Data Processing Agreement

1. **Introduction**. This data processing agreement ("**DPA**") forms an integral part of the master services agreement (the "**Agreement**") between Lusha Systems, Inc. ("**Lusha**") and the Customer. Lusha and the Customer shall hereafter be collectively known as the "**Parties**" and each individually known as a "**Party**". This DPA supersedes and replaces any existing data processing terms in place between the Parties relating to the processing of personal data. To the extent that any of the terms or conditions contained in this DPA may contradict or conflict with any of the terms or conditions of the Agreement, it is expressly understood and agreed that the terms of this DPA shall take precedence.

2. **Definitions**. Capitalized terms used in this DPA but not defined herein or in the Agreement have the meaning ascribed to them in Regulation (EU) 2016/679 General Data Protection Regulation ("**GDPR**") or in the California Consumer Privacy Act (CCPA, Cal. Civ. Code §1798.100 et seq and 11 CCR §999.300) ("**CCPA**").

3. **Scope**. Sections 4 to 8 of this DPA apply only if and to the extent that Lusha acts as a Data Processor to Process Personal Data that Lusha receives from the Customer, where the Customer is a Data Controller subject to: (a) GDPR; and/or (b) the GDPR as it forms part of the laws of the United Kingdom ("**UK**") as retained EU law (as defined in the European Union (Withdrawal) Act 2018), the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and any further UK laws addressing data transfers from the UK (collectively, "**UK GDPR**") with respect to the Personal Data that Lusha Processes. Section 9 of this DPA applies only if and to the extent that Lusha acts as a "service provider" to Process Personal Information that Lusha receives from the Customer, where the Customer is a Business subject to the CCPA.

4. **SCCs**. The Customer and Lusha hereby assent to the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**SCCs**", available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN), as follows:

4.1. In Section II (Obligations of the Parties), Clause 9(a) for MODULE TWO: Transfer controller to processor: The data importer shall specifically inform the data exporter in writing of any intended changes to its list of sub-processors through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). If, in Lusha's reasonable opinion, such objections are legitimate, Lusha shall either refrain from using such sub-processor in the context of the Processing of Personal Data or shall notify Customer of its intention to continue to use the sub-processor. Where Lusha notifies Customer of its intention to continue to use the sub-processor in these circumstances, Customer may, by providing written notice to Lusha, terminate the Agreement immediately.

4.2. In Section IV (Final Provisions), Clause 17 for MODULE TWO: Transfer controller to processor: The Parties agree that this shall be the EU member state in which the Customer is established, or, if the Customer is not established in any EU member state, then the law of the Republic of Ireland.

4.3. In Section IV (Final Provisions), Clause 18(b) for MODULE TWO: Transfer controller to processor: The Parties agree that those shall be the courts of the EU member state's town in which the Customer is established, or, if the Customer is not established in any EU member state, then the courts of Dublin, Ireland.

4.4. In Annex I, for MODULE TWO: Transfer controller to processor:

4.4.1. Data Exporter: Customer.

1. Activities relevant to the data transferred under these Clauses: an organization using Lusha's services which involves Lusha Processing Personal Data received from the Customer.
2. Role: Controller.

4.4.2. Data Importer: Lusha.

1. Activities relevant to the data transferred under these Clauses: Developer, operator and provider of the Lusha services which involve Lusha Processing Personal Data received from the Customer.
2. Role: Processor.

4.4.3. Description of Transfer:

1. Categories of data subjects whose personal data is transferred: business professionals requested by the Customer ("**Contacts**").
2. Categories of personal data transferred: Names, job titles and job affiliation.
3. Sensitive data transferred: None.
4. The frequency of the transfer: on a continuous basis.
5. Nature of the processing: recording, storage, consultation, use, disclosure by transmission and erasure.
6. Purpose(s) of the data transfer and further processing: the provision of Lusha's services.
7. The period for which the personal data will be retained: the period of the Agreement. Lusha shall be entitled to maintain Personal Data following the termination of the main agreement for statistical and/or financial purposes provided that Lusha maintains such Personal Data on an aggregated basis or otherwise after having removed all personally identifiable attributes from such Personal data.
8. Transfers to (sub-) processors: see here.

9 Competent Supervisory Authority: the data protection authority in the EU member state in which the Customer is established, or the Customer's lead supervisory authority for GDPR purposes. If the Customer is not established in any EU member state, then the supervisory authority of the EU member state in which the Customer's EU representative pursuant to Article 27 of the GDPR is located.

4.5. In Annex II, for MODULE TWO (TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA): Transfer controller to processor – See Section 8 below.

4.6. If Lusha's assistance to the Customer under Clause 10 of the SCCs entails material costs, expenses or resources to Lusha, then the Parties shall first discuss and agree on the fees payable to Lusha for such assistance.

5. **Audits.** Not more than once per annum, Lusha shall allow for and contribute to audits conducted under Clause 8.9 of the SCCs, including carrying out inspections on Lusha's business premises conducted by Customer or another auditor mandated by Customer during normal business hours and subject to a prior notice to Lusha of at least 30 days as well as appropriate confidentiality undertakings by Customer covering such inspections in order to establish Lusha's compliance with this DPA and the provisions of the GDPR as regards the Personal Data that Lusha Processes as a Processor on behalf of Customer. If such audits entail material costs or expenses to Lusha, the Parties shall first come to agreement on Customer reimbursing Lusha for such costs and expenses.

6. **Legal basis.** The Customer may only use the Lusha Service to Process Personal Data pursuant to a recognized and applicable lawful basis under the GDPR. The Customer shall provide Lusha only with instructions that are lawful under the GDPR and would not cause Lusha to breach the GDPR.

7. **Additional Safeguards**. Lusha agrees and warrants to implement and maintain a procedure for reviewing, and responding to any subpoena, warrant or other judicial, regulatory, governmental or administrative order, proceeding, demand or request (whether formal or informal) by a non-EEA government or quasi-governmental or other regulatory authority (including law enforcement or intelligence agencies) seeking or requiring access to or disclosure of personal data ("**Government Authority Requests**"). Such procedure shall require that where Lusha receives a Government Authority Request, Lusha shall:

7.1. where permitted by applicable law, promptly notify Customer, in writing, of the Government Authority Request, so that Customer may contest or seek to narrow such disclosure or seek a protective order or other appropriate remedy. Where permitted by applicable law, Lusha shall use reasonable efforts to seek to redirect the relevant requesting authority to request or obtain the Personal Data directly from Customer;

7.2. where permitted by applicable law, provide such reasonable assistance as the Customer may require in responding to the Government Authority Request;

7.3. where permitted by applicable law, promptly notify the Data Subject (if the Data Subject's identity is known to Lusha) of the Government Authority Request;

7.4. where Lusha is prohibited by applicable laws from notifying Customer of the Government Authority Request, Lusha shall use reasonable efforts to seek relevant permission to allow Customer to intervene in the proceedings, scrutinize any such Government Authority Request to determine whether the Government Authority Request is valid, legally binding and lawful and reject or contest any the Government Authority Request that is not valid, legally binding and lawful and will not disclose any information until a competent court of last instance has issued a legally binding order that cannot be further challenged;

7.5. where any attempt to contest, or to seek to narrow such Government Authority Request, or obtain a protective order or seek another remedy is not successful so that some or all the Personal Data is required to be disclosed, Lusha will take reasonable steps to ensure that the Personal Data disclosed or to which access is provided is proportionate and limited to the minimum amount strictly necessary for the purpose of complying with the Government Authority Request; and

7.6. where any Government Authority Request or any subsequent disclosure or other action by Lusha prevents or would prevent Lusha from complying with this DPA or the instructions of the Customer, Lusha agrees to promptly inform the Customer of its inability to comply.

Lusha agrees to maintain a written record that, to the extent permitted by applicable law, includes details of (i) the authority(ies) making the Government Authority Request, (ii) the number of Government Authority Requests received including in relation to the Customer's Personal Data and how Lusha responded to the relevant Government Authority Request, (iii) the types of Personal Data provided in response to a Government Authority Request, and (iv) the number of EEA or UK data subjects whose Personal Data was made available in response to a Government Authority Request. To the extent permitted by applicable law, Lusha shall make aggregated information from such records available to the Customer upon request.

8. **Security Measures.** In this Section, "**Security Measures**" mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Lusha's business, the level of sensitivity of the data collected, handled and stored, and the nature of Lusha's business activities.

8.1. Lusha represents, warrants, and agrees to use Security Measures (i) to protect the availability, confidentiality, and integrity of any Personal Data collected, accessed, or Processed by Lusha in connection with this DPA, and (ii) to protect such data from Personal Data Breach incidents, as more fully described in Schedule 2 (Technical and Organizational Security Measures).

8.2. The Security Measures are subject to technical progress and development and Lusha may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the services procured by the Customer.

8.3. Lusha shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision which has access to, and Processes, Personal Data. Lusha shall ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9. **CCPA.** In its capacity as a Service Provider, Lusha is prohibited from retaining, using or disclosing Customer's Personal Information: (a) For any purpose other than those as set out in the Agreement and specifically to search the Lusha database for information about a Contact (as defined above) at the Customer's request, or as otherwise permitted under 11 CCR §999.314(c); (b) by way of Selling Customer's Personal Information; and (c) by way of retaining, using or disclosing the Customer's Personal Information outside of the direct business relationship between the Parties, except as permitted under 11 CCR §999.314(c). Lusha certifies that it understands the restriction specified in the preceding subsection and will comply with it.

10. **Changes.** Lusha may change this DPA if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of Lusha as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's rights to use or otherwise process Personal Data; or (iii) have a material adverse impact on Customer, as reasonably determined by Lusha. If Lusha intends to change this DPA under this Section, and such change will have a material adverse impact on Customer, as reasonably determined by Lusha, then Lusha will use commercially reasonable efforts to inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

Schedule 1

Processing Details

Processing Operations

The Personal Data Processed by Data Processor will be subject to the following basic Processing activities:

Storage, retrieval, consultation, use and erasure.

Data Subjects

The Personal Data Processed by Data Processor concern the following categories of Data Subjects:

See DPA, Section 4.4.3.1.

Categories of Data

The Personal Data Processed by Data Processor includes the following categories of data:

See DPA, Section 4.4.3.2.

Special Categories of Data (if appropriate)

The Personal Data Processed by Data Processor concern the following special categories of data:

None.

Schedule 2

Technical and Organizational Security Measures

- **Security Policies and Procedures**. Lusha maintains and implements security policies and procedures designed to ensure employees and contractors Process Personal Data in accordance with the SCCs.
- **Intrusion Prevention**. Lusha ensures that its security infrastructure is consistent with leading industry standards for virus protection, firewalls and intrusion prevention technologies to prevent any unauthorized access or compromise of Lusha's network, systems, servers and applications from unauthorized access.
- **Security Awareness Training**. Lusha implements and maintains security awareness training regarding the handling and securing of confidential information and sensitive information such as Personal Data consistent with applicable law.
- **Physical Access Controls**. Lusha has established limits on physical access to information systems and facilities using physical controls (e.g., coded badge access) that provide reasonable assurance that access to data centers and offices is limited to authorized individuals.
- **Logical Access Controls**. Lusha ensures proper user authentication for all employees and contractors with access to Personal Data, including, without limitation, by assigning each employee/contractor unique access credentials for access to any system on which Personal Data Processed by Lusha in accordance with this DPA can be accessed and prohibiting employees/contractors from sharing such access credentials. Lusha restricts and tracks access to Personal Data Processed by Lusha in accordance with this DPA to only those employees/contractors whose access is necessary to perform the services. Lusha implements and maintains logging and monitoring technology to help detect and prevent unauthorized access attempts to networks and production systems. Lusha conducts periodic reviews of changes affecting systems' handling authentication, authorization, and auditing, and privileged access to production systems. Lusha shall ensure that upon termination of any employee/contractor, the terminated employee's access to any Personal Data Processed by Lusha in accordance with this DPA on Lusha's systems will be immediately revoked.
- **Environmental Access Controls**. Lusha implements and maintains appropriate and reasonable environmental controls for data centers, such as air temperature and humidity controls, and appropriate protections against power failures.
- **Disaster Recovery and Back-up Controls**. Lusha maintains: (i) periodic backups of production file systems and databases according to a defined schedule; and (ii) a formal disaster recovery plan for the production data center and conduct regular testing on the effectiveness of such plan.
- **Business Continuity and Cyber Incident Response Plan**. Lusha maintains business continuity and incident response plans to manage and minimize the effects of unplanned events (cyber, physical, or natural) ("**Incident Response Plans**") that include procedures to be followed in the event of an actual or potential security breach or business interruption and which have a stated goal of resumption of routine services within thirty-six (36) hours of such an event. The Incident Response Plans shall require record keeping of root cause analysis and remediation efforts.
- **Storage and Transmission Security**. Lusha secures the transmission of all Personal Data Processed by Lusha in accordance with this DPA and encrypt such data while in motion consistent with industry standards and at a minimum of 256-bit encryption.
- **Internal Audits**. Lusha regularly conducts internal security audits and shall contract annually for external security assessments and penetration tests of Lusha systems including, without limitation, cloud architecture, business processes and procedures, access controls and encryption measures.
- **Risk Identification and Assessment**. Lusha implements and maintains a risk assessment program to help identify foreseeable internal and external risks to its information resources and to determine if existing controls, policies, and procedures are adequate.
- **Vendor and Services Providers**. Prior to engaging new third-party contractors, service providers or vendors who will have access to Personal Data Processed by Lusha in accordance with this DPA (collectively, "**Vendors**"), Lusha shall conduct a risk assessment on Vendor's data security practices. Lusha shall conduct periodic Vendor reviews to ensure compliance with the terms of the SCCs.
- **Change and Configuration Management**. Lusha implements and maintains policies and procedures for managing changes to production systems, applications, and databases, including without limitation, processes for documenting testing and approval of changes into production, security patching, and authentication.
- **Certifications**. Lusha maintains the following third-party certifications: ISO 27001, and other certifications as appropriate.