LYDALL, INC. PRIVACY POLICY

EFFECTIVE: June 1, 2018

A. SCOPE

1. Lydall, Inc. and its worldwide subsidiaries ("Lydall" or "the Company") follow these principles regarding the collection, use, storage, transfer, and eventual destruction of "Personal Information" by Lydall or its "agents" (as defined below). Personal Information will be managed as described below to ensure that the company adheres to legal and contractual standards regarding the collection, transfer, and use of Personal Information. This Policy applies to Lydall and its global operating companies. Lydall will extend the requirements of this Policy to third parties that access and/or process Personal Information.

2. For Personal Information collected in the European Union ("EU) these principles are intended to meet the requirements of the EU's General Data Protection Regulation ("GDPR") effective May 2018.

3. Lydall complies with the EU-U.S. Privacy Shield Framework ("Privacy Shield") as set forth forth by the U.S. Department of Commerce regarding the collection, use and retention of personal information transferred from the EU to the United States. Lydall has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. This certification includes Lydall and the covered entities listed under Lydall's certification found at www.privacyshield.gov/list. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. Lydall is subject to the investigatory and enforcement powers of the Federal Trade Commission. To learn more about the Privacy Shield Program, and to view our certification, please visit www.privacyshield.gov/.

4. In accordance with the law of the State of California, U.S.A., California residents may request and obtain information (if any) that Lydall shared within the prior calendar year with other businesses for direct marketing use (as defined by California's "Shine the Light Law"), using the contact information described in this Policy.

5. In accordance with Connecticut, U.S.A. law, Lydall protects the confidentiality of, prohibits unlawful disclosure of, and limits access to Social Security numbers ("SSNs"). Lydall does not intentionally communicate SSNs to the general public, print SSNs on any document required for an individual to access products or services, require an individual to transmit SSNs over an unencrypted Internet connection, or require an individual to use SSNs to access an Internet web site unless a password or other unique is also required.

6. Lydall complies with the U.S. Health Insurance Portability and Accountability Act ("HIPAA") to the extent it is a "covered entity," as defined below. HIPAA only applies to entities operating in the United States.

B. DEFINITIONS

1. "Agent" means any third party that controls or processes Personal Information to perform tasks on behalf of and under the instructions of Lydall.

2. "Business Associate" is a service provider to a Covered Entity under HIPAA.

3. "Covered Entity" under HIPAA is defined at 45 C.F.R. § 160.103.

4. "Data Breach(es)" is any set of circumstances that involves actual or a reasonable possibility of unauthorized access to or possession of, or the loss or destruction of Personal information. The circumstances contributing to a breach may be unintentional or accidental and the access, loss, or destruction may be confirmed or only suspected. Personal information can be lost or destroyed in many ways, such as by stolen computer hardware (e.g., laptops), physical destruction or compromise due to natural disaster or accidents (e.g., flood of an office, destroying the only copy of certain records); and inability to access the only copy of data on a server if there is no anticipated resolution or the inability to access lasts for more than a week. Data Breaches can include unauthorized access, possession or denial of service at a third party or Business Associate.

5. "Personal Information" means information relating to an identified or identifiable natural person, regardless of the medium in which the information is collected, processed, or transferred. The term includes Sensitive Personal Information. The term includes information about a Lydall director, employee, contractor, contract laborer, customer, supplier, or other third party. Anonymous aggregate information used for statistical, historic, and scientific or other purposes is excluded. The term includes information collected, processed, and/or transferred in any format, including but not limited to hard copy, electronic, video recording, and audio recording.

6. "Protected Health Information" or "PHI" is a term unique to HIPAA, and means all Individually Identifiable Health Information held or transmitted by a Covered Entity, in any form or media, whether electronic, paper, or oral. "Individually Identifiable Health Information" is information, including demographic data, that relates to an individual's past, present or future physical or mental health or condition; the provision of healthcare to the individual; or the past, present, or future payment for the provision of healthcare to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually Identifiable Health Information includes many common identifiers (e.g., name, address, birth date, Social Security number, etc.).

7. "Sensitive Personal Information" is a subset of Personal Information and means information relating to an identified or identifiable person that involves racial or ethnic

origin; political opinions; religious or philosophical beliefs; trade union membership; health; sexual preference; sex life; or the commission or alleged commission of any crime.

C. PRIVACY PRINCIPLES

1. Compliance with Laws and Regulations: Lydall complies with laws and regulations applicable to its operating units worldwide that relate to the protection of Personal information. Local laws, regulations, and other pertinent restrictions will apply to the extent of any conflicts with this Policy. The Privacy Shield Principles or the GDPR shall govern in the event of any conflict with this Policy.

2. Collection, Use, and Retention of Personal Information:

a. Lydall collects, uses, and retains Personal Information only as necessary and appropriate for legitimate business and legal purposes, ensuring that the collection, processing, and transfer of Personal Information are adequate, relevant, and not excessive in relation to the purpose or purposes for which the information is processed.

b. Collection and uses by Lydall of the Personal Information of directors, employees and third parties include the collection and use of Personal Information described in detail in **Exhibit 1**. In some cases, such as with human resources data, the data are necessary in order for Lydall to manage employment relationships and contractual agreements regarding pay and benefits.

c. Lydall does not keep Personal Information for longer than needed for the purpose(s) for which it was collected, unless otherwise required by law or with consent;

3. Notices:

a. When Lydall collects Personal Information directly from individuals, it informs them about the purposes for which it collects and uses Personal Information about them, the types of agents to which Lydall discloses that information, and the choices and means Lydall offers for limiting its use and disclosure. Lydall identifies the purposes for which it is collecting Personal Information and does not process the Personal Information for any incompatible purpose(s) unless supported by consent of the individual data subject, a legal obligation, a threat of physical harm, or another legitimate interest recognized by law.

b. Notice is provided in clear and conspicuous language when individuals are first asked to provide such information to Lydall, or as soon as practicable thereafter, and in any event before Lydall uses the information for a purpose other than that for which it was originally collected. Privacy notices shall be accessible to data subjects and posted online whenever practicable;

c. Lydall provides appropriate notices regarding individuals' rights of access, correction, and updating. Lydall ensures that an individual is given the chance to discuss

the results of any automated decision-making (such as employee background checks) before any negative action is taken based on that decision-making;

d. Lydall sees the Internet and the use of other technologies as valuable tools for communicating and interacting with employees, customers, business partners, and others. Lydall recognizes the importance of maintaining the privacy of information collected online and has created specific Internet privacy policies for its websites, governing the treatment of Personal Information collected through web sites that it operates. With respect to Personal Information that is transferred from the European Economic Area ("EEA"), each website privacy policy is subordinate to this Privacy Policy. Lydall ensures that each of its online websites (both external/www. and internal/intranet) that collect Personal Information provide a privacy notice. The privacy notice identifies:

1. The Personal Information that is collected;
2. The purpose(s) for which that Personal Information is collected;
3. The ways that Lydall uses Personal Information;
4. Use of "cookies" or other tracking devices by external-facing websites and, if used, how to reconfigure the browser to decline the cookies;
5. Third parties with whom Lydall shares the information;
6. The choices provided to individuals, the means for limiting collection, use, and disclosure of Personal Information, and the consequences of those choices; and
7. How to contact Lydall with questions or complaints about privacy matters concerning the website or to correct/update Personal Information already provided.

e. Each privacy notice is reviewed by the owner at least once every three years to ensure that it is current and accurate. Where required by law, Lydall ensures that Sensitive Personal Information is collected online only with an individual's explicit consent, via a meaningful opt-in approach, and is appropriately protected against improper use.

4. <u>Consent:</u>

a. Depending on the location in which the data subject lives, local laws may require that the data subject give specific consent for the collection, use and disclosure of Personal Information for some of the purposes described in Exhibit 1. Individuals who opt-in are notified of the process to follow in exercising this choice.

b. Where required, Lydall asks for consent by appropriate and permitted means. Lydall offers individuals the opportunity to opt-out of providing Personal Information if it is to be (1) disclosed to a Lydall agent, or (2) used for a purpose other than the purpose for which it was originally collected or subsequently authorized. Lydall may occasionally inform individuals of offers available from selected non-agent third parties. For Sensitive Personal Information, Lydall gives individuals the opportunity to affirmatively and explicitly opt-in prior to (1) disclosing the information to a non-agent third party, or (2)

using the information for a purpose other than the purpose for which it was originally collected or subsequently authorized. Lydall offers appropriate opportunities to opt-out when using Personal Information for direct marketing;

5. Access & Correction:

a. Lydall takes reasonable steps to ensure that Personal Information is relevant to its intended use, accurate, complete, and current.

b. As described in **Exhibit 2**, Lydall grants individuals reasonable access to their Personal Information. In addition, Lydall takes reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete. In addition, the data subject has the right to object to the data processing as well as the right to data portability. If explicit consent has been provided for the processing of data, then the data subject has the right to withdraw that consent at any time.

6. Data Security:

a. Lydall takes reasonable precautions to protect Personal Information in its possession from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. Lydall computer networks and systems, including Internet and Intranet-based applications, are designed to protect Personal Information from unauthorized access, loss, disclosure, or use. Personal Information is made available within Lydall only to those persons who possess a business need-to-know.

b. Lydall maintains systems and procedures to assure the security and integrity of Personal Information, whether provided by employees, generated by Lydall and its operating companies, or otherwise provided by agents or third parties. These measures include reasonable restrictions upon physical access to hard copy records containing Personal information and the storage of such records in locked facilities, storage areas, or containers.

c. The security program identifies and assesses reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any records containing Personal information, and evaluates and improves, where necessary, the effectiveness of the current safeguards for limiting such risks. The program includes:

- Ongoing employee (including temporary and contract employee) training;
- Means of ensuring employee compliance with security program policies and
- procedures;
- Means for detecting and preventing security program failures;
- Security policies for employees relating to the storage, access and transportation of
- records containing Personal information outside of business systems or premises;
- Disciplinary measures for violations of security program rules;
- Means of preventing terminated employees from accessing records;

- Regular monitoring to ensure that the security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Personal information, and upgrading information safeguards as necessary to limit risks;
- Annual reviews of the scope of security rules and more often when there is a material change in business practices that may reasonably implicate the security or integrity of Personal information;
- Documentation of responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Personal information; and
- Procedures for sanitization and destruction of storage or other media removed from service, prior to disposal.

d. Lydall periodically reevaluates these measures to ensure they remain current, reasonable, and appropriate.

e. Lydall does not transfer Personal Information from one country to another or from one legal entity to another unless properly supported by law and under appropriate security measures for the data while in transit and in storage;

f. Lydall ensures that handling of employees' and third parties' Personal Information is consistent with the relevant Privacy Notice for the information in question, subject to local supplement or amendment to ensure compliance with local law.

g. Lydall takes proper care of government-issued identification numbers by protecting the confidentiality, limiting collection, ensuring access on a need-to-know basis, implementing appropriate safeguards, including but not limited to encryption, and ensuring proper disposal in accordance with Lydall's document and data retention policies and practices;

7. Data Breaches:

A. Lydall maintains and implements a Data Breach response plan to respond to and remediate any actual data breaches, and discloses breaches involving Personal Information, as appropriate and as legally required.

8. Transfers of Personal Information To Third Parties:

a. Personal Information is used by and shared among Lydall entities, agents (e.g., IT and other professional and nonprofessional services, benefit plan sponsors and administrators, etc.). Lydall also discloses Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Lydall discloses Personal Information to applicable government organizations and agencies, and third parties as permitted or required by law, regulation,

or court order. Lydall shares Personal Information with companies Lydall acquires and transfers and to effect the divestiture of companies Lydall divests.

b. If services by a third party to Lydall involve access to Personal Information, third parties are selected and managed so that they are capable of maintaining appropriate security measures to protect such information, and are required by contract to implement and maintain appropriate security measures. Lydall enters into a written agreement obligating third parties that collect, process, access, or possess Personal Information on behalf of Lydall to follow this Policy or equivalent requirements. The written agreement uses the standard terms and conditions approved by the Senior Vice President, General Counsel and Chief Administration Officer. Lydall obtains assurances from the transferee(s) that they will safeguard Personal Information consistently with this Privacy Policy. Examples of appropriate assurances include: a contract, agreement, or relevant provision obligating the agent to provide at least the same level of protection as is required by the relevant Privacy Shield Principles; Privacy Shield certification by the agent; or being subject to an adequacy finding by the European Commission.

c. Lydall and its operating units execute and maintain the model clauses (also called the standard contractual clauses) adopted by the European Commission as an authorization for the transfer of Personal Information from the EEA to the U.S. Lydall and its operating units comply with the requirements of the model clauses for intra-company transfers. To authorize the transfer of Personal Information to third parties, Lydall and/or its operating units enter into the model clauses with a service provider. In the context of an onward transfer, Lydall has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. Lydall shall remain liable under the Privacy Shield Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

d. Where Lydall has knowledge that a transferee is using or disclosing Personal Information in a manner contrary to this Policy, Lydall takes reasonable steps to prevent or stop the use or disclosure, up to and including termination of our contractual or other business relationship with the agent.

8. Compliance with HIPAA:

a. Lydall operating units that are subject to the U.S. Health Insurance Portability and Accountability Act ("HIPAA"):

- Maintain reasonable measures to protect the privacy of Protected Health Information;

- Post on Lydall's external website(s) a notice of its privacy practices to the individuals whose Protected Health Information it collects;

- Enter into appropriate Business Associate Agreements with any third parties that handle Protected Health Information on behalf of Lydall; and

- Ensure proper and prompt notification of any Data Breaches.

9. Privacy Risk Assessment:

a. Lydall maintains an effective privacy risk assessment process to evaluate company-wide risks and to develop appropriate mitigation plans. The Privacy Risk Assessment process reviews Lydall's overall collection, processing (including storage and destruction), and transfer of Personal Information and is updated as needed.

b. Whenever Lydall or an operating unit seeks to implement a new or modified system, or use a new or modify the use of a third party to collect, process, or transfer Personal Information, a written Privacy Impact Assessment is completed before adoption of the new or modified process or new or modified use of the third party. A Privacy Impact Assessment must be completed only for systems or service providers that collect, process, or transfer Personal Information and for the launch of a new system or service provider or substantial modification of a system or use of the service provider involving Personal Information.

10. Governance & Training:

a. Lydall ensures that individuals who in any material way are involved in the collection, use, and storage of Personal Information, including designing, modifying, or managing automated systems, are trained to identify privacy concerns, to receive privacy complaints, and to forward both to the appropriate resources for review and resolution. In addition, each operating unit appoints at least one professional to serve as a resource for local management and staff in the operating unit with privacy-related issues. The structure of the Lydall privacy compliance organization and staff are managed, evaluated, and amended as needed from time-to-time by the Senior Vice President, General Counsel and Chief Administration Officer.

b. Lydall ensures that all professional staff and employees who handle Personal Information as an integral part of their responsibilities receive annual training on data privacy and security.
Education and training are provided to all employees on the proper use of the computer security systems and the importance of information security, e.g., limiting collection and storage of unneeded information; use of encryption; restricting access to drives, folders, and files; recognizing risks to information security posed by file sharing programs.

c. Lydall has a strategic communications plan to raise awareness and educate employees and third parties, as appropriate, regarding data privacy and security.

d. Lydall conducts assurance reviews in the form of periodic self-assessments and/or audits and has a hotline in place for the receipt of confidential reports of violations of this

Privacy Policy. This is to verify adherence to this Policy and to support annual Privacy Shield compliance certifications to the U.S. Department of Commerce. The Senior Vice President, General Counsel and Chief Administration Officer and the Vice President, Chief Accounting Officer & Treasurer administer assurance and audit programs to evaluate compliance with this Policy by staff organizations and operating units. Lydall's internal and external auditors periodically will audit the operating units and staff organizations to ensure compliance with this Policy.

e. Lydall enforces this Policy and any implementing procedures. Failure to adhere to this Policy or its implementing procedures may lead to disciplinary action for employees, up to and including dismissal, and termination of its contractual relationship with Lydall for third parties.

D. QUESTIONS & DISPUTES

1. Questions or concerns from persons regarding a particular website or system should be addressed to the contact listed in the privacy notice provided on that website or system.

2. Requests for access or correction from employees should be addressed to their local Human Resources representative.

3. Complaints or questions regarding compliance with this Policy should be addressed to Lydall's Senior Vice President, General Counsel and Chief Administration Officer.

4. Questions or comments regarding this Privacy Policy can be directed to:

- By mail addressed to:
- ydall, Inc., General Counsel, P. O. Box 151, Manchester, CT 06045-0151 USA
- Telephone: 1-800-454-7958
- Lydall's Workplace Alert Line, toll-free at 800-454-7958, or submitted electronically through a secure, encrypted internet connection at Workplace Alert Line.
- Information requested under the California "Shine the Light" law should be requested via email to privacy@lydall.com with "California Shine the Light Privacy Request" in the subject line as well as in the body of the message.

5. Privacy Shield Complaints:

a. In compliance with the Privacy Shield Principles related to transfers of Personal Information from the EEA to the U.S., Lydall commits to resolve complaints about our collection or use of such Personal Information.

- Lydall will investigate and attempt to resolve questions, complaints, and disputes in accordance with the principles contained in this Policy within 45 days of the receipt of an individual's initial contact with Lydall.
- For complaints that cannot be resolved by Lydall, Lydall provides, at no cost to the individual, independent recourse mechanisms by which each individual's complaints and disputes can be investigated and expeditiously resolved, as follows:

    - If the dispute concerns human resources data transferred to Lydall in the U.S. from the EU in the context of the individual's employment relationship with Lydall, the individual may contact the Data Protection Authority ("DPA") in their home country. Lydall will cooperate with and comply with the advice given by such DPA.
    - If the dispute concerns other than human resources data, Lydall has further committed to enable individuals to file complaints at no cost to them. An individual who decides to invoke this option must: (1) raise the claimed violation directly with Lydall and afford Lydall an opportunity to resolve the issue within 45 days; (2) contact the appropriate EU DPA; and (3) raise the issue through the DPA to the U.S. Department of Commerce and afford the Department an opportunity to use best efforts to resolve the issue within 90 days.
    - In the event the above mechanisms do not fully and finally resolve the dispute, Lydall commits to binding arbitration for any residual claims, upon the request of the individual data subject. This option is available to an individual to determine whether Lydall has violated its obligations under the Privacy Shield Principles as to that individual, and whether any such violation remains fully or partially unremedied. The scope and requirements of binding arbitration are described in Annex I to the Privacy Shield Principles.

E. CHANGES TO THIS POLICY

1. Lydall amends this Policy as needed to conform to the EU-US Privacy Shield Principles or to reflect accurately any changes in Lydall's practices and policies. Appropriate notice of amendments is provided.

Exhibit 1
Types of Personal Information Collected and Uses

The types of Personal Information Lydall collects and shares depend on the nature of the individual's relationship with Lydall (e.g., a director, employee, customer, supplier, other third party) and the provisions/restrictions of applicable laws. Examples of this information include:

- Management and employee communications and notices;
- Maintenance of employee biographies, curriculum vitae, and similar information;
- Emergency contacts;
- Global enterprise headcount and demographics;
- Career development, performance feedback, and progression;
- Staffing planning;
- Succession planning;
- Compensation and benefits;
- Establishment and administration of employee benefits and benefit plans;
- Rewards and recognition;
- Travel and expense reimbursement, including travel and/or credit card administration;
- Training;
- Relocation;
- Tax reporting and withholdings;
- Payroll administration, including deductions, contributions, etc.;
- Enterprise Resource Planning (ERP) systems;
- Industrial relations, including grievance proceedings;
- Planning and provision of health services, including drug screening, processing of workers' compensation or similar health and safety programs;
- Personal security, including access controls and security for computer and other systems;
- Reporting and statistical analyses;
- Personnel transactions, including tenure with the company, hire/start date of employment, termination date, and other transaction dates such as promotion, salary increase, etc.;
- Legal and regulatory reporting and other requirements, including right-to-work screening, workplace environment, health and safety reporting, and administration;
- Visas, licenses and other right-to-work authorizations;
- Management of litigation and related discovery/e-discovery issues;
- Import, export, and other trade compliance controls, including automated information technology controls;
- Sanctions screening, including screening of the U.S. Entity List, Specially Designated Nationals and Blocked Persons List, Denied Persons List, and the Unverified List, and similar lists maintained by the U.S. and other countries;
- Internal and external investigations, including management reviews and audits of the status of Lydall's compliance with laws and

regulations in all the places in which we do business; audits and reviews of the status of employee's compliance with laws, Lydall's Code of Ethics and Business Conduct and company policies; online and telephonic contacts with Lydall's reporting hotline (Compliance Line);
- Internet, intranet, e-mail, social media, and other electronic screening;
- Law enforcement and other government inquiries;
- Business planning, including prosecution of mergers, acquisitions, and divestitures, including acquisition of Personal Information from an acquired company and transfers of Personal Information to a divested company;
- Identification of persons via photographs or other likenesses, including facial recognition;
- Location tracking, duration, and other telematics of certain Lydall assets;
- Time collection and allocation;
- Data mining for internal company management purposes;
- Biometrics;
- Forensics analysis;
- Data supplied to vendors providing benefits;
- Physical and information technology security monitoring;
- Data backup and recovery; and
- Automated information technology threat assessments and response.
- Given and Family names, including suffixes;
- Middle name(s);
- Preferred name;
- Country of birth;
- Citizenships held (past and present);
- U.S. and other country permanent resident and/or asylee status;
- SMTP address;
- Place of work, including street mailing address and other pertinent contact information
- Home address and other pertinent contact information;
- Supervisor identifier;
- Job-related information such as title, department, job function, title, etc.
- Other data to support human resources applications;
- Management reports and data mining (usually anonymized and not containing individually identifying data);
- Computer asset location & billing data, including computer location;
- For third parties resident in Lydall business locations, identification of persons via photographs or other likenesses, including facial recognition; location tracking, duration, and other telematics; biometric data; forensics analysis; physical and information technology security monitoring; sanctions screening and automated information technology threat assessments and response.
- Time collection and allocation;
- E-mail message content (end-user controlled);
- Message attachments (end-user controlled);
- Public folder content (local administrator supplies folder permissions);
- Web page address;

- Instant Messaging address; and
- Calendar data (meeting and conference room information, including any-user-supplied attachments to calendar entries and meeting notices);
- Authorizing, granting, administering, monitoring and terminating access to or use of Lydall systems, facilities, records, property and infrastructure;
- Administration of customer and supplier contracts and agreements, joint ventures, and other business combinations;
- Support of marketing efforts;
- Budget planning and administration;
- Invoice processing and payment-related purposes;
- Training and certification of customer and supplier personnel;
- Data collected as part of job application and hiring processes;
- Background checks and sanctions screening;
- Problem resolution, internal investigations, auditing, compliance, risk management and security;
- Project management;
- Conflict of interest reporting;
- Company communications;
- On-site injury and illness evaluation and reporting, for those who access Lydall facilities;
- Monitoring and surveillance for industrial hygiene, public health and safety;
- Legal proceedings and government investigations, including preservation of relevant data; and
- As required or expressly authorized by laws or regulations applicable to our business globally or by government agencies that oversee our business globally;
- Personal data (e.g., date of birth, day or year of birth, citizenship(s), preferred language);
- Biographies, curriculum vitae, and similar information;
- Organizational and institutional affiliations;
- Professional credentials;
- Agreements, programs, and activities in which the data subject participates(d);
- Agreements entered into with Lydall;
- Payment-related information, including social security number or tax identification number and bank information;
- Communications preferences;
- Education and training;
- Industrial hygiene exposure assessment and monitoring information:
- Computer or facilities access and authentication information (e.g., identification codes, passwords, address lists, etc.);
- Photographs and other visual images of the data subject;
- Provide investor services;
- Provide the information, item, or service you have requested;
- Communicate with you about products, services, and events relating to Lydall;
- Improve our products, services, and websites;
- Evaluate your interest in and/or allow you to apply for employment with Lydall;
- Verify your identity to ensure security for one of the other purposes listed here;

- Ensure or enhance the security of Lydall's electronic systems;
- Protect against fraud;
- Screen against sanctions and antiterrorism lists as required by law;
- Respond to a legitimate legal request from law enforcement authorities or other government regulators;
- Investigate suspected or actual illegal activity;
- Prevent physical harm or financial loss; and
- Support the sale or transfer of all or a portion of our business or assets (including through bankruptcy).

Exhibit 2

Accessing & Correcting Personal Data

For Lydall employees and third parties who are subject to the European Union's General Data Protection Regulation, normally within one month (subject to certain exceptions) after receipt from you (or from a competent legal representative you designate), Lydall is committed to providing you with the following:

- Confirmation of whether, and where, Lydall is processing your personal data;
- Information about the purposes of the processing;
- Information about the categories of your data that are being processed;
- Information about the categories of recipients with whom the data may be shared;
- Information about the period for which the data will be stored (or the criteria used to determine that period);
- Information about your rights to erasure, to rectification, to restriction of processing and to object to processing;
- Information about your right to complain to the relevant EU data protection authority;
- Where the data were not collected directly from you, information as to the source of the data; and
- Information about the existence and an explanation of how automated processing is being used to process your data and/or make decisions regarding you or your data solely on the basis of automated processing.

You may request a copy of your personal data that are being processed. Copies will be provided in a structured, commonly used, machine-readable format that supports re-use. Upon reasonable request, Lydall will transfer your personal data from one data controller to another, store your personal data for further personal use on a private device, and/or have your personal data transmitted directly from Lydall to another controller without hindrance. This is not applicable to personal data you did not provide to Lydall directly, and Lydall is not obligated to retain your personal data for longer than is otherwise necessary.

Normally, Lydall does not charge any costs or fees for the above. However, as provided by law, we reserve the right to charge a reasonable fee for repetitive, excessive, or unfounded requests, and for additional copies.

Lydall takes all reasonable measures to ensure that inaccurate or incomplete personal data are erased or rectified. You have the right to inform Lydall of any discrepancies or inaccuracies and to rectification of inaccurate personal data.

You have the right to restrict the continued processing of your personal data if:

- You contest the accuracy of your data (and only for as long as it takes to verify and correct the accuracy of your data);

- The processing is unlawful and you request restriction (as opposed to exercising the right to erasure);
- Lydall no longer needs the data for its original purpose, but the data are still required by Lydall to establish, exercise or defend its legal rights; or
- If you have validly requested erasure or destruction of your data, but Lydall is evaluating other overriding grounds for retaining and processing your data.
- Lydall will erase or otherwise render inaccessible your personal data when:
- Your data are no longer needed for their original purpose (and no new lawful purpose exists);
- The legal basis for the processing is your consent, you withdraw that consent, and no other lawful ground exists;
- You exercise your right to object to Lydall's continued processing of your data and the company has no overriding grounds for continuing the processing;
- Your data have been processed unlawfully; or
- Erasure is necessary for compliance with EU law or the law of the relevant Member State of the EU to which you are subject.

Where Lydall has disclosed your personal data to any third parties, and you subsequently exercise any of the rights described above, Lydall will notify those third parties unless it is impossible or would require disproportionate effort. You may request the identity of those third parties. In exceptional cases where Lydall has made your data public, Lydall will take reasonable steps (taking costs into account) to inform relevant third parties.

Questions regarding implementation of these requirements should be addressed as described in elsewhere in this Policy.