LAST UPDATED: June 22, 2021

Data Processing Addendum

This Data Processing Addendum (the "**DPA**") is an addendum to The Lincoln Electric Company End-User License Agreement ("**EULA**") and is applicable between The Lincoln Electric Company (the "**Data Processor**") and the Authorized User pursuant to the EULA (the "**Data Controller**"), (each a "**Party**", and together the "**Parties**").

WHEREAS

The EULA governs the right for the Authorized User to use the Licensed Application and, as applicable, other online services provided by The Lincoln Electric Company. For purposes of satisfying its obligations under the EULA, Lincoln Electric Company shall act as a Data Processor on behalf of the Authorized User. In order to ensure compliance with Personal Data regulations, the Parties have agreed to supplement the EULA to set forth the terms and conditions applicable to the Processing of Personal Data by the Data Processor on behalf of the Data Controller.

IT IS AGREED THAT

1. DEFINITIONS

1.1 In this DPA, capitalized terms shall have the following meanings, unless defined in the EULA or otherwise required given the context:

"**Data Controller**" means the entity which determines the purposes and means of the Processing of Personal Data;

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller;

"Data Subject" means an identified or identifiable individual whose Personal Data is being processed;

"Instruction" means the instructions provided by the Data Controller to the Data Processor to Process Personal Data pursuant to the provision of services in accordance with the EULA;

"Personal Data" means any information relating to an identified or identifiable individual; an identifiable individual 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 his or her physical, physiological, genetic, mental, economic, cultural or social identity;

"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;

"Process"/"Processing" /"Processed" means any action performed on Personal Data such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restriction, deletion or destruction;

"Processing Services" means Processing of Personal Data by the Data Processor in connection with the EULA;

"Special Categories of Personal Data" means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership in trade union, associations or foundations, appearance, criminal convictions and security measures, financial and property information, whereabouts information, or credit information and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or data concerning minors aged 14 or below;

"Standard Contractual Clauses" means the standard contractual clauses adopted by the EU Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries or any substitute set of standard clauses agreed between the Parties. Where the Data Controller is established in a jurisdiction outside of the European Union, the references to Member States in the substantive provisions of the Standard Contractual Clauses shall be construed as references to the jurisdiction where the Data Controller is established;

"Subprocessor" means any processor engaged by the Data Processor (or by any other Subprocessor of the Data Processor) to Process Personal Data on behalf of the Data Controller in accordance with its Instructions and the terms of the written subcontract.

1.2 The captions and section headings used are for the purposes of reference and convenience only, are not a part of this DPA, and shall not be used in construing this DPA.

2. SCOPE AND APPLICATION OF THIS DPA

2.1 This DPA only supplements the provisions of the EULA in relation to the Processing Services provided by the Data Processor to the Data Controller pursuant to the EULA.

3. DATA PROCESSING

3.1 The Data Processor agrees to Process the Personal Data in accordance with the terms and conditions set out in this DPA, and in particular the Data Processor undertakes:

3.1.1 to Process the Personal Data only on behalf of the Data Controller and at all times in compliance with the Data Controller's Instructions as defined in this DPA, and all applicable data protection laws;

3.1.2 to ensure that any personnel entrusted with the Processing Services have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality ;

3.1.3 to take technical, physical and organizational measures to ensure the security and confidentiality of the Personal Data and appropriately protect Personal Data Processed on behalf of the Data Controller against misuse and loss, as provided in Schedule 2 of this DPA;

3.1.4 that it will promptly notify the Data Controller about: (a) any legally binding request for disclosure of the Personal Data by a government authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement or intelligence investigation, (b) any Personal Data Breach affecting the Personal Data processed on behalf of the Data Controller, (c) any request received directly from the Data Subjects (including rights to access, rectification, deletion, objection, restriction, data transfer, and the right not to be subject to a decision based solely on automated Processing, including profiling); the Data Processor (i) will not respond directly to that request, except to notify the Data Subject that it is acting on behalf of the Data Controller and to furnish the Data Subject with the contact information of the Data Controller, and (ii) taking into account the nature of the Processing, will assist the Data Controller by appropriate technical, physical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights;

3.1.5 to provide commercially reasonable cooperation to the Data Controller to assist the Data Controller comply with its own legal obligations related to Personal Data security, such as: notification of a Personal Data Breach to the competent supervisory authority, communication of such Personal Data Breach to the Data Subjects affected and, where applicable, implementation of data protection impact assessments and prior consultations with supervisory authorities, taking into account the nature of the Processing and the information available to the Data Processor;

3.1.6 to make available to the Data Controller all information necessary to prove compliance with the obligations laid out in this DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller as set forth in Section 6; and, 3.1.7 that any Processing Services carried out by a Subprocessor will be carried out in accordance with Section 7.

3.2 With respect to the Processing Services, the Data Controller will be responsible for complying with all requirements that apply to it under applicable law regarding the Processing of Personal Data and the Instructions it issues to the Data Processor. In particular but without prejudice to the generality of the foregoing, the Data Controller acknowledges and agrees that it will be solely responsible for the following: (i) the accuracy, quality, and legality of Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable law for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations from Data Subjects or otherwise; (iii) ensuring the Data Controller has the right to transfer, or provide access to, the Personal Data to the Data Processor and that the Data Controller has provided any required notifications and obtained any required consents and/or authorizations in relation to that transfer or access and, more generally, for Processing in accordance with the terms of the EULA (including this DPA); and (iv) ensuring that its Instructions comply with applicable laws. Upon request from the Data Processor, the Data Controller shall provide to the Data Processor within three (3) business days written evidence of such notifications, consents and authorizations. The Data Controller will not input into the Processing Services, or otherwise provide the Data Processor, with any Special Categories of Personal Data, unless otherwise agreed to separately in writing by the Data Controller. The Data Controller will inform the Data Processor, immediately and without undue delay, if Data Controller is not able to comply with its responsibilities set forth in this DPA. The Authorized User is solely responsible for reviewing the Processing Services, including any available security documentation and features, to determine whether they satisfy the Authorized User's requirements, business needs, and legal obligations.

3.3 The Data Controller authorizes the Data Processor to anonymize the Personal Data Processed pursuant to the EULA in order to derive analytics data relating to the use of Licensed Application and the Lincoln products and equipment. Further use of the resulting statistical data by the Data Processor is not subject to prior authorization from the Data Controller.

4. <u>INTERNATIONAL DATA TRANSFERS</u>

4.1 The Data Controller hereby acknowledges and agrees that, for providing the Processing Services under the EULA, the Data Processor may transfer and retain Personal Data in the United States of America, and any other country in which the Data Processor is located, for the purpose of providing the Processing Services. Therefore, in the course of the provision of the Processing Services, it may be necessary to transfer Personal Data to the Data Processor located outside of the country of establishment of the Data Controller. If the Data Controller is located in the European Economic Area or in Switzerland, the Parties undertake to apply the provisions of the Standard Contractual Clauses for the transfer of Personal Data by the Data Controller (acting as data exporter pursuant to the Standard Contractual Clauses) to the Data Processor (acting as data importer pursuant to the Standard Contractual Clauses).

4.2 If the Data Controller is located outside of the European Economic Area and Switzerland, the Parties also undertake to apply the provisions of the Standard Contractual Clauses for the transfer of Personal Data by the Data Controller (acting as data exporter pursuant to the Standard Contractual Clauses) to the Data Processor (acting as data importer pursuant to the Standard Contractual Clauses), provided that the Standard Contractual Clauses are legally required and sufficient to meet the requirements of the applicable data protection regulations for the transfer of Personal Data by the Data Controller to the Data Processor pursuant to the EULA.

4.3 If the Parties apply the Standard Contractual Clauses pursuant to Sections 4.1 or 4.2 of this DPA:

4.3.1 Appendix 1 of the Standard Contractual Clauses shall be applied on the following basis: (a) Data exporter: the Data Controller, (b) Data importer: the Data Processor, (c) Data subjects: personnel of the Data Controller (the Authorized User), (d) Categories of data: data relating to the use of products and equipment owned, licensed, or managed by the Data Processor, as monitored by the Licensed Application pursuant to the EULA, including registration data (i.e., usernames and passwords), (e) Special Categories of Personal Data: N/A, and (f) Processing operations: collection, copy, transfer, storage, modification, deletion and other operations necessary for the Processing Services pursuant to the EULA.

4.3.2 The description of the technical, physical and organizational security measures implemented by the Data Processor acting as data importer for the purpose of Appendix 2 of the Standard Contractual Clauses shall be as provided in Schedule 2 of this DPA.

4.4 If the Standard Contractual Clauses are applicable between the Parties pursuant to Section 4.1 or 4.2, their provisions will be deemed incorporated by reference into this DPA, unless the Parties execute the Standard Contractual Clauses as a standalone document pursuant to Section 4.5.

4.5 To the extent required by the applicable data protection regulations, the Parties shall enter into and execute the Standard Contractual Clauses as a separate document.

5. TERMINATION

5.1 This DPA will become effective upon the effective date of the EULA.

5.2 This DPA will terminate automatically upon the later of termination or expiry of (a) the EULA or (b) of the Data Processor's obligations in relation to the Processing Services, and such termination shall not require a court order or court proceeding or any other action of the Data Processor, the Data Controller or any other party in order to be effective. Where applicable, on termination of this DPA, the Data Processor shall return to the Data Controller or delete, at the Data Controller's request, all the Data Controller's Personal Data in its possession or under its control. Upon the request of the Data Controller, the Data Processor shall confirm compliance with such obligations in writing and delete all existing copies, unless applicable law requires storage or otherwise permits retention of the Personal Data.

5.3 The Data Controller shall be entitled to terminate this DPA by notice in writing to the Data Processor if the Data Processor is in a material or persistent breach of this DPA which, in the case of a breach capable of remedy, shall not have been remedied within thirty (30) working days from the date of receipt by the Data Processor of a notice from the Data Controller identifying the breach and requiring its remedy.

5.4 The Data Processor shall be entitled to terminate this DPA by notice in writing to the Data Controller if the Data Controller is in a material or persistent breach of this DPA which, in the case of a breach capable of remedy, shall not have been remedied within thirty (30) working days from the date of receipt by the Data Controller of a notice from the Data Processor identifying the breach and requiring its remedy.

6. AUDITS AND INFORMATION REQUESTS

6.1. Within the limit of one (1) audit per year and subject to the notification by the Data Controller with a thirty (30) day prior notice, except in the case of an audit requested by a supervisory authority, the Data Controller may during regular business hours, without unreasonably interfering with Data Processor's business operations, personally audit the Data Processor, or appoint a third-party auditor being subject to confidentiality obligations to carry out such audit.

6.2. The Data Processor shall cooperate in the case of an audit under this Section 6 and provide to the Data Controller all information necessary to carry out such audit. The Data Controller shall cover the costs and expense incurred by each party in relation to audits under this Section 6.

7. APPOINTMENT OF SUBPROCESSORS

7.1 The Data Controller authorizes the Data Processor to use the service of Subprocessors listed in the page accessible at [https://www.lincolnelectric.com/en/Legal-Information/Subprocessors], solely as required for the performance of the Services in connection with the EULA.

7.2 The Data Controller authorizes the Data Processor to use the services of new Subprocessors, subject to prior notification to the Data Controller by the Data Processor with a fifteen (15) day notice prior to the change of Subprocessor. If the Data Controller objects to the change of Subprocessor notified, the Data Controller may, throughout the period of notice, terminate this DPA in writing. If the Data Controller does not terminate within the notice period, this formalizes the consent of the Data Controller to the notified change of Subprocessor.

7.3 In any event, where the Data Processor uses the services of a Subprocessor the latter shall be, by way of contract, bound to comply with the same obligations to which the Data Processor is bound in terms of Personal Data Processing under this DPA.

8. MISCELLANEOUS PROVISIONS

8.1 Amendments or additions to this DPA must be made in writing to be effective. Notwithstanding the foregoing, the Data Processor may, at any time and without notice to Data Controller, amend the technical, physical and organizational measures set forth in Schedule 2, provided such amendment does not materially impact the security, confidentiality, or integrity of Personal Data.

8.2. References in this DPA to “writing” or “written” includes e-mail communications and certified mail.

8.3 Should any provision of this DPA be or become invalid, this shall not affect the validity of the remaining terms. In the event of invalidation of any provision of this DPA, the Parties shall, in any case, endeavor, in good faith, to replace the invalidated provision by another one, enforceable, valid and legal, having to the greatest possible extent a legal impact equal or equivalent to the one of the initial provision.

8.4 This DPA is governed by the same governing law as the EULA.

SCHEDULE 1 - JURISDICTION SPECIFIC TERMS

When the Data Controller is established in one of the jurisdictions listed in this Schedule 1 the following terms apply for the DPA, and such terms shall supersede and control in the event of any conflict with the other provisions of the DPA. All terms in the EULA that are not specifically modified by the applicable jurisdiction-specific terms in this Schedule remain unchanged and in full force and effect.

Brazil:

The Parties acknowledge and agree that the following change to the DPA shall apply:

a) All occurrences of "Special Categories of Personal Data" in the DPA shall be replaced by "Sensitive Personal Data".

Mexico:

The Parties acknowledge and agree that the following changes to the DPA shall apply:

a) All occurrences of "Special Categories of Personal Data" in the DPA shall be replaced by "Sensitive Personal Data";

b) For the application of the Standard Contractual Clauses, all references to "transfers" of personal data shall be construed as remissions of personal data in accordance with Mexican Federal law on the Protection of Personal Data held by the Private Parties ("*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*").

Russia:

In addition to the provisions of the DPA, the Parties undertake as follows:

a) The Data Processor hereby confirms that it is fully aware that the purpose of the Personal Data Processing activities pursuant to the DPA are only to provide the Processing Services and shall process the Personal Data only for the purpose for which the Personal Data is disclosed and the Data Controller requires it from the Data Processor. In addition, the Data Processor shall promptly confirm in writing that this rule is observed upon request from the Data Controller.

b) Prior to disclosing the Personal Data originated from Russian nationals to the Data Processor, the Data Controller shall ensure that all such Personal Data has been recorded, systemized, accumulated, stored, clarified (updated, changed), and extracted with the use of databases located in the territory of the Russian Federation when such Personal Data was collected in any manner, including via the Internet.

c) If the Data Controller detects illegal processing or inaccuracy of the Personal Data, the Data Controller shall immediately instruct the Data Processor to block this Personal Data and initiate an inspection. The affected Personal Data shall be blocked for the whole inspection period. If the inspection confirms inaccuracy of the Personal Data, the Data Controller shall request the relevant Data Subject (his/her representative) or the data protection authority (if applicable) for the amendments and forward them to the Data Processor. Inaccurate Personal Data shall be amended shortly, and within seven (7) business days at the latest, from the day when the amendments were delivered to the Data Processor. The Personal Data shall be unblocked immediately upon amendment.

d) If it is detected that the Personal Data is processed illegally, the Data Controller shall instruct the Data Processor to stop such illegal processing within three (3) business days from the date of detection. If it appears to be impossible to eliminate the violations and ensure the legality of the Personal Data processing, then the Data Controller shall instruct the Data Processor to destroy the illegally processed Personal Data within ten (10) business days from the date of detection. The Data Controller shall be also obliged to notify the relevant Data Subject (his/her representative) and, when required by law, the data protection authority about the elimination of the violations.

e) If a Data Subject revokes his/her consent to the Personal Data processing, the Data Controller shall immediately notify the Data Processor and the Data Processor shall stop the processing and destroy the Personal Data of this Data Subject within thirty (30) days from the date of receipt by the Data Controller of the cancellation notice.

f) If it is impossible to comply with the time periods set forth in Clauses d) and e) here above, the Data Processor shall block the relevant Personal Data at the request of the Data Controller for at most six (6) months and destroy this Personal Data within the same period unless applicable law prescribes otherwise.

South Africa:

The Parties acknowledge and agree that the following changes to the DPA shall apply with respect to the definitions provided in section 1 of the DPA:

a) “Data Subject” means a person whose Personal Data is being processed.

b) “Personal Data” means personal information as defined in POPIA, including any information relating to an identified or identifiable individual.

c) “POPIA” means the South African Protection of Personal Information Act 4 of 2013, and any binding regulation, directive, ruling, order or guideline published under POPIA.

United States:

In addition to the provisions of the DPA, the Parties undertake as follows:

a) Each Party acknowledges and agrees that the collection and disclosure of Personal Data transmitted to the Processing Services (i) does not constitute, and is not the intent of either party for such activity to constitute, a sale of Personal Data, and (ii) if valuable consideration, monetary or otherwise, is being provided by Authorized User to Data Processor, such valuable consideration, monetary or otherwise, is so being provided for use of the Processing Services and not for the disclosure of Personal Data. Data Processor shall not retain, use, disclose, or sell Personal Data for any purpose other than for the specific purpose of performing the Processing Services, or as otherwise permitted by law or the EULA. For the avoidance of doubt, Data Processor shall not sell Personal Data or authorize or otherwise permit any Subprocessor to undertake the same, unless otherwise permitted by the EULA or applicable law.

Schedule 2 - Security Measures implemented by the Data Processor

1. Physical Access control to premises and facilities

Data Processor will implement technical and organizational measures to control access to premises and facilities, particularly to check authorization to ensure prevention of unauthorized access.

Specifically:

- Access control system
- ID reader, magnetic card, chip card
- Issue of keys
- Door locking
- Security staff, guards
- Surveillance facilities
- Alarm system, video/CCTV monitor

2. Access control to systems

Data Processor will implement technical (ID/password security) and organizational measures for user identification and authentication to prevent unauthorized access to IT systems.

Specifically:

- Password procedures (incl. special characters, minimum length, change of password)
- Automatic blocking (e.g. password or timeout)
- Encryption of data media, including removable and portable.

3. Logical Access control to data

Data Processor will ensure activities in IT systems not covered by the allocated access rights will be prevented by utilizing requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses.

Specifically:

- Role-based access rights (profiles, roles, transactions and objects)
- Use of a commercial Privileged Account Management solution to facilitate the secure authentication of administrative accounts to systems for maintenance or other administrative purposes
- Automated reports that are regularly reviewed and followed up on for anomalous or suspicious activity
- Access, using a least privilege model to only permit access to systems and/or data based on need-to-know

4. Disclosure and Data Protection Control

Data Processor will control Personal Data disclosure by incorporating measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking via electronic transfer, data transport and transmission control.

Specifically:

- Encryption/tunneling
- Electronic signature
- Logging and continuous monitoring of security events and alerts
- Transport security to encrypt data in transit
- Encryption of data at-rest
- Regular rotation of encryption keys
- Restriction of access to encryption keys to limited persons
- Password complexity enabled, with two-factor authentication required for all remote access sessions

5. Input control

Data Processor will maintain full documentation of data management and maintenance must be maintained, including measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

Specifically:

- Logging and reporting systems

6. Job control

Data Processor will Process Personal Data according to Data Controller's instructions and to agree to measures (technical/organizational) to segregate the responsibilities between the Data Controller and the Data Processor:

Specifically:

- Unambiguous wording of the contract
- Formal commissioning (request form)
- Criteria for selecting the Data Processor
- Monitoring of contract performance

7. Availability control

Data Processor will ensure that data will be protected against accidental or malicious destruction or loss by taking measures to assure the physical and logical security of the data.

Specifically:

- Backup procedures
- Mirroring of hard disks, e.g. RAID technology
- Uninterruptible power supply (UPS)
- Remote or disk-based storage that is replicated to alternate data centers
- Anti-virus and/or anti-malware software that is updated regularly and application-aware firewall systems configured with default deny statements, permitting only traffic explicitly allowed for business purposes
- Business Continuity and Disaster Recovery Plan

8. Segregation control

Data Processor will seek to ensure that data collected for different purposes will be Processed separately and not co-mingled with other customer data by implementing specific measures to provide for separate Processing (storage, amendment, deletion, transmission) of data for different purposes:

Specifically:

- "Internal client" concept / limitation of use
- Segregation of functions (production/testing)