LYDALL, INC.隐私权政策

生效日期：2018年6月1日

A. 范围

1. Lydall, Inc.及其全球子公司（以下简称“Lydall”或“本公司”）遵循这些用于指导Lydall或其“代理”（定义见下文）对于“个人信息”的收集、使用、存储、传递和最终销毁等工作的原则。个人信息将按照以下所述方式进行管理，以确保本公司遵守关于个人信息的收集、传递和使用的法律及合约标准。本政策适用于Lydall及其全球运营公司。Lydall将把本政策的覆盖范围延伸至访问和/或处理个人信息的第三方。

2. 对于在欧盟区域内收集的个人信息，这些原则旨在用于满足2018年5月生效的《欧盟一般数据保护条例》（简称“GDPR”）的要求。

3. 对于从欧盟传递到美国的个人信息的收集、使用和留存，Lydall遵守美国商务部规定的《欧盟－美国隐私盾协议》（EU-U.S. Privacy Shield Framework，简称“隐私盾协议”）。Lydall已向美国商务部提交了其遵守隐私盾协议原则的认证。此认证包括Lydall和Lydall的认证证书中列出的适用实体，证书的网址为：www.privacyshield.gov/list。如果本隐私权政策的条款与隐私盾协议原则之间存在任何冲突，则以隐私盾协议原则为准。Lydall需遵从美国联邦贸易委员会的调查和执行权力。 如需进一步了解隐私盾协议计划并查看我们的认证，请访问 www.privacyshield.gov/。

4. 根据美国加利福尼亚州的法律，加州居民可以使用本政策中所述的联系信息，索取Lydall在前一个日历年内与其他企业分享的、用于直接市场营销的信息（若有）（如《加利福尼亚州反客户信息披露法 (Shine the Light Law)》中所定义）。

5. 根据美国康涅狄格州的法律，Lydall保护社会保障号（简称“SSN”）的机密性，禁止非法披露并限制取得个人的SSN。Lydall不会蓄意向公众传播SSN、将SSN打印在个人访问产品或服务所需的任何文件上、要求个人通过未加密的互联网连接传送SSN，或是要求个人使用SSN访问互联网站（除非同时需要密码或其他唯一性的标识性内容）。

6. 当Lydall符合《美国健康保险流通与责任法案》（U.S. Health Insurance Portability and Accountability Act，简称“HIPAA”）中的“适用实体”的定义时，会遵守这项法律。“适用实体”的定义详见下文。HIPAA只适用于在美国运营的实体。

B. 定义

1. “代理”指任何为了代表Lydall和根据Lydall的指示执行任务而控制或处理个人信息的第三方。

2. HIPAA中的“商业伙伴”指为适用实体提供服务的服务提供者。

3. HIPAA中的“适用实体”的定义见45 C.F.R. § 160.103。

4. “数据泄露”是指涉及到对于个人信息的实际或有理由认为可能的未经过授权的访问或拥有，或导致个人信息丢失或损毁的任何一种情形。造成泄露的情形可能是无意的或意外性的，而数据的访问、丢失或损毁可以是已经得到确认的，也可以仅是疑似的。个人信息的丢失或损毁可能有很多种方式，例如计算机硬件（如笔记本电脑）失窃、由于自然灾害或事故而导致的物理损毁或泄露（如办公室淹水而损毁某些记录的唯一版本），以及若无预期解决方案即无法访问服务器上的唯一数据版本，或持续超过一周无法访问数据。数据泄漏可能包括在第三方或商业伙伴办公地点对于数据的未授权访问和拥有，或拒绝服务。

5. “个人信息”指与某个已识别或可识别的自然人有关的信息，无论这些信息是以何种媒介收集、处理或传递。此术语包括敏感性个人信息。此术语包括有关Lydall董事、员工、承包商、合同工、客户、供应商或其他第三方的信息。用于统计、历史、科学或其他目的的匿名汇总信息不包括在内。此术语包括以任何格式（包括但不限于硬拷贝、电子、录像和录音）收集、处理和/或传递的信息。

6. “受保护的健康信息”或其缩写“PHI”是HIPAA独有的术语，指适用实体以任何形式或媒介（无论是电子、纸张还是口头）持有或传播的所有可识别的个人健康信息。“可识别的个人健康信息”是指与个人过去、现在或未来身体或心理健康或状况有关的信息、关于向个人提供医疗保健服务的信息、关于在过去、现在或未来向个人支付医疗保健费用的信息，以及能用于识别个人身份或有合理依据相信能用于识别个人身份的信息，包括人口统计数据。可识别的个人健康信息包括许多常见的标识性内容（例如姓名、地址、出生日期、社会保障号等）。

7. “敏感的个人信息”是个人信息的一个子集，指与某个已识别的个人或可识别个人相关的、涉及种族或族裔、政治观点、宗教或哲学信仰、工会成员身份、健康、性偏好、性生活或实施任何犯罪行为或被指称实施任何犯罪行为的信息。

C. 隐私权原则

1. 遵守法律法规：Lydall遵守适用于其全球各地的运营单位的个人信息保护相关法律法规。如当地法律、法规和其他相关限制与本政策出现任何冲突，则以当地法律、法规和其他相关限制为准。如隐私盾协议原则或GDPR与本政策有任何冲突，则以隐私盾协议原则或GDPR为准。

2. 个人信息的收集、使用和保留：

a. Lydall仅在出于对于合法商业和法律目的必要而且适当的情况下收集、使用和保留个人信息，同时确保个人信息的收集、处理和传递恰当、切合实际且不超出处理信息的目的的范围。

b. Lydall对于董事、员工和第三方的个人信息的收集和使用包括收集和使用**附件1**中所详细描述的个人信息。在某些情况下（例如针对人力资源数据时），为了便于Lydall管理雇佣关系和关于薪酬及福利的合同协议，必须收集相关数据。

c. 除法律有所要求或取得数据主体同意的情况以外，Lydall保留个人信息的时间不会超过为了实现收集目的而需要的时间。

3. 声明：

a. Lydall直接向个人收集个人信息时，会向其告知收集和使用其个人信息的目的、Lydall向其披露该信息的代理的类型，以及Lydall为了限制其使用和披露而提供的选择和方法。Lydall会鉴别收集个人信息的目的，且不会出于任何与该目的不一致的目的而处理个人信息，除非获得了个人数据主体的同意，或为了满足法律义务、或因遇到人身威胁而被迫为之，或得到了法律认可的其他合法利益的支持。

b. 当个人第一次被要求向Lydall提供此类信息或在现实允许情况下尽快提供时，以及在Lydall在任何情况下将信息用于最初的收集目的之外的目的之前，均会以清晰明显的语言提供声明。在任何可行的情况下，隐私权声明应发布在网络上且数据主体应有查阅的权限；

c. Lydall就个人对于数据的访问、更正和更新的权利提供适当的声明。Lydall确保在根据任何自动化决策（例如员工背景调查）来采取任何负面的行动之前，让个人有机会讨论该决策的结果；

d. Lydall将互联网和其他技术视为与员工、客户、业务合作伙伴和其他人员进行沟通和互动的宝贵工具。 Lydall认可维护在线收集的信息的隐私性非常重要，并为其网站制定了具体的互联网隐私权政策，以便管控通过其运营的网站收集的个人信息的处理。 关于从欧洲经济区（简称“EEA”）传递出的个人信息，每个网站的隐私权政策均服从本隐私权政策。Lydall确保其每个收集个人信息的在线网站（包括外部网站/万维网和内部网站/内网）都提供隐私权声明。 隐私权声明识别：

1. 收集的个人信息；
2. 收集个人信息的目的；
3. Lydall使用个人信息的方式；
4. 外部网站是否使用“Cookie”或其他跟踪设备，以及如果使用Cookie需如何重新配置浏览器以拒绝Cookie；
5. Lydall与哪些第三方共享信息；
6. 向个人提供的选择，限制收集、使用和披露个人信息的方法，以及这些选择的后果；和
7. 如何联系Lydall提出涉及网站的、关于隐私权事项的问题或投诉，或如何更正/更新已提供的个人信息。

e. 每份隐私权声明至少每三年由负责人审阅一次，以确保其及时性和准确性。如法律要求收集敏感的个人信息，Lydall确保仅在取得个人通过切合实际的选择加入方式明确同意的情况下才会在线收集敏感的个人信息，并适当地防止对敏感性个人信息的不当使用。

4. 同意：

a. 根据数据主体居住地的不同，当地法律可能会要求数据主体针对附件1中所述的某些目的表达对于个人信息之收集、使用和披露的明确同意。选择加入的个体会被告知执行此项选择需遵循的流程。

b. 如有需要，Lydall会以适当且被允许的方式征得同意。如果个人信息将 (1) 披露给Lydall代理，或 (2) 用于最初收集或随后取得授权的目的以外的目的，Lydall会向个人提供选择不再提供个人信息的机会。Lydall偶尔会向个人告知可从选定的非代理第三方获得的优惠。对于敏感的个人信息，Lydall在 (1) 向非代理第三方披露信息之前，或在(2) 将信息用于最初收集的目的或随后取得授权的目的以外的目的之前，会向个人提供让他们表达是否肯定地、明确地选择加入的机会。使用个人信息进行直接营销时，Lydall会向个人提供适当的选择退出的机会。

5. 访问和更正：

a. Lydall会采取合理措施来确保个人信息与其预期用途相关、准确、完整和及时更新。

b. 如**附件2**所描述，Lydall会向个人授予访问其个人信息的合理权限。此外，Lydall采取合理措施允许个人更正、修订或删除已证明不准确或不完整的信息。此外，数据主体有对于数据处理提出反对意见的权利，对于数据可携带性也拥有权利。如果数据主体已对数据处理表示明确的同意，那么数据主体仍有权随时撤回该同意。

6. 数据安全：

a. Lydall采取合理的预防措施来保护其所拥有的个人信息，以防丢失、滥用和未经授权的访问、披露、更改或损毁。Lydall计算机网络和系统（包括基于互联网和内网的应用程序）旨在防止个人信息遭受未经授权的访问、丢失、披露或使用。在Lydall内部，个人信息仅提供给因正当业务需求而需要知晓的人员。

b. Lydall维护系统和程序，以确保个人信息（无论是由员工提供、由Lydall及其运营公司生成，还是由代理或第三方提供）的安全性和完整性。这些措施包括合理限制对包含个人信息的硬拷贝记录的实际访问，以及将此类记录存储在锁定的设施、存储区域或容器中。

c. 安全计划针对包含个人信息的任何记录的安全性、机密性和/或完整性，识别并评估可合理预见的内部和外部风险，并在必要时评估和改进目前限制此类风险的保护措施的有效性。安全计划包括：

- 正在进行的员工（包括临时员工及合同制员工）培训；
- 确保员工遵守安全计划的政策和程序的方法；

- 用于检测和防止安全计划失败的方法；
- 针对员工、关于在业务系统或经营场所以外存储、访问和运输包含个人信息的记录的安全政策；
- 对于违反安全计划的纪律处分措施；
- 防止离职员工访问记录的方法；
- 定期进行监控，以确保安全计划的运行方式经合理计算，防止个人信息的未经授权的访问或未经授权使用，并根据需要升级信息安全措施，以限制风险；
- 每年对安全规则的范围进行一次审查，当业务实践做法发生可能会影响个人信息的安全性或完整性的重大变化时，则会更加频繁地审查；
- 记录针对导致安全性遭到破坏的事件所采取的响应行动，在事件发生后对事件和所采取行动（若有）进行的强制性审查，以改变有关个人信息保护的业务实践；以及
- 在处置之前对停止使用的存储器或其他媒介执行卫生处理和销毁程序。

d. Lydall定期对这些措施进行重新评估，以确保其保持及时性、合理性和适当性。

e. Lydall不会将个人信息从一个国家传递到另一个国家，或从一个法律实体传递到另一个法律实体，除非得到适当法律支持，并且在传输和存储过程中对数据采取适当的安全措施；

f. Lydall确保对员工和第三方个人信息的处理与针对相关信息的隐私权声明一致，并遵守根据当地情况所做的补充或修改内容，以确保符合当地法律。

g. Lydall通过保护其机密性、限制收集、确保进行的访问只基于知情需求、实施适当的安全措施（包括但不限于加密），并确保根据Lydall的文件和数据保留政策和做法进行妥善处置，来对政府颁发的身份识别号码进行妥善保管。

7. 数据泄露：

A. Lydall维护并实施数据泄露响应计划，用以响应和纠正任何实际的数据泄露事件，并根据法律要求披露涉及个人信息的泄露情况。

8. 向第三方传递个人信息：

a. 个人信息由Lydall实体、代理（例如IT和其他专业和非专业服务机构、福利计划发起人和管理人员等）使用和共享。Lydall还根据政府机构的合法要求披露个人信息，包括满足国家安全或执法方面的要求。在法律、法规或法庭命令的许可或要求下，Lydall需将个人信息披露给适用的政府组织和机构以及第三方。Lydall与Lydall所收购和转让的公司共享个人信息，并影响Lydall所剥离的公司的分拆情况。

b. 如果第三方提供给Lydall的服务涉及访问个人信息，则会对第三方进行挑选和管理，以便他们能够保持适当的安全措施来保护这些信息，并通过合同要求来执行和保持适当的安全措施。Lydall签署书面协议，强制要求代表Lydall收集、处理、访问或拥有个人

信息的第三方承担遵守本政策或同等要求的责任。书面协议使用高级副总裁、总法律顾问和首席行政官批准的标准条款和条件。Lydall会向数据接收方取得保证，让其保证将始终一致地根据本隐私权政策来保护个人信息的安全。适当的保证的例子包括：要求代理至少提供相关的“隐私盾协议原则”认证所要求的相同级别的保护的合同、协议或相关规定；由代理进行隐私盾协议认证；或需遵循欧盟委员会作出的充分性裁决。

c. Lydall及其运营单位执行和维护欧盟委员会通过的标准条款（也称为标准合同条款），将其当作将个人信息从欧洲经济区传递到美国的授权。Lydall及其各运营单位在公司内部传递方面遵循标准条款的要求。 如要授权将个人信息传递给第三方，Lydall和/或其运营单位需与服务提供商签订标准条款。 在转发的情况下，Lydall需负责根据隐私盾协议规定来处理其收到的、之后再传递给担任其代理的第三方的个人信息。如果其代理以不符合隐私盾协议原则的方式处理此类个人信息，则根据隐私盾协议原则，Lydall应承担责任，除非该组织证明其对造成损害的事件不需承担责任。

d. 当Lydall得知数据接收方以违反本政策的方式使用或披露个人信息时，Lydall会采取合理措施阻止或停止相关使用或披露，情况严重者将导致我们与该代理的合同或其他业务关系的终止。

8. 遵守HIPAA：

a. 需遵守《美国健康保险流通与责任法案》（“HIPAA”）的Lydall运营单位：

- 保持合理的措施以保护受保护的健康信息的隐私；
- 在Lydall的外部网站上，向其收集受保护的健康信息的个人，发布关于其保护隐私权做法的声明；
- 与代表Lydall处理受保护的健康信息的任何第三方签订适当的商业伙伴协议；并
- 确保正确和及时地就任何数据泄露发布通知。

9. 隐私风险评估：

a. Lydall保持一套有效的隐私风险评估流程，用以评估全公司的风险并制定适当的风险缓解计划。隐私风险评估流程审核Lydall的个人信息收集、处理（包括存储和销毁）及传输的整体过程，并根据需要对其进行更新。

b. 当Lydall或运营单位寻求实施新系统或修改版系统，或使用一个新的第三方或改变对于收集、处理或传递个人信息的第三方的使用时，在采用新流程或修改版流程或是新使用或修改使用第三方之前，需完成书面的隐私影响评估。隐私影响评估必须仅针对收集、处理或传递个人信息的系统或服务提供商来完成，以及仅针对启动涉及个人信息的新系统或新服务提供商，或对系统或服务提供商的使用进行重大修改来完成。

10. 管控与培训：

a. Lydall确保以任何实质方式参与收集、使用和存储个人信息（包括设计、修改或管理自动化系统）的个人都经过培训，以便能够识别隐私疑虑、接收隐私投诉，并将其转发给适当的支持人员进行审查和解决。此外，每个运营单位至少任命一名专业人员，针对与隐私保密相关的问题，担任本地管理人员和职员的支持人员。Lydall隐私合规组织和员工的架构由高级副总裁、总法律顾问和首席行政官不时根据需要进行管理、评估和修改。

b. Lydall确保将个人信息作为其职责组成部分的所有专业人员和员工每年接受一次关于数据隐私和安全性的培训。
Lydall为所有员工提供关于正确使用计算机安全系统和信息安全的重要性的教育和培训，例如限制收集和存储不必要的信息、使用加密、限制访问驱动器、文件夹和文件、认识文件共享程序对信息安全造成的风险。

c. Lydall制定了战略沟通计划，用以提高员工和第三方（如适用）对数据隐私和安全性的意识并为他们提供教育培训。

d. Lydall以定期自我评估和/或审核的形式进行“保证审查”，并设有热线，用来接收关于违反本隐私政策的保密性举报。此举是为了验证本政策是否得到了遵守，并支持美国商务部的年度隐私盾协议合规认证。高级副总裁、总法律顾问和首席行政官，以及副总裁、首席会计官和总会计师负责管理保证和审核计划，以评估员工组织和运营单位遵守本政策的情况。Lydall的内部和外部审核员会定期审核运营单位和员工组织，以确保本政策得到了遵守。

e. Lydall执行本政策和任何实施程序。未遵守本政策或其实施程序可能导致员工受到纪律处分，严重者可导致解雇；对于第三方来说，则其与Lydall的合同关系可能会被终止。

D. 问题与争议

1. 有关某个特定网站或系统的问题或疑虑，应发送给该网站或系统上提供的隐私权声明中所列出的联系人。

2. 员工的访问或更正请求应发送给其当地的人力资源代表。

3. 有关遵守本政策的投诉或问题应发送给Lydall的高级副总裁、总法律顾问和首席行政官。

4. 如有关于本隐私权政策的问题或意见，可通过以下方式联系：

- 通过信函邮寄到：Lydall, Inc., General Counsel, P. O. Box 151, Manchester, CT 06045-0151 USA

- 电话：1-800-454-7958
- 拨打免费电话800-454-7958通过Lydall的Workplace Alert Line（工作场所警报热线）联系，也可以通过安全的加密互联网连接在Workplace Alert Line上提交。
- 根据《加利福尼亚州反客户信息披露法 (Shine the Light Law)》要求提供的信息应通过电子邮件发送至privacy@lydall.com，并在主题栏以及邮件正文中加上“加利福尼亚州反客户信息披露法隐私请求”。

5. 涉及隐私盾协议的投诉：

a. 根据与从欧洲经济区向美国传递个人信息相关的隐私盾协议原则，Lydall承诺解决有关我们收集或使用此类个人信息的投诉。

- Lydall将在收到个人与Lydall的首次联系后的45天内，根据本政策中包含的原则开展调查并尝试解决问题、投诉和争议。
- 对于Lydall无法解决的投诉，Lydall向个人免费提供独立的追索机制，以便用于调查和迅速解决每个人的投诉和争议，具体如下：

    - 如果争议涉及到从欧盟转移到美国Lydall的人力资源数据，在个人与Lydall存在雇佣关系的情况下，相关个人可以联系其原籍国的数据保护管理局（简称“DPA”）。Lydall将配合及遵循相关DPA给出的建议。
    - 如果争议涉及人力资源数据以外的事项，Lydall进一步承诺让个人免费提出投诉。决定行使这一选项的个人必须：（1）直接向Lydall提出其指控的违规行为，并给予Lydall 45天的时间解决问题；（2）联系相应的欧盟DPA；（3）通过DPA向美国商务部提出举报，并期待商务部尽最大努力在90天内解决问题。
    - 如果上述机制未能完全彻底解决争议，Lydall承诺会根据个人数据主体的请求，对任何剩余求偿权采取有约束力的仲裁。个人可以利用这一选项来确定Lydall是否违反了“隐私盾协议原则”中其关于该个人所承担的义务，以及是否有任何此类违规行为全部或部分未得到解决。有约束力的仲裁的范围和要求详见“隐私盾协议原则”附录I。

E. 本政策的修订

1. Lydall会根据需要修改本政策，以使其与欧盟－美国隐私盾协议原则相一致，或使其准确地反映Lydall的实践和政策的任何变化。每一次修改均会时会提供适当的通知。

附件1
所收集个人信息的类型及其用途

Lydall收集和共享的个人信息的类型取决于个人与Lydall之间关系的性质（例如董事、员工、客户、供应商、其他第三方）以及适用法律的规定/限制。此类信息的例子有：

- 管理层和员工的沟通与通知；
- 员工简介、简历和类似信息的保管；
- 紧急联系人；
- 全球企业人数和人口统计资料；
- 职业生涯发展、绩效反馈和进展；
- 人员配置规划；
- 接班人规划；
- 薪酬和福利；
- 员工福利的设立和管理以及福利计划；
- 奖励和认可；
- 差旅和费用报销，包括差旅和/或信用卡管理；
- 培训；
- 调动；
- 税务申报与代扣；
- 工资管理，包括扣除、供款等；
- 企业资源规划（ERP）系统；
- 劳资关系，包括申诉程序；
- 规划和提供保健服务，包括药物筛查、处理工人伤残赔偿或类似的健康和安全计划；
- 个人安全，包括计算机和其他系统的访问控制和安全；
- 报告和统计分析；
- 人事事务，包括在公司的任期、聘用/雇佣关系开始日期、离职日期和其他事务的日期，如晋升、加薪等；
- 法律和监管报告以及其他要求，包括工作权利筛查、工作场所环境、健康和安全报告以及管理；
- 签证、许可证和其他工作权利许可；
- 管理诉讼和相关的证据披露/电子证据披露问题；
- 进出口和其他贸易合规控制，包括自动化IT控制；
- 制裁筛查，包括筛查美国实体名单（U.S. Entity List）、被特别指认国民和被阻禁者名单（Specially Designated Nationals and Blocked Persons List）、禁止人员名单（Denied Persons List）和未经证实名单（the Unverified List）以及美国和其他国家保存的类似名单；
- 内部和外部调查，包括管理层审核及对Lydall在我们开展业务的所有地方遵守法律和法规情况的审核；对员工遵守法律情况、Lydall的《道德与商业行为守则》以及公司政策的审核与审查；与Lydall举报热线（合规热线）进行的在线和电话联系；
- 互联网、内网、电子邮件、社交媒体和其他电子筛查；
- 执法和其他政府调查；
- 业务规划，包括对于兼并、收购和资产剥离的起诉，包括向被收购公司获取个人信息以及将个人信息传递给被剥离公司；
- 通过照片或其他类似方式识别人员身份，包括面部识别；
- 某些Lydall资产的位置跟踪、持续时间和其他远程信息处理；
- 时间收集和分配；
- 出于内部企业管理目的进行的数据挖掘；

- 生物识别技术；
- 取证分析；
- 向提供福利的供应商提供的数据；
- 物理和信息技术安全监测；
- 数据备份和恢复；以及
- 自动化信息技术威胁评估和响应。
- 名字和姓氏，包括后缀；
- 中间名；
- 偏好的名字；
- 出生国；
- 所持国籍（过去和现在）；
- 美国和其他国家永久居民和/或受庇护者身份；
- SMTP地址；
- 工作地点，包括街道通信地址和其他相关联系信息；
- 家庭住址及其他相关联系信息；
- 主管的标识符；
- 与工作有关的信息，如职位、部门、工作职能、职称等。
- 其他用于辅助人力资源应用的数据；
- 管理报告和数据挖掘（通常为匿名，不包含能识别个人身份的数据）；
- 计算机资产位置和账单数据，包括计算机位置；
- 对于住在Lydall经营地点的第三方居民，通过照片或其他形象识别人员（包括面部识别）、位置跟踪、持续时间和其他远程信息处理、生物识别数据、取证分析、物理和信息技术安全监测、制裁筛查和自动化信息技术威胁评估和响应。
- 时间收集和分配；
- 电子邮件内容（被最终用户控制的）；
- 邮件的附件（被最终用户控制的）；
- 公用文件夹的内容（本地管理员提供文件夹权限）；
- 网页地址；
- 即时消息地址；和
- 日历数据（会议室和会议厅信息，包括任何用户提供的附于日历条目和会议通知上的附件）；
- 授权、授予、管理、监控和终止访问或使用Lydall的系统、设施、记录、财产和基础设施；
- 客户和供应商合同和协议、合资企业及其他企业组合的管理；
- 对营销工作的支持；
- 预算规划和管理；
- 与发票处理和支付相关的目的；
- 客户和供应商人员的培训和认证；
- 作为职位申请和招聘流程的一部分而收集的数据；
- 背景调查和合规筛查；
- 解决问题、内部调查、审核审计、合规、风险管理和安全；
- 项目管理；
- 利益冲突报告；
- 公司通讯；
- 现场伤害和疾病评估和报告（针对访问Lydall设施者）；
- 工业卫生、公共卫生和安全的监控和监测；
- 法律诉讼和政府调查，包括保存相关数据；以及
- 根据全球各地适用于我们的业务的法律或法规的要求或明确授权，或根据全球各地监督我们业务的政府机构的要求或明确授权；
- 个人数据（如出生日期、出生日或年份、国籍、习惯语言）；
- 传记、简历和类似信息；
- 组织和机构从属关系；
- 专业证书；
- 数据主体参与的协议、计划和活动；
- 与Lydall签订的协议；

- 与付款相关的信息，包括社会保障号或税务识别码和银行信息；
- 沟通偏好；
- 教育和培训；
- 工业卫生暴露评估和监测信息；
- 计算机或设施访问和身份验证信息（例如身份识别代码、密码、地址列表等）；
- 数据主体的照片和其他视觉图像；
- 提供投资者服务；
- 提供您所请求的信息、项目或服务；
- 与您沟通有关Lydall的产品、服务和活动；
- 改进我们的产品、服务和网站；
- 评估您对Lydall的兴趣和/或允许您申请Lydall的工作；
- 验证您的身份以确保此处列出的其他目的之一的安全性；
- 确保或加强Lydall电子系统的安全性；
- 防止欺诈；
- 根据法律的要求，按照制裁和反恐名单进行筛查；
- 回应执法机关或其他政府监管机构的合法请求；
- 调查涉嫌或实际的非法活动；
- 防止人身伤害或财务损失；以及
- 支持我们的全部或部分业务或资产的出售或转让（包括通过破产）。

附件2

访问和更正个人数据

对于需遵守《欧盟一般数据保护条例》的Lydall员工和第三方，通常在我们收到您（或您指定的合格法定代表）提交的个人数据后一个月内（除某些例外情况外），Lydall会尽力为您提供以下各项信息：

- 对于Lydall是否正在处理您的个人数据的确认，以及处理这些数据的地点；
- 关于处理这些数据的目的的信息；
- 关于正在被处理的您的数据所属类别的信息；
- 关于可能获得共享数据的接收者所属类别的信息；
- 关于数据存储周期（或用于确定该周期的标准）的信息；
- 关于您所拥有的清除、更正这些数据的权利以及限制对于这些数据进行处理和反对对于这些数据进行处理的权利的信息；
- 关于您向欧盟相关数据保护机构申诉的权利的信息；
- 对于不是直接向您收集的数据：关于数据从何而来的信息；以及
- 关于是否存在自动化处理的信息；关于如何使用“自动化处理”方式来对您的数据进行处理的解释；以及/或者关于如何使用“自动化处理”方式、且仅仅基于自动化处理来作出关于您的或关于您的数据的决策的解释。

您可以索取一份您的正在被处理的个人数据的拷贝。拷贝将以支持重复使用的结构化的、常用的、机器可读的格式提供。如果我们收到合理的要求，Lydall会将您的个人数据从一个数据控制方传递至另一个数制控制方，将您的个人数据存储在私人设备上供个人使用，以及/或将您的个人数据畅通无阻地直接从Lydall传递给另一个控制方。这一点不适用于不是由您直接提供给Lydall的个人数据，Lydall也没有义务将您的个人数据保留到超过其所需要的时间。

通常情况下，Lydall不对上述各项工作收取任何费用。但是，根据法律规定，我们保留对重复的、过度的或无根据的请求和额外的拷贝收取合理费用的权利。

Lydall会采取一切合理措施，确保不准确或不完整的个人数据被清除或得到更正。您有权向Lydall告知任何资料不相符或不准确的情况，也有要求更正不准确的个人数据的权利。

在下列情况下，您有权对于您的个人数据的继续处理作出限制：

- 您对自己的个人数据的准确性提出质疑（且只限于验证和纠正您的数据的准确性所需的时间）；
- 对于数据的处理违反法律，因而您要求限制这种处理（而不是行使数据清除权利）；
- Lydall不再出于其原始目的而需要该数据，但Lydall仍然需要将该数据用于建立、行使或维护其合法权利；或

- 如果您正当地要求清除或销毁您的数据，但Lydall正在评估保留和处理您的数据的超越您的权利的其他理由。
- 在以下情况下，Lydall会清除您的个人数据，或以其他方式将其改为无法访问：
- 不再出于其原始目的而需要您的数据（并且不存在新的合法目的）；
- 处理数据的法律依据是您表示同意，而您撤销了相关同意，且不存在令数据继续存在的任何其他合法理由；
- 您行使反对Lydall继续处理您的数据的权利，并且Lydall公司没有关于继续处理您的数据的、超越您的权利的理由；
- 您的数据已被非法处理；或
- 数据清除是您遵守欧盟法律或欧盟相关成员国法律的必要条件。

如果Lydall已经向任何第三方披露您的个人数据，而您随后行使上述任何权利，则Lydall将通知这些第三方（除非无法履行或需要付出不成比例的努力）。您可以要求被告知这些第三方的身份。在Lydall已将您的数据公开的特殊情况下，Lydall将采取合理措施（考虑成本）通知各相关第三方。

关于实施这些要求的问题，应按照本政策其他部分的规定处理。