最后更新日期：2021 年 6 月 22 日

数据处理附录

本《数据处理附录》（“**DPA**”）是《林肯电气公司最终用户许可协议》（“ **EULA** ”）的附录，适用于林肯电气公司（“**数据处理者**”）和 EULA 规定的授权用户（“**数据控制者**”）（各称以下称为“**一方**”，统称为“**双方**”）之间。

鉴于

EULA 规定了授权用户使用授权应用程序以及林肯电气公司提供的其他在线服务（若适用）的权利。为履行 EULA 规定的义务，林肯电气公司应代表授权用户担任数据处理者。为确保遵守个人数据法规，双方同意补充 EULA，以规定适用于数据处理者代表数据控制者处理个人数据的条款和条件。

双方特此约定如下：

1. 定义

1.1 在本 DPA 中，以大写字母表示术语应具有以下含义，除非 EULA 中定义或根据上下文另有要求：

“数据控制者”	是指确定个人数据处理目的和方式的实体；
“数据处理者”	是指代表数据控制者处理个人数据的实体；
“数据主体”	是指其个人数据正在被处理的已识别或可识别身份的个人；
“指示”	是指数据控制者向数据处理者提供的指示，以根据 EULA 提供的服务处理个人数据；
“个人数据”	是指与已识别或可识别身份的个人有关的任何信息；可识别身份的个人是可以直接或间接识别其身份的人，特别是通过参考身份标识符，例如姓名、身份证号码、位置数据、在线标识符，或其特定的一个或多个身体、生理、遗传、心理、经济、文化或社会身份等因素；
“个人数据泄露”	是指违反安全导致意外或非法破坏、丢失、更改、未经授权披露或访问已传输、存储或以其他方式处理的个人数据；
“处理”	是指对个人数据执行的任何操作，例如收集、记录、组织、存储、改编或更改、检索、咨询、使用、通过传输、传播、转移或以其他提供方式进行披露、整理或组合、限制、删除或销毁；
“处理服务”	是指数据处理者对与 EULA 相关的个人数据进行的处理；
“特殊类别的个人数据”	是指揭示种族或民族血统、政治观点、宗教或哲学信仰、或工会、协会或基金会成员身份、外表、刑事定罪和安全措施、财务和财产信息、行踪信息或信用信息的任何个人数据，以及处理基因数据、用于唯一识别自然人的生物特征数据、健康数据、或自然人性生活或性取向数据，或者关于14岁以下未成年人的数据；
“标准合同条款”	是指欧盟委员会 2010 年 2 月 5 日以第 2010/87 号决议通过的关于将个人数据传输到在第三国设立的处理者的标准合同条款，或双方商定的任何替代标准条款集。如果数据控制者设立在欧盟以外的司法管辖区，标准合同条款的实体规定中提到的成员国应解释为数据控制者设立所在的司法管辖区；
“下级处理者”	是指数据处理者（或数据处理者的任何其他下级处理者）聘请的按照其指示和书面分包合同的条款代表数据控制者处理个人数据的任何处理者。

1.2 本 DPA 中使用的标题和条款标题仅供参考和方便查阅之用，不属于本 DPA 的组成部分，并且不得用于解释本 DPA。

2. 本 DPA 的范围和适用

2.1 本 DPA 仅补充 EULA 中关于数据处理者根据 EULA 向数据控制者提供的处理服务的规定。

3. 数据处理

3.1 数据处理者同意根据本 DPA 中规定的条款和条件处理个人数据，尤其是数据处理者承诺：

3.1.1 仅代表数据控制者处理个人数据，并始终遵守本 DPA 中定义的数据控制者的指示以及所有适用的数据保护法律；

3.1.2 确保委托履行处理服务的任何人员已承诺保密或承担适当的法定保密义务；

3.1.3 按照本 DPA 附件 2 的规定，采取技术、物理和组织措施确保个人数据的安全性和机密性，并适当保护代表数据控制者处理的个人数据免遭滥用和丢失；

3.1.4 其将立即通知数据控制者：(a) 任何政府主管部门提出的要求披露个人数据的具有法律约束力的请求，除非另有禁止，例如刑法禁止保留执法或情报调查的机密性， (b) 影响代表数据控制者处理的个人数据的任何泄露，(c) 直接从数据主体收到的任何请求（包括访问权、更正权、删除权、反对权、限制权、数据传输权以及不受仅基于自动化处理（包括数据画像）的决定之约束的权利）；数据处理者 (i) 不会直接回应该请求，除非通知数据主体其正在代表数据控制者实施行为，并向数据主体提供数据控制者的联系信息，以及 (ii)基于到处理的性质，将在可能的情况下通过适当的技术、物理和组织措施协助数据控制者，以履行数据控制者回应数据主体关于行使权利请求的义务；

3.1.5 向数据控制者提供商业上合理的合作，以协助数据控制者履行其承担与个人数据安全相关的法律义务，例如：向主管监管机构通知个人数据泄露，将此类个人数据泄露通知受影响的数据主体，并且在适用的情况下，基于处理的性质和数据处理者可获得的信息，实施数据保护影响评估并与监管机构事先协商；

3.1.6 向数据控制者提供所有必要的信息，以证明遵守本 DPA 中规定的义务，并且允许和协助由数据控制者或数据控制者委托的其他审计人员进行第6条中所述的审计（包括检查）；以及

3.1.7 下级处理者履行的任何处理服务将按照第 7 条规定进行。

3.2 关于处理服务，数据控制者将负责遵守适用法律中关于个人数据的处理以及其向数据处理者发出指示的所有要求。特别是但不影响上述基本规定之前提下，数据控制者确认和同意其将全权负责以下事项：(i) 个人数据的准确性、质量和合法性；(ii) 在收集和使用个人数据时遵守适用法律规定的所有必要的透明度和合法性要求，包括从数据主体或其他方获得任何必要的同意和授权；(iii) 确保数据控制者有权向数据处理者传输或提供对个人数据的访问权，并且数据控制者已提供任何必要的通知，已获得与该传输以及与根据EULA（包括本DPA）的条款进行数据处理相关的任何必要的同意和/或授权；以及 (iv) 确保其指示符合适用法律。经数据处理者要求，数据控制者应在三 (3) 个工作日内向数据处理者提供关于此类通知、同意和授权的书面证据。数据控制者不会将任何特殊类别的个人数据输入到处理服务中，或以其他方式向数据处理者提供任何特殊类别的个人数据，除非数据控制者另行书面同意。如果数据控制者无法履行其在本 DPA 中规定的职责，数据控制者将立即通知数据处理者，不得无故拖延。授权用户全权负责审查处理服务，包括任何可用的安全文档和功能，以确定它们是否满足授权用户的要求、业务需求和法律义务。

3.3 数据控制者授权数据处理者对根据 EULA 处理的个人数据进行匿名处理，以获取与使用授权应用程序和林肯产品和设备相关的分析数据。数据处理者对由此产生的统计数据的进一步使用无须获得数据控制者的事先授权。

4. 国际数据传输

4.1 数据控制者在此确认和同意，为了根据 EULA 提供处理服务，数据处理者可以在美国以及数据处理者所在的任何其他国家传输和保留个人数据，以提供处理服务。因此，在提供处理服务的过程中，可能有必要将个人数据传输到位于数据控制者所在国家以外的数据处理者。如果数据控制者位于欧洲经济区或瑞

士，双方则承诺将标准合同条款的规定适用于数据控制者（根据标准合同条款作为数据出口方）将人数据传输至数据处理者（根据标准合同条款作为数据进口方）。

4.2 如果数据控制者位于欧洲经济区和瑞士以外，双方还承诺将标准合同条款的规定适用于数据控制者（根据标准合同条款作为数据出口方）将个人数据传输至数据处理者（根据标准合同条款作为数据进口方），但前提是标准合同条款是法律要求的，并且足以满足关于数据控制者根据EULA将个人数据传输至数据处理者的适用数据处理法规要求。

4.3 如果双方根据本 DPA 第 4.1 条或第 4.2 条规定适用标准合同条款：

4.3.1 标准合同条款的附件 1 应在以下基础上适用：(a) 数据出口方：数据控制者，(b) 数据出口方：数据处理者，(c) 数据主体：数据控制者（授权用户）的人员，(d) 数据类别：与使用数据处理者拥有、许可或管理的产品和设备相关的数据，该等数据由授权应用程序根据 EULA 进行监控，包括注册数据（即，用户名和密码），(e) 特殊类别的个人数据：不适用，以及 (f) 处理操作：根据 EULA 提供处理服务所需的收集、复制、传输、存储、修改、删除和其他操作。

4.3.2 就标准合同条款附件 2 所述的目的而言，作为数据进口方的数据处理者实施的技术、物理和组织安全措施的描述应在本 DPA 的附件 2 中规定。

4.4 如果标准合同条款根据第 4.1 条或第 4.2 条在双方之间适用，其条款则将被视为通过引述纳入本 DPA，除非双方根据第 4.5 条将标准合同条款作为独立文件进行签订执行。

4.5 在适用的数据保护法规要求的范围内，双方应作为单独的文件签订并执行标准合同条款。

5. 终止

5.1 本 DPA 将在 EULA 生效日期时生效。

5.2 本 DPA 将在 (a) EULA 或 (b) 数据处理者与处理服务相关的义务终止或到期后（以日期在先者为准）自动终止，并且此终止不需要法院命令或法院程序，或者数据处理者、数据控制者或任何其他方采取任何其他行动。在适用的情况下，当本 DPA 终止时，数据处理者应返还数据控制者或按照数据控制者的要求删除其持有或控制的所有数据控制者的个人数据。经数据控制者要求，数据处理者应以书面方式确认遵守该等义务并删除所有现有副本，除非适用法律要求存储或以其他方式允许保留个人数据。

5.3 如果数据处理者严重违反或持续违反本 DPA，并且在可以补救的情况下，但是在数据处理者收到数据控制者指明违规且要求补救的通知之日起三十（30）个工作日内未得到补救，数据控制者有权书面通知数据处理者终止本 DPA。

5.4 如果数据控制者严重违反或持续违反本 DPA，并且在可以补救的情况下，但是在数据控制者收到数据处理者指明违规且要求补救的通知之日起三十（30）个工作日内未得到补救，数据处理者有权书面通知数据控制者终止本 DPA。

6. 审计和信息请求

6.1. 在每年不超过一（1）次审计的限度内，并且经数据控制者提前三十 (30) 天通知后，除非监管机构要求进行审计，数据控制者可在正常营业时间在不会无理干扰数据处理者的业务运营的情况下，亲自或指定第三方审计人员（须承担与该审计相关的保密义务）对数据处理者进行审计。

6.2. 数据处理者应在根据第 6 条进行的审计中给予配合，并向数据控制者提供进行此类审计所需的所有信息。数据控制者应承担各方因第 6 条规定的审计而产生的费用和支出。

7. 下级处理者的指定

7.1 仅在履行EULA相关服务所需的情况下，数据控制者授权数据处理者使用在 [https://www.lincolnelectric.com/en/Legal-Information/Subprocessors] 可访问的页面中列出的下级处理者的服务。

7.2 数据控制者授权数据处理者使用新的下级处理者的服务，但是数据处理者须在下级处理者变更前提前十五 (15) 天通知数据控制者。如果数据控制者对通知的下级处理者的变更提出异议，数据控制者可以在通知期间内以书面方式终止本 DPA。如果数据控制者未在通知期内终止，则表明数据控制者正式同意下级处理者的变更。

7.3 在任何情况下，如果数据处理者使用下级处理者的服务，下级处理者应通过合同遵守与数据处理者根据本 DPA 处理个人数据相关的同等义务。

8. 其他条款

8.1 对本 DPA 的修订或补充必须以书面形式进行方可生效。尽管有上述规定，数据处理者可以随时在不通知数据控制者的情况下修改附件 2 中规定的技术、物理和组织措施，但前提是此修订不会对个人数据的安全性、机密性或完整性产生重大影响。

8.2. 本 DPA 中提到的“书面”包括电子邮件通信和挂号邮件。

8.3 如果本 DPA 的任何条款无效或变得无效，这不会影响其余条款的有效性。如果本 DPA 的任何条款无效，双方则应在任何情况下真诚地努力将无效的条款替换为另一项可执行、有效且合法的条款，并且该替代条款应尽可能与原先条款具有相同或等同的法律效力。

8.4 本 DPA 受与 EULA 相同的适用法律管辖。

附件 1 - 司法管辖区特定条款

如果数据控制者在本附件 1 中所列的司法管辖区之一设立，以下条款则应适用于 DPA；如果该等条款与 DPA 的其他规定存在冲突，则应以该等条款为准并替代 DPA 中存在冲突的规定。EULA 中未由本附件中适用的司法管辖区特定条款专门修改的所有条款应保持不变且具有完全效力。

巴西：

双方确认和同意适用对 DPA 作出的以下修改：

a) DPA 中所有出现的“特殊类别的个人数据”均应替换为“敏感个人数据”。

墨西哥：

双方确认和同意适用对 DPA 作出的以下修改：

a) DPA 中所有出现的“特殊类别个人数据”均应替换为“敏感个人数据”；
b) 对于标准合同条款的适用，所有提到的个人数据“传输”均应解释为根据墨西哥联邦关于保护私人持有的个人数据的法律（“*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*”）进行的个人数据转发。

俄罗斯：

除 DPA 的规定以外，双方承诺如下：

a) 数据处理者在此确认，其完全了解根据 DPA 开展的个人数据处理活动的目的仅是提供处理服务，并且应仅出于披露个人数据的目的处理个人数据，而数据控制者需要数据处理者提供的处理服务。此外，当数据控制者要求时，数据处理者应及时以书面方式确认其已遵守此规则。
b) 在向数据处理者披露源自俄罗斯国民的个人数据之前，在以任何方式（包括通过互联网）收集此类个人数据时，数据控制者应确保所有此类个人数据已被记录、系统化、积累、保存、澄清（更新、更改）并使用位于俄罗斯联邦境内的数据库进行提取。
c) 如果数据控制者检测到个人数据的非法处理或不准确，数据控制者应立即指示数据处理者封锁此个人数据并启动检查。受影响的个人数据将在整个检查期内被封锁。如果检查确认个人数据不准确，数据控制者应要求相关数据主体（或其代表）或数据保护机构（若适用）进行修改，并将修改转发给数据处理者。不准确的个人数据应在相关修改交付给数据控制者之日起七（7）个工作日内尽快进行修改。个人数据一经修改将立即解除封锁。
d) 如果发现个人数据被非法处理，数据控制者应指示数据处理者在发现之日起三 (3) 个工作日内停止此类非法处理。如果可能无法消除违规行为并且为了确保个人数据处理的合法性，数据控制者应指示数据处理者在发现之日起十 (10) 个工作日内销毁非法处理的个人数据。数据控制者还应通知相关数据主体（或其代表），并在法律要求的情况下通知数据保护机构其已消除违规行为。
e) 如果数据主体撤销其对个人数据处理的同意，数据控制者应立即通知数据处理者，数据处理者应在数据控制者收到取消通知之日起三十（30）天内停止处理并销毁此数据主体的个人数据。
f) 如果无法遵守上述 d) 项和 e) 项规定的期限，数据处理者应在收到数据控制者的要求后，在最长不超过六（6）个的期限内封锁相关个人数据，并在此期限内销毁该等个人数据，除非适用法律另有规定。

南非：

双方确认和同意，对 DPA 的以下修改应适用于 DPA 第 1 条提供的定义：

a) “数据主体”是指正在被处理的个人数据的拥有主体。
b) “个人数据”是指 POPIA 中定义的个人信息，包括与已识别或可识别身份的个人有关的任何信息。
c) “POPIA”是指南非 2013 年第 4 号《个人信息保护法》，以及根据 POPIA 发布的任何具有约束力的法规、指令、裁决、命令或指南。

美国:

除 DPA 的规定以外，双方承诺如下：

a) 各方确认和同意，收集和披露传输进行处理服务的个人数据 (i) 不构成，并且任何一方不希望此类活动构成个人数据的销售，以及 (ii) 如果授权用户向数据处理者提供有偿对价（包括金钱或其他形式），此有偿对价（包括金钱或其他形式）均是为了使用处理服务而提供，而不是为了披露个人数据而提供。除非为了履行处理服务或者存在法律或EULA允许的其他情况，否则数据处理者不得为任何目的保留、使用、披露或销售个人数据。为免生疑义，除非 EULA 或适用法律另行允许，数据处理方不得出售个人数据，亦不得授权或以其他方式允许任何下级处理者出售个人数据。

附件 2 - 数据处理者实施的安全措施

1. 对场所和设施的物理访问控制

数据处理者将实施技术和组织措施，以控制对场所和设施的访问，特别是检查授权以确保防止未经授权的访问。

具体如下：

- 门禁系统
- ID读卡器、磁卡、芯片卡
- 钥匙发放
- 门锁
- 保安人员、警卫
- 监控设施
- 报警系统、视频/闭路电视监视器

2. 对系统的访问控制

数据处理者将实施技术（ID/密码安全）和组织措施识别和验证用户身份，以防止对 IT 系统的未授权访问。

具体如下：

- 密码程序（包括特殊字符、最小长度、密码更改）
- 自动阻止（例如，密码或超时）
- 数据载体的加密，包括可移动和便携式数据载体。

3. 对数据的逻辑访问控制

数据处理者将使用授权方案和访问权限的需求驱动定义以及访问的监控和日志记录，以确保阻止未包含在分配的访问权限范围内的 IT 系统活动。

具体如下：

- 基于角色的访问权限（配置文件、角色、交易和对象）
- 使用商业特权帐户管理解决方案促进管理帐户对系统的安全身份验证，以用于维护或其他管理目的
- 定期审查和跟进异常或可疑活动的自动生成报告
- 使用最小权限模型，仅允许基于需要知悉原则访问系统和/或数据

4. 披露和数据保护控制

数据处理者将在数据载体（手动或电子）上传送、传输和交流或存储数据时采取措施，以及通过电子传输、数据传送和传输控制进行后续检查，从而对个人数据的披露进行控制。

具体如下：

- 加密/隧道
- 电子签名
- 记录并持续监控安全事件和警报
- 确保传输安全，对传输中的数据进行加密
- 静态数据加密
- 定期轮换加密密钥
- 仅限有限的人员访问加密密钥
- 启用复杂密码要求，所有远程访问会话都需要两重因素身份验证

5. 输入控制

数据处理者将维护数据管理和维护的完整文档，包括后续检查数据是否已输入、更改或清除（删除）的相关措施，以及关于由谁实施输入、更改或清除（删除）的记录文档：

具体如下：

- 记录和报告系统

6. 作业控制

数据处理者将根据数据控制者的指示处理个人数据，并同意采取（技术/组织）措施以分离数据控制者与数据处理者之间的职责：具体如下：

- 合同措辞明确
- 正式调试（申请表）
- 选择数据处理者的标准
- 监督合同履行

7. 可用性控制

数据处理者将采取措施确保数据的物理和逻辑安全性，确保数据免遭意外或恶意破坏或丢失。

具体如下：

- 备份程序
- 硬盘镜像，例如 RAID 技术
- 不间断电源（UPS）
- 复制到备用数据中心的远程或基于磁盘的存储
- 定期更新的防病毒和/或反恶意软件以及使用默认拒绝语句配置的应用程序感知防火墙系统，仅允许明确许可用于业务目的的流量
- 业务连续性和灾难恢复计划

8. 隔离控制

数据处理者将通过实施特定措施，为不同目的对数据进行单独处理（存储、修改、删除、传输），以确保为不同目的收集的数据将被单独处理，而不会与其他客户数据混合：

具体如下：

- “内部客户”概念/使用限制
- 职能分离（生产/测试）