Data can be transferred from the European Union (EU) Member States, Norway, Iceland, Liechtenstein (collectively, "EEA"), Switzerland, and the United Kingdom (UK) to countries recognized for having adequate data protection levels by EEA, Switzerland, or UK authorities, under adequacy decisions or equivalent mechanisms ("Adequacy Decisions"). This includes adherence to the European Commission's decision as of 10 July 2023, endorsing the EU-US Data Privacy Framework.
9.2. Direct Transfers from the EEA, Switzerland, and the UK to Non-Adequate Countries. For Personal Data transferred directly from the EEA, Switzerland, or the UK to countries lacking an Adequacy Decision:
(i) For transfers from the EEA to non-adequate countries ("EEA Transfers"), the EU Standard Contractual Clauses (SCCs) will apply;
(ii) For transfers from the UK to non-adequate countries ("UK Transfers"), the UK Addendum will govern;
(iii) For transfers from Switzerland to non-adequate countries ("Switzerland Transfers"), the Swiss Addendum will control;
(iv) Annex V of the EU SCCs, offering Additional Safeguards, will apply to any EEA, UK, and Switzerland Transfers covered by the Standard Contractual Clauses.

9.3. Further Transfers from the EEA, Switzerland, and the UK to Non-Adequate Countries. For onward transfers of Personal Data from the EEA, UK, and Switzerland to authorized Sub-processors or Processor Affiliates in countries without an Adequacy Decision, the Standard Contractual Clauses (Module 3) as specified in the EU 2021/914 Implementing Decision and adjusted following Swiss Federal Data Protection and Information Commissioner's guidance, the IDTA, and/or SCCs will apply.

9.4. Transfers from Other Jurisdictions: Should the Processor process Personal Data involving transfers mandated by the Customer from jurisdictions requiring specific lawful transfer mechanisms, the Customer must inform the Processor of these obligations, and both Parties will consider necessary DPA modifications per Section 11.2's stipulations.

10. AUTHORIZED AFFILIATES
10.1. Agreement Coverage. By entering this DPA, the Customer also does so on behalf of, and as representative for, its Authorized Affiliates, making them bound by the Customer's obligations herein if the Processor processes their Personal Data, hence they act as "Controllers" for their processed Personal Data. Authorized Affiliates' access and usage of the Services must adhere to the Agreement and this DPA's terms, with any breaches by an Authorized Affiliate considered breaches by the Customer.

10.2. Communication Role. The Customer is tasked with all communications with the Processor under this DPA and the Agreement, authorized to act and receive communications on behalf of its Authorized Affiliates in matters concerning this DPA.

11. ADDITIONAL TERMS
11.1. Support for Data Protection Impact Assessments. Upon the Customer's request, the Processor will aid the Customer, at the Customer's expense, in fulfilling their obligation to conduct a data protection impact assessment concerning their use of the Services, as far as this information is not already accessible to the Customer and is available to the Processor. This assistance extends to cooperation or prior consultation with the Supervisory Authority, as necessary under the GDPR or UK GDPR.

11.2. DPA Amendments. Parties may request DPA modifications at least 45 days in advance if required by changes in Data Protection Laws, to ensure lawful Personal Data Processing. Parties will aim to agree on necessary adjustments promptly. The Processor may also unilaterally update this DPA occasionally without notice, as long as such updates do not materially disadvantage the Customer. Should significant changes affect the Customer's rights or Processor's obligations, the Processor will provide notice through its website, the Platform, or email.

Schedule 1 – Processing Activities

Period of Processing
As determined by any part of the DPA and/or the Agreement addressing the Processing period and the aftermath of its conclusion or cancellation, the Processor shall handle Personal Data throughout the Agreement's term and while providing the Services, unless a different arrangement is specified in writing.

Personal Data Types
The Customer has the liberty to input Personal Data into the Services, with the nature and scope being solely at the Customer's discretion.

Data Subject Categories
The Categories of Data Subjects whose Personal Data may be processed by the Processor depend on the Customer and can include, but are not limited to, the following:

- Customer's employees, agents, consultants, and independent contractors;
- Potential clients, existing clients, partners, and suppliers of the Customer;
- Representatives or contacts of the Customer's potential clients, existing clients, partners, and suppliers;
- Any other individual outside party whose Personal Data may be processed through the Services.

Nature and Purpose of Processing
1. Delivering Services to the Customer;
2. Fulfilling the Agreement, this DPA, and/or any additional agreements formed between the Parties;
3. Following the Customer's directives that align with the Agreement's conditions;
4. Distributing Personal Data to external entities following the Customer's directives or as necessitated by the Customer's utilization of the Services (for instance, through connections between the Services and external services, set up by or for the Customer, enabling the exchange of Personal Data between the Services and such external services);
5. Transforming Personal Data into Anonymized Information;
6. Adhering to relevant legal and regulatory requirements;
7. Conducting activities related to the aforementioned points.