

# LYDALL, INC. DATENSCHUTZRICHTLINIE

**GÜLTIG AB: Freitag, 1. Juni 2018**

---

A.

1. Lydall, Inc. und seine weltweiten Tochterunternehmen („Lydall“ oder „das Unternehmen“) befolgen diese Prinzipien bezüglich der Erfassung, Nutzung, Speicherung, Übertragung und schließlich Vernichtung von „persönlichen Informationen“ durch Lydall oder seine „Beauftragten“ (gemäß nachstehender Definition). Persönliche Informationen werden wie nachstehend beschrieben gehandhabt, um sicherzustellen, dass das Unternehmen rechtliche und vertragliche Vorschriften zur Erhebung, Übertragung und Nutzung persönlicher Informationen erfüllt. Diese Datenschutzrichtlinie gilt für Lydall und seine global agierenden Unternehmen. Lydall weitet die Anforderungen dieser Richtlinie auf Dritte aus, die auf persönliche Informationen zugreifen und/oder diese verarbeiten.

2. Für in der Europäischen Union („EU“) erhobene persönliche Informationen erfüllen diese Prinzipien die Anforderungen der EU-Datenschutz-Grundverordnung („DSGVO“), die ab Mai 2018 in Kraft tritt.

3. Lydall hält sich an das EU-U.S. Privacy Shield Framework („Privacy Shield“), wie es vom US-Handelsministerium in Bezug auf die Erfassung, Verwendung und Speicherung von personenbezogenen Daten, die von der EU in die Vereinigten Staaten übertragen werden, festgelegt wurde. Lydall hat dem Handelsministerium bescheinigt, dass es die „Privacy Shield Principles“ befolgt. Diese Bescheinigung umfasst Lydall und die unter der Lydall-Zertifizierung auf [www.privacyshield.gov/list](http://www.privacyshield.gov/list) aufgeführten Unternehmen. Im Falle von Widersprüchen zwischen den Bestimmungen dieser Datenschutzrichtlinie und den „Privacy Shield Principles“ haben die „Privacy Shield Principles“ Vorrang. Lydall unterliegt den Untersuchungs- und Durchsetzungsbefugnissen der Federal Trade Commission. Um mehr über das Privacy-Shield-Programm zu erfahren und unsere Zertifizierung anzusehen, besuchen Sie [www.privacyshield.gov/](http://www.privacyshield.gov/).

4. Gemäß den Gesetzen des Bundesstaats Kalifornien (USA) können Einwohner Kaliforniens mithilfe der in dieser Richtlinie angegebenen Kontaktinformationen Informationen anfordern und beziehen, die Lydall innerhalb des vergangenen Kalenderjahres mit anderen Unternehmen zu Direktvermarktungszwecken geteilt hat (nach Definition des kalifornischen „Shine the Light Law“).

5. Gemäß den Gesetzen des Bundesstaats Connecticut (USA) schützt Lydall die Vertraulichkeit von Sozialversicherungsnummern („SSNs“), verbietet deren unrechtmäßige Offenlegung und schränkt den Zugriff auf sie ein. Lydall gibt SSNs nicht vorsätzlich an die Öffentlichkeit, druckt SSNs nicht auf Dokumente, die zum Zugriff auf

Produkte oder Dienstleistungen erforderlich sind, erfordert keine Übertragung von SSNs über eine unverschlüsselte Internetverbindung und erfordert nicht die Nutzung von SSNs zum Zugriff auf eine Internet-Webseite, solange nicht auch ein Kennwort oder eine andere eindeutige Kennung erforderlich ist.

6. Lydall erfüllt die Anforderungen des U.S. Health Insurance Portability and Accountability Act („HIPAA“) insoweit es gemäß nachstehender Definition als „Covered Entity“ davon betroffen ist. HIPAA gilt nur für in den USA aktive Unternehmen.

## **B. BEGRIFFSBESTIMMUNGEN**

1. „Beauftragter“ bezieht sich auf jede Drittpartei, die persönliche Informationen kontrolliert oder verarbeitet, um Aufgaben im Auftrag von und unter Anweisung von Lydall auszuführen.

2. „Geschäftspartner“ ist ein Serviceanbieter für eine „Covered Entity“ im Rahmen von HIPAA.

3. „Covered Entity“ im Rahmen von HIPAA wird unter 45 C.F.R. § 160.103 definiert.

4. „Datenlecks“ sind Umstände, bei denen ein unbefugter Zugriff auf persönliche Informationen, deren Inbesitznahme bzw. der Verlust oder die Zerstörung von persönlichen Informationen tatsächlich erfolgt oder eine zumutbare Möglichkeit ist. Die Umstände, die zu einem Datenleck beitragen, können versehentlich oder zufällig sein und der Zugriff, Verlust oder die Zerstörung kann bestätigt oder nur vermutet werden. Persönliche Informationen können auf unterschiedliche Weise verloren gehen oder zerstört werden, etwa durch gestohlene Computerhardware (z. B. Laptops), physische Zerstörung oder Beeinträchtigung durch Naturkatastrophen oder Unfälle (z. B. Überflutung von Büros, Zerstörung der einzigen Datensatzkopie), sowie durch verhinderten Zugriff auf die einzige Datenkopie auf einem Server, falls eine Lösung des Problems nicht erwartet wird oder der Zugriff länger als eine Woche verhindert ist. Datenlecks können unbefugten Zugriff, Inbesitznahme oder Nichtverfügbarkeit eines Internetdienstes (Denial of Service/ DoS) bei einer Drittpartei oder einem Geschäftspartner umfassen.

5. „Persönliche Informationen“ sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, unabhängig vom Medium, in dem die Informationen erhoben, verarbeitet oder übertragen werden. Der Begriff umfasst auch sensible persönliche Informationen. Der Begriff umfasst Informationen zu einem Director, Mitarbeiter, Vertragsnehmer, Vertragsarbeiter, Kunden oder Zulieferer von Lydall oder einer anderen Drittpartei. Anonyme, aggregierte Informationen zu statistischen, historischen, wissenschaftlichen oder sonstigen Zwecken sind ausgenommen. Der Begriff umfasst Informationen, die in jeder Form erhoben, verarbeitet und/oder übertragen werden, u. a. als Papierversion, in elektronischer Form, als Video- oder als Audioaufzeichnung.

6. „Geschützte Gesundheitsinformationen“ („Protected Health Information“/ „PHI“) ist ein für HIPAA geltender Begriff, der sich auf alle individuell identifizierbaren Gesundheitsinformationen bezieht, die von einer „Covered Entity“ in jedweder Form, ob elektronisch, auf Papierbasis oder mündlich, gespeichert oder übertragen werden. „Individuell identifizierbare Gesundheitsinformationen“ sind Informationen, darunter auch demografische Daten, die sich auf den vergangenen, aktuellen oder zukünftigen körperlichen oder geistigen Zustand einer Person beziehen, auf seine gesundheitliche Versorgung oder auf die vergangene, aktuelle oder zukünftige Bezahlung der gesundheitlichen Versorgung, und die die Person identifizieren oder Grund zur Annahme geben, dass sie die Identifizierung der Person ermöglichen. Individuell identifizierbare Gesundheitsinformationen umfassen viele geläufige Identifikatoren (z. B. Name, Anschrift, Geburtsdatum, Sozialversicherungsnummer usw.).

7. „Sensible persönliche Informationen“ sind eine Untergruppe von persönlichen Informationen. Sie beziehen sich auf Informationen zu einer identifizierten oder identifizierbaren Person, die Aufschluss zu ihrer ethnischen Herkunft, zu politischen, religiösen oder philosophischen Ansichten, zur Mitgliedschaft bei einer Gewerkschaft, zur Gesundheit, zu Sexualpräferenz, zum Sexualleben oder zur Begehung oder angeblichen Begehung einer Straftat geben.

### C. DATENSCHUTZPRINZIPIEN

1. Einhaltung von Gesetzen und Vorschriften: Lydall hält die weltweit für seine Betriebe geltenden Gesetze und Vorschriften ein, die sich auf den Schutz von persönlichen Informationen beziehen. Örtliche Gesetze, Vorschriften und andere relevante Einschränkungen gelten im Falle etwaiger Konflikte mit dieser Richtlinie. Die Privacy-Shield-Prinzipien und die DSGVO haben im Falle von Konflikten mit der Richtlinie Vorrang.

#### 2. Erhebung, Verwendung und Beibehaltung persönlicher Informationen:

a. Lydall erhebt, verwendet und speichert persönliche Informationen nur soweit dies für legitime geschäftliche und rechtliche Zwecke erforderlich und angemessen ist. Damit wird sichergestellt, dass die Erhebung, Verarbeitung und Übertragung persönlicher Informationen adäquat, relevant und im Hinblick auf den entsprechenden Verwendungszweck nicht übermäßig umfangreich ist.

b. Die Erhebung und Verwendung von persönlichen Informationen von Directors, Mitarbeitern und Dritten durch Lydall umfasst auch die Erhebung und Verwendung persönlicher Informationen wie unter **Anhang 1** beschrieben. In einigen Fällen (etwa bei Personaldaten) sind die Daten nötig, damit Lydall Mitarbeiterbeziehungen und vertragliche Vereinbarungen bezüglich Entgelt und Sozialleistungen handhaben kann.

c. Lydall speichert persönliche Informationen nicht länger als für den Erhebungszweck erforderlich, solange nicht gesetzlich oder durch Einwilligung anders bestimmt.

### 3. Mitteilungen:

a. Wenn Lydall persönliche Informationen direkt von Personen erhebt, werden sie vom Unternehmen über die Zwecke informiert, für die persönliche Informationen von ihnen erhoben und verwendet werden, die Art von Beauftragten, gegenüber denen Lydall die Informationen offenlegt, sowie über die Entscheidungen und Mittel, die Lydall zur Einschränkung der Verwendung und Offenlegung anbietet. Lydall identifiziert die Zwecke, für die es persönliche Informationen erhebt und verarbeitet die persönlichen Informationen nicht zu ungeeigneten Zwecken, sofern keine Einwilligung der betroffenen Person vorliegt oder eine rechtliche Verpflichtung, eine physische Bedrohung oder ein anderes rechtlich anerkanntes Motiv.

b. Die Mitteilung erfolgt in deutlicher und sichtbarer Form, wenn Personen zum ersten Mal zur Bereitstellung der Informationen gebeten werden, oder so bald wie möglich nach der Erhebung; in jedem Fall aber vor der Nutzung der Informationen durch Lydall zu einem anderen Zweck als für den, für den sie ursprünglich erhoben wurden. Datenschutzmitteilungen müssen, soweit umsetzbar, für betroffene Personen zur Verfügung stehen und online veröffentlicht werden.

c. Lydall stellt angemessene Mitteilungen zum persönlichen Recht auf Zugriff, Korrektur und Aktualisierung bereit. Lydall stellt sicher, dass Personen die Gelegenheit haben, das Ergebnis einer automatischen Entscheidung (etwa Strafregisterprüfungen von Mitarbeitern) zu besprechen, bevor aufgrund solcher Entscheidungen eine negative Maßnahme durchgeführt wird.

d. Lydall sieht das Internet und andere Technologien als wertvolle Werkzeuge zur Kommunikation und Interaktion mit Mitarbeitern, Kunden, Geschäftspartnern und anderen an. Lydall ist sich der Bedeutung des Datenschutzes für online erhobene Informationen bewusst und hat spezielle Internet-Datenschutzrichtlinien für seine Webseiten erstellt, die die Behandlung von auf Lydall-Websites erhobenen persönlichen Informationen regeln. Hinsichtlich der aus dem Europäischen Wirtschaftsraum (EWR) übertragenen persönlichen Informationen gilt, dass jede Webseiten-Datenschutzrichtlinie dieser Datenschutzrichtlinie untersteht. Lydall stellt sicher, dass all seine Online-Websites (sowohl extern/www. wie auch intern/Intranet), die persönliche Informationen erheben, eine Datenschutzerklärung aufweisen. Die Datenschutzerklärung gibt an:

1. Persönliche Informationen, die erhoben werden;
2. Zweck(e), für die diese persönlichen Informationen erhoben werden;
3. Wie Lydall persönliche Informationen verwendet;
4. Die Nutzung von „Cookies“ oder anderen Tracking-Programmen durch externe Websites und, falls verwendet, wie der Browser auf die Ablehnung von Cookies konfiguriert werden kann;
5. Dritte, mit denen Lydall Informationen teilt;
6. Gegenüber Personen gebotene Entscheidungen, die Mittel zur Einschränkung der Erhebung, Nutzung und Offenlegung von Informationen und die Folgen solcher Entscheidungen; und
7. Wie Personen Lydall für Fragen oder Beschwerden zu Datenschutzangelegenheiten im Zusammenhang mit der Website kontaktieren oder wie sie bereits angegebene Informationen korrigieren/aktualisieren können.

e. Jede Datenschutzerklärung wird vom dafür verantwortlichen Besitzer mindestens einmal alle drei Jahre auf Genauigkeit und Aktualität überprüft. Sofern gesetzlich erforderlich, stellt Lydall sicher, dass sensible persönliche Informationen im Internet nur mit der ausdrücklichen Einwilligung einer Person über ein explizites Opt-in-Anmeldeverfahren erhoben und angemessen vor Missbrauch geschützt werden.

#### 4. Einwilligung:

a. Abhängig vom Wohnort der betroffenen Person können örtliche Gesetze eine ausdrückliche Einwilligung zur Erhebung, Verwendung und Offenlegung von persönlichen Informationen für die unter Anhang 1 beschriebenen Zwecke erfordern. Personen, die sich anmelden (Opt-in), werden über den zu befolgenden Prozess zur Durchführung dieser Entscheidung benachrichtigt.

b. Falls erforderlich, bittet Lydall über angemessene und gestattete Wege um Einwilligung. Lydall bietet Personen die Möglichkeit, die Angabe persönlicher Informationen zu verweigern (Opt-out), falls diese (1) gegenüber einem Lydall-Beauftragten offengelegt oder (2) zu einem anderen Zweck als dem ursprünglichen oder einem nachträglich genehmigten Erhebungszweck verwendet werden sollen. Lydall kann Personen gelegentlich über Angebote informieren, die bei ausgewählten, nicht beauftragten Dritten erhältlich sind. Bei sensiblen persönlichen Informationen gewährt Lydall Personen die Möglichkeit, vor (1) Offenlegung der Informationen gegenüber nicht beauftragten Dritten oder (2) Verwendung der Informationen zu einem anderen Zweck als dem ursprünglichen Erhebungszweck explizit einzuwilligen. Lydall bietet angemessene Möglichkeiten zur Verweigerung der Nutzung persönlicher Informationen zu Direktvermarktungszwecken.

## 5. Zugriff und Korrektur:

a. Lydall unternimmt angemessene Schritte, um sicherzustellen, dass persönliche Informationen für den beabsichtigten Zweck relevant, genau, vollständig und aktuell sind.

b. Wie in **Anhang 2** erläutert gewährt Lydall Personen angemessenen Zugang zu ihren persönlichen Informationen. Darüber hinaus unternimmt Lydall angemessene Schritte, um Personen die Korrektur, Ergänzung oder Löschung von nachweislich ungenauen oder unvollständigen Informationen zu ermöglichen. Darüber hinaus hat die betroffene Person das Recht, der Datenverarbeitung zu widersprechen sowie das Recht auf Datenübertragbarkeit. Falls für die Verarbeitung von Daten eine ausdrückliche Einwilligung erfolgt ist, hat die betroffene Person das Recht, diese Einwilligung jederzeit zurückzuziehen.

## 6. Datensicherheit:

a. Lydall unternimmt angemessene Vorsichtsmaßnahmen, um persönliche Informationen in seinem Besitz vor Verlust, Missbrauch, unbefugtem Zugriff, Offenlegung, Änderung oder Vernichtung zu schützen. Computernetzwerke und Systeme von Lydall, darunter Internet- und Intranet-basierte Anwendungen, sind darauf ausgelegt, persönliche Informationen vor unbefugtem Zugriff, Verlust, Offenlegung oder Verwendung zu schützen. Persönliche Informationen werden innerhalb Lydall nur denjenigen Personen zur Verfügung gestellt, die diese aus geschäftlichen Gründen kennen müssen.

b. Lydall betreibt Systeme und Verfahren, um die Sicherheit und Integrität persönlicher Informationen zu gewährleisten, unabhängig davon, ob diese von Mitarbeitern bereitgestellt, von Lydall und seinen Betreiberunternehmen erzeugt oder anderweitig von Beauftragten oder Dritten bereitgestellt wurden. Diese Maßnahmen umfassen angemessene Einschränkungen für den physischen Zugriff auf Papierakten mit persönlichen Informationen sowie die Lagerung solcher Daten in versperren Anlagen, Lagerbereichen oder Behältern.

c. Das Sicherheitsprogramm identifiziert und beurteilt vernünftigerweise vorhersehbare interne und externe Risiken für die Sicherheit, Vertraulichkeit und/oder Integrität von Unterlagen mit persönlichen Informationen. Es bewertet und verbessert falls erforderlich die Effektivität der aktuellen Schutzmaßnahmen zur Minderung solcher Risiken. Das Programm umfasst:

- Laufende Mitarbeiterschulungen (darunter auch für Zeitarbeits- und Vertragsangestellte);
- Sicherstellung der Einhaltung von Sicherheitsprogrammrichtlinien und -verfahren durch Mitarbeiter;
- Maßnahmen zur Erkennung und Verhinderung von Sicherheitsprogrammausfällen;

- Sicherheitsrichtlinien für Mitarbeiter bezüglich Lagerung, Zugriff auf und Transport von Daten mit persönlichen Informationen außerhalb der Geschäftssysteme oder -standorte;
- Disziplinarmaßnahmen für Verstöße gegen solche Sicherheitsprogrammregeln;
- Maßnahmen, um gekündigte Mitarbeiter am Zugriff auf Unterlagen zu hindern;
- Reguläre Überwachung, um sicherzustellen, dass das Sicherheitsprogramm in einer vernünftigerweise zu erwartenden Art betrieben wird, um den unbefugten Zugriff auf oder die unbefugte Nutzung von persönlichen Informationen zu verhindern, sowie ggf. Aufrüsten von Informationsschutzmaßnahmen zur Minderung von Risiken;
- Jährliche Überprüfung des Umfangs von Sicherheitsregeln und insbesondere dann, wenn eine wesentliche Änderung von Geschäftspraktiken erfolgt ist, welche sich auf die Sicherheit oder Integrität von persönlichen Informationen auswirkt;
- Dokumentierung von Maßnahmen, die in Verbindung mit Sicherheitszwischenfällen durchgeführt wurden, sowie verpflichtende anschließende Aufarbeitung von Zwischenfällen und ggf. durchgeführten Maßnahmen, um Geschäftspraktiken hinsichtlich des Schutzes von persönlichen Informationen zu ändern; und
- Verfahren zur Löschung und Vernichtung von Speicher- oder anderen außer Dienst gestellten Medien vor der Entsorgung.

d. Lydall bewertet diese Maßnahmen regelmäßig neu, um sicherzustellen, dass sie aktuell, vernünftig und angemessen sind.

e. Lydall überträgt persönliche Informationen aus einem Land in ein anderes oder von einem Rechtsträger zu einem anderen nur im gesetzlich zulässigen Rahmen und unter Nutzung angemessener Schutzmaßnahmen für die Daten auf dem Transportweg oder bei der Lagerung.

f. Lydall stellt sicher, dass der Umgang mit persönlichen Informationen durch Mitarbeiter und Dritte der relevanten Datenschutzerklärung für die betreffenden Informationen entspricht, die örtlich angepasst oder ergänzt werden kann, um die Einhaltung örtlicher Gesetze sicherzustellen.

g. Lydall gewährleistet eine ordentliche Handhabung behördlicher Identifikationsnummern, indem es die Vertraulichkeit schützt, die Erhebung einschränkt, den Zugriff auf Bedarfsbasis (Need-to-know) sicherstellt, angemessene Sicherheitsmaßnahmen implementiert (darunter u.a. Verschlüsselung) und eine angemessene Entsorgung gemäß der Dokument- und Datenhaltungsrichtlinien und -praktiken gewährleistet.

## 7. Datenlecks:

A. Lydall hält und implementiert einen Maßnahmenplan für Datenlecks, um auf tatsächliche Datenlecks zu reagieren und Schäden zu beheben. Es legt Datenlecks mit Auswirkungen auf persönliche Informationen gemäß gesetzlichen Vorgaben offen.

## 8. Übertragung persönlicher Informationen an Dritte:

a. Persönliche Informationen werden von Lydall-Unternehmen, Beauftragten (z. B. IT- und anderen professionellen und nicht professionellen Dienstleistern, Rententrägern und Verwaltern usw.). Lydall gibt persönliche Informationen auch bei rechtmäßigen Anfragen von Behörden weiter, unter anderem zur Erfüllung nationaler Sicherheits- oder Strafverfolgungsanforderungen. Lydall gibt persönliche Informationen an zuständige staatliche Organisationen und Behörden sowie an Dritte weiter, soweit dies durch Gesetze, Verordnungen oder Gerichtsbeschlüsse zulässig oder erforderlich ist. Lydall teilt persönliche Informationen mit Unternehmen, die Lydall übernimmt und überträgt, und im Rahmen der Desinvestition von Unternehmen, die Lydall veräußert.

b. Wenn bei Dienstleistungen, die Dritte für Lydall bereitstellen, auf persönliche Informationen zugegriffen wird, werden Dritte so ausgewählt und verwaltet, dass sie angemessene Sicherheitsmaßnahmen zum Schutz dieser Informationen vornehmen können und werden vertraglich zur Implementierung und Durchführung solcher Maßnahmen verpflichtet. Lydall geht eine schriftliche Vereinbarung mit Dritten ein, die im Auftrag von Lydall persönliche Informationen erheben, verarbeiten oder besitzen, und verpflichtet sie zur Befolgung dieser Richtlinie oder gleichwertiger Anforderungen. Die schriftliche Vereinbarung nutzt die üblichen Bestimmungen und Bedingungen, die von Senior Vice President, General Counsel und Chief Administration Officer genehmigt wurden. Lydall verlangt Zusicherungen von den Datenempfängern, dass diese persönliche Informationen im Einklang mit dieser Datenschutzrichtlinie schützen. Angemessene Zusicherungen umfassen: Verträge, Vereinbarungen oder relevante Bestimmungen, die den Beauftragten zu einem Maß an Schutz verpflichten, das mindestens den relevanten Privacy-Shield-Prinzipien entspricht; eine Privacy-Shield-Zertifizierung des Beauftragten; oder Bescheinigung eines angemessenen Schutzniveaus durch die Europäische Kommission.

c. Lydall und seine Betriebe erfüllen und pflegen die von der Europäischen Kommission beschlossenen Modellklauseln (auch Standardvertragsklauseln genannt) als Autorisierung für die Übertragung persönlicher Informationen aus dem EWR in die USA. Lydall und seine Betriebe erfüllen die Anforderungen der Modellklauseln für Übertragungen innerhalb des Unternehmens. Um die Übertragung persönlicher Informationen zu Dritten zu autorisieren, können Lydall und/oder seine Betriebe die Modellklauseln mit einem Dienstleistungsanbieter vertraglich vereinbaren. Bei einer Weiterleitung ist Lydall für die Verarbeitung der persönlichen Informationen verantwortlich, die es im Rahmen des Privacy Shield erhält und anschließend an einen Dritten weiterleitet, der in Lydalls Auftrag handelt. Lydall verbleibt im Rahmen der „Privacy Shield Principles“ haftbar, wenn sein Beauftragter solche persönlichen Informationen in einer Weise verarbeitet, die mit den Prinzipien nicht vereinbar ist, es sei denn, das Unternehmen weist nach, dass es nicht für das schadensverursachende Ereignis verantwortlich ist.

d. Erfährt Lydall davon, dass ein Datenempfänger persönliche Informationen entgegen diesen Richtlinien verwendet oder offenlegt, unternimmt Lydall angemessene Schritte, um die Verwendung oder Offenlegung zu verhindern oder aufzuhalten, bis hin

zur Auflösung unserer vertraglichen oder anderen Geschäftsbeziehungen mit dem Beauftragten.

8. Einhaltung von HIPAA:

a. Lydall-Betriebe, die dem U.S. Health Insurance Portability and Accountability Act ("HIPAA") unterliegen:

- führen angemessene Schritte durch, um die Sicherheit geschützter Gesundheitsinformationen sicherzustellen;
- veröffentlichen auf externen Lydall-Websites eine Erklärung der Datenschutzpraktiken für Personen, deren persönliche Gesundheitsinformationen erhoben werden;
- gehen geeignete Partnervereinbarungen mit Dritten ein, die im Auftrag von Lydall geschützte Gesundheitsinformationen verarbeiten und
- stellen eine angemessene und umgehende Benachrichtigung über Datenlecks sicher.

9. Datenschutzrisikobeurteilung:

a. Lydall nutzt einen wirkungsvollen Prozess zur Beurteilung des Datenschutzrisikos, um unternehmensweite Risiken zu bewerten und einen angemessenen Risikominderungsplan zu entwickeln. Der Datenschutzrisikobeurteilungsprozess überprüft die von Lydall eingesetzten Verfahren zur Erhebung, Verarbeitung (einschließlich Speicherung und Vernichtung) und Übertragung persönlicher Informationen und wird bei Bedarf aktualisiert.

b. Wenn Lydall oder einer seiner Betriebe den Einsatz eines neuen oder modifizierten Systems oder eine neue oder geänderte Nutzung einer Drittpartei zur Erhebung, Verarbeitung oder Übertragung persönlicher Informationen beabsichtigt, wird eine schriftliche Datenschutzfolgenabschätzung verfasst, bevor der neue oder geänderte Prozess oder die neue oder geänderte Nutzung einer Drittpartei übernommen wird. Eine Datenschutzfolgenabschätzung muss nur für Systeme oder Dienstleistungsanbieter durchgeführt werden, die persönliche Informationen erheben, verarbeiten oder übertragen, bei der Einführung eines neuen Systems oder Dienstleistungsanbieters, sowie bei einer maßgeblichen Änderung eines Systems oder Nutzung eines Dienstleistungsanbieters mit Auswirkung auf persönliche Informationen.

10. Leitung und Schulung:

a. Lydall stellt sicher, dass Personen, die maßgeblich an der Erhebung, Verwendung und Speicherung persönlicher Informationen beteiligt sind (darunter die Entwicklung, Modifikation oder Verwaltung automatischer Systeme), für die Identifikation von

Datenschutzbedenken und den Erhalt von Datenschutzbeschwerden geschult und dazu angewiesen werden, beide zur angemessenen Weiterbearbeitung an die richtigen Personen weiterzuleiten. Darüber hinaus ernennt jeder Betrieb mindestens einen Mitarbeiter als lokalen Ansprechpartner für Datenschutzangelegenheiten. Die Struktur von Organisation und Mitarbeitern für Datenschutzangelegenheiten bei Lydall wird von Senior Vice President, General Counsel und Chief Administration Officer verwaltet, bewertet und bei Bedarf von Zeit zu Zeit überarbeitet.

b. Lydall stellt sicher, dass alle Fachkräfte und Mitarbeiter, die im Rahmen ihrer wesentlichen Aufgaben persönliche Informationen handhaben, eine jährliche Schulung zu Datenschutz und Sicherheit durchführen.

Alle Mitarbeiter werden hinsichtlich der angemessenen Nutzung von Computer-Sicherheitssystemen und der Bedeutung der Informationssicherheit informiert und geschult, d. h. Einschränkung der Erhebung und Speicherung nicht benötigter Informationen; Verwendung von Verschlüsselung; Einschränkung des Zugangs zu Laufwerken, Ordnern und Dateien; Erkennen von Risiken für die Informationssicherheit durch Filesharing-Programme.

c. Lydall besitzt einen strategischen Kommunikationsplan, um Mitarbeiter und Dritte nach Ermessen auf Datenschutz und Sicherheit hinzuweisen und entsprechend zu schulen.

d. Lydall führt Prüfungen in Form regelmäßiger Selbsteinschätzungen und/oder Audits durch und besitzt eine Hotline für vertrauliche Meldungen über Verstöße gegen diese Datenschutzrichtlinie. Damit wird die Einhaltung dieser Richtlinie und die jährliche Privacy-Shield-Zertifizierung durch das US-amerikanische Handelsministerium sichergestellt. Senior Vice President, General Counsel, Chief Administration Officer sowie Vice President, Chief Accounting Officer und Treasurer führen Zusicherungs- und Audit-Programme durch, um die Einhaltung dieser Richtlinie durch Mitarbeiterorganisationen und Betriebe zu gewährleisten. Die internen und externen Prüfer von Lydall werden die Betriebe und Mitarbeiterorganisationen regelmäßig prüfen, um die Einhaltung dieser Richtlinie sicherzustellen.

e. Lydall setzt diese Richtlinie und die dafür zu implementierenden Verfahren durch. Die Nichteinhaltung dieser Richtlinie oder der dafür zu implementierenden Verfahren kann zu Disziplinarmaßnahmen für Mitarbeiter bis hin zur Entlassung führen sowie bei Dritten zur Kündigung des Vertragsverhältnisses.

#### **D. FRAGEN UND STREITFÄLLE**

1. Fragen oder Bedenken von Personen zu einer bestimmten Website oder einem System sollten an die in der Datenschutzerklärung aufgeführte Person gerichtet werden.

2. Zugriffs- oder Korrekturanfragen von Mitarbeitern sollten an die örtliche Personalabteilung gerichtet werden.

3. Beschwerden oder Fragen bezüglich der Einhaltung dieser Richtlinie sollten an den Senior Vice President, General Counsel und Chief Administration Officer von Lydall gerichtet werden.

4. Fragen oder Anmerkungen zu dieser Datenschutzrichtlinie können gerichtet werden an:

- Auf dem Postweg an: Lydall, Inc., General Counsel, P. O. Box 151, Manchester, CT 06045-0151 USA
- Telefon: 1-800-454-7958
- Die Workplace Alert Line von Lydall, gebührenfrei unter 800-454-7958, oder auf elektronischem Wege über eine sichere, verschlüsselte Internetverbindung auf Workplace Alert Line.
- Informationen, die im Rahmen des kalifornischen „Shine the Light“-Gesetzes angefordert werden, können bei [privacy@lydall.com](mailto:privacy@lydall.com) mit „California Shine the Light Privacy Request“ im Betreff und im Text erhalten werden.

5. Beschwerden zu Privacy Shield:

a. Im Rahmen der Privacy-Shield-Prinzipien für die Übertragung persönlicher Informationen aus dem EWR in die USA hat sich Lydall der Beilegung von Beschwerden zur Erhebung oder Nutzung persönlicher Informationen verpflichtet.

- Lydall untersucht Fragen, Beschwerden und Streitfälle in Einklang mit den Prinzipien dieser Richtlinie innerhalb von 45 Tage nach Erstkontakt einer Person mit Lydall und bemüht sich, eine Lösung zu finden.
- Bei Beschwerden, die nicht durch Lydall beigelegt werden können, bietet Lydall ohne weitere Kosten für die Person unabhängige Schiedsverfahren, mit denen diese Beschwerden und Streitfälle wie folgt untersucht und zügig beigelegt werden können:
  - Betrifft der Streitfall Personaldaten, die im Zusammenhang mit einem Beschäftigungsverhältnis mit Lydall aus der EU in die USA übertragen wurden, kann sich die Person an die Datenschutzbehörde in ihrem Heimatland wenden. Lydall kooperiert mit einer solchen Datenschutzbehörde und befolgt deren Empfehlungen.
  - Betrifft der Streitfall andere Angelegenheiten als Personaldaten, verpflichtet sich Lydall, das kostenfreie Einreichen von Beschwerden zu ermöglichen. Eine Person, die sich für diese Option entscheidet, muss: (1) den behaupteten Verstoß direkt an Lydall melden und Lydall die Möglichkeit geben, die Angelegenheit innerhalb von 45 Tagen zu klären; (2) die zuständige EU-Datenschutzbehörde kontaktieren; und (3) die Angelegenheit über die Datenschutzbehörde dem US-Handelsministerium melden und dem Ministerium die Möglichkeit geben, die Angelegenheit innerhalb von 90 Tagen nach bestem Bemühen beizulegen.
  - Falls die obigen Verfahren nicht zur endgültigen Klärung der Angelegenheit führen, verpflichtet sich Lydall auf Aufforderung der betroffenen Person zu

einem verbindlichen Schiedsverfahren zur Erledigung sämtlicher Restansprüche. Diese Option steht einer Person zur Verfügung, um festzustellen, ob Lydall seine Verpflichtungen im Rahmen der Privacy-Shield-Prinzipien gegenüber dieser Person verletzt hat, und ob dieser Verstoß gänzlich oder teilweise ungeahndet geblieben ist. Der Umfang und die Anforderungen verbindlicher Schiedsverfahren werden in Annex I der Privacy-Shield-Prinzipien beschrieben.

#### E. ÄNDERUNGEN AN DIESER RICHTLINIE

1. Lydall ändert diese Richtlinie bei Bedarf, um die Einhaltung der EU-US-Privacy-Shield-Prinzipien zu gewährleisten oder Änderungen in den Verfahren und Richtlinien von Lydall genau widerzuspiegeln. Änderungen werden entsprechend mitgeteilt.

## **Anhang 1**

### **Arten von erhobenen persönlichen Informationen und Verwendung**

Die Arten der persönlichen Informationen, die Lydall erhebt und teilt, hängen von der Art der Beziehung der Person zu Lydall ab (z. B. Director, Angestellter, Kunde, Zulieferer, sonstiger Dritter) sowie von den Bestimmungen/Einschränkungen geltender Gesetze. Beispiele dieser Informationen sind:

- Mitteilungen und Bekanntmachungen für Vorstand und Mitarbeiter;
- Verwaltung von Angestelltenbiografien, Lebensläufen und ähnlichen Informationen;
- Notfallkontakte;
- Globale Unternehmens-Mitarbeiterzahlen und demographische Daten;
- Karriereentwicklung, Leistungs-Feedback und Fortschritte;
- Personalplanung;
- Nachfolgeplanung;
- Vergütung und Sachleistungen;
- Aufstellung und Verwaltung von Mitarbeiterleistungen und Leistungsplänen;
- Prämien und Anerkennung;
- Reise- und Kostenrückerstattung, darunter Verwaltung von Reisen und/oder Kreditkarten;
- Schulungen;
- Versetzungen;
- Steuererklärung und Steuerabzüge;
- Lohnabrechnung, darunter Abzüge, Beiträge usw.;
- Enterprise-Resource-Planning-Systeme (ERP);
- Arbeitsbeziehungen darunter Beschwerdeverfahren;
- Planung und Bereitstellung von Gesundheitsleistungen, darunter Drogentests, Arbeitsunfallversicherung und ähnliche Arbeitsschutzprogramme;
- Persönliche Sicherheit, darunter Zugriffskontrollen und Sicherheit für Computer und andere Systeme;
- Berichte und statistische Analysen;
- Personaltransaktionen, darunter Beschäftigungsdauer im Unternehmen, Einstellungsdatum, Kündigungsdatum und andere Transaktionsdaten wie Beförderung, Gehaltserhöhung usw.;
- Gesetzliche und aufsichtsbehördliche Meldevorschriften und andere Anforderungen, darunter Arbeitserlaubnis-Screenings (Right-to-Work Screenings), Arbeitsumfeld, Arbeitsschutzberichte und Verwaltung;
- Visa, Lizenzen und Arbeitserlaubnisse (Right-to-Work Authorization);
- Verwaltung von Rechtsstreitigkeiten und damit zusammenhängenden Offenlegungs-/e-Discovery-Angelegenheiten;
- Import-, Export- und andere Trade-Compliance-Kontrollen, darunter automatisierte IT-Kontrollen;

- Sanktionsprüfungen, darunter Prüfung der U.S. Entity List., Specially Designated Nationals and Blocked Persons List, Denied Persons List und der Unverified List sowie ähnlicher Listen, die in den USA und anderen Ländern geführt werden;
- Interne und externe Untersuchungen, darunter Managementbewertungen und Audits der Compliance von Lydall hinsichtlich Gesetzen und Vorschriften an allen relevanten Geschäftsstandorten; Audits und Prüfungen der Einhaltung von Gesetzen, des Lydall Code of Ethics and Business Conduct und von Unternehmensrichtlinien durch Mitarbeiter; Online- und Telefonkontakte bei der Compliance Line (Melde-Hotline) von Lydall;
- Screening von Internet, Intranet, E-Mail, Sozialen Medien und anderen elektronischen Medien;
- Anfragen von Strafverfolgungs- und anderen staatlichen Behörden;
- Geschäftsplanung, darunter Verfolgung von Fusionen, Übernahmen und Veräußerungen, darunter die Übernahme persönlicher Informationen von einem übernommenen Unternehmen und die Übertragung persönlicher Informationen zu einem veräußerten Unternehmen;
- Identifikation von Personen über Fotos oder andere Abbildungen, darunter Gesichtserkennung;
- Verfolgung von Standort, Dauer und anderen Telematikdaten bestimmter Lydall-Anlagen;
- Zeiterfassung und -zuweisung;
- Daten-Mining zu internen Managementzwecken;
- Biometrie;
- Forensische Analyse;
- Daten, die Leistungsanbietern zur Verfügung gestellt werden;
- Mechanische und IT-basierte Sicherheitsüberwachung;
- Datensicherung und -wiederherstellung;
- Automatisierte IT-Bedrohungsbeurteilungen und Gegenmaßnahmen.
- Vor- und Nachnamen, einschließlich Namenszusätze;
- Zweite Vornamen;
- Bevorzugter Name;
- Geburtsland;
- Staatsangehörigkeit(en) (früher und gegenwärtig);
- Dauerhafte Aufenthaltserlaubnis und/oder Asylstatus in den USA und in anderen Ländern;
- SMTP-Adresse;
- Arbeitsplatz, darunter Postanschrift und andere relevante Kontaktinformationen;
- Privatanschrift und andere relevante Kontaktinformationen;
- Vorgesetztenkennung;
- Arbeitsbezogene Informationen wie Stellenbezeichnung, Abteilung, Funktion usw.;
- Andere Daten zur Unterstützung der Personalverwaltung;
- Geschäftsberichte und Datenmining (in der Regel anonymisiert und ohne persönlich identifizierende Daten);
- Standort von Computeranlagen und Rechnungsdaten, darunter Computerstandorte;

- Bei Drittparteien, die an Lydall-Geschäftsstandorten tätig sind: Identifikation von Personen über Fotos oder andere Abbildungen, darunter Gesichtserkennung; Verfolgung von Standort, Dauer und anderen Telematikdaten; biometrische Daten; forensische Analyse; mechanische und IT-Sicherheitsüberwachung; Sanktionsüberprüfung und automatisierte IT-Bedrohungsbewertungen und Gegenmaßnahmen.
- Zeiterfassung und -zuweisung;
- Inhalt von E-Mail-Nachrichten (endnutzerkontrolliert);
- Nachrichtenanhänge (endnutzerkontrolliert);
- Inhalte öffentlicher Ordner (lokaler Administrator gewährt Ordnerberechtigungen);
- Webseitenadresse;
- Instant-Messaging-Adresse;
- Kalenderdaten (Meeting- und Konferenzrauminformationen, einschließlich von Benutzern hinzugefügte Anhänge für Kalendereinträge und Meeting-Termine);
- Autorisierung, Gewährung, Verwaltung, Überwachung und Aufkündigung des Zugriffs auf oder die Verwendung von Systemen, Anlagen, Unterlagen, Eigentum und Infrastruktur von Lydall;
- Verwaltung von Kunden- und Zuliefererverträgen und -vereinbarungen, Joint Ventures und anderen Unternehmenszusammenschlüssen;
- Unterstützung von Vermarktungsarbeit;
- Budgetplanung und -verwaltung;
- Rechnungsverarbeitung und zahlungsbezogene Zwecke;
- Schulung und Zertifizierung von Kunden- oder Zuliefererpersonal;
- Daten, die im Rahmen von Einstellungsverfahren erhoben werden;
- Strafregisterprüfungen und Sanktions-Screenings;
- Problemlösung, interne Untersuchungen, Audits, Compliance, Risikomanagement und Sicherheit;
- Projektmanagement;
- Meldung von Interessenkonflikten;
- Unternehmensmitteilungen;
- Bewertung und Meldung von Verletzungen und Krankheit am Arbeitsplatz für Personen mit Zugang zu Lydall-Anlagen;
- Kontrolle und Überwachung von Arbeitshygiene, öffentlicher Gesundheit und Sicherheit;
- Gerichtsverfahren und behördliche Untersuchungen, darunter Speicherung relevanter Daten; und
- wie durch Gesetze oder Vorschriften, die global für unser Unternehmen gelten, oder von staatlichen Aufsichtsbehörden gefordert oder ausdrücklich autorisiert;
- Persönliche Daten (z. B. Geburtsdatum, Geburtstag oder -jahr, Staatsangehörigkeit(en), bevorzugte Sprache);
- Biografien, Lebensläufe und ähnliche Informationen;
- Organisations- oder Institutionszugehörigkeiten;
- Berufliche Qualifikationen;
- Vereinbarungen, Programme und Aktivitäten, an denen die

- betroffene Person teilnimmt oder teilgenommen hat;
- Mit Lydall eingegangene Vereinbarungen;
- Zahlungsbezogene Informationen, darunter Sozialversicherungsnummer, Steuernummer und Bankinformationen;
- Bevorzugte Kommunikationswege;
- Bildung und Schulung;
- Bewertungs- und Überwachungsinformationen zur Arbeitshygiene;
- Zugang zu Computern/Anlagen und Authentifizierungsinformationen (ID-Codes, Kennwörter, Adressenlisten usw.);
- Fotos und andere visuelle Abbildungen der betroffenen Person;
- Bereitstellung von Investor Services;
- Bereitstellung der angeforderten Informationen, Artikel oder Dienstleistungen;
- Mitteilungen an Sie zu Produkten, Dienstleistungen und Veranstaltungen im Bezug auf Lydall;
- Verbesserung unserer Produkte, Dienstleistungen und Websites;
- Bewertung Ihres Interesses an Lydall und/oder Ermöglichung Ihrer Bewerbung bei Lydall;
- Verifizieren Ihrer Identität aus Sicherheitsgründen zu einem der anderen hier aufgeführten Zwecke;
- Sicherstellen oder Verbessern der Sicherheit der elektronischen Systeme von Lydall;
- Schutz vor Betrug;
- Abgleich mit Sanktions- und Antiterrorismus-Listen im gesetzlichen Rahmen;
- Antwort auf Anfragen von Strafverfolgungs- oder anderen Aufsichtsbehörden;
- Untersuchung vermuteter oder tatsächlicher illegaler Aktivitäten;
- Verhinderung von körperlichen Schäden oder finanziellen Verlusten;
- Unterstützung des Verkaufs oder der Übertragung eines Teils oder aller unserer Geschäfte oder Anlagen (darunter durch Insolvenz).

## **Anhang 2**

### **Zugriff auf und Korrektur persönlicher Daten**

Lydall ist verpflichtet, bei Mitarbeitern von Lydall und Dritten, die der Datenschutz-Grundverordnung der EU unterliegen, in der Regel innerhalb eines Monats (mit bestimmten Ausnahmen) nach Erhalt einer diesbezüglichen Anforderung von Ihnen (oder einem von Ihnen bestimmten zuständigen gesetzlichen Vertreter) Folgendes bereitzustellen:

- Bestätigung, ob und wo Lydall Ihre persönlichen Daten verarbeitet;
- Informationen über den Zweck der Verarbeitung;
- Informationen über die verarbeiteten Datenkategorien;
- Informationen über die Kategorien von Empfängern, mit denen die Daten ggf. geteilt werden;
- Informationen über den Zeitraum, für den die Daten gespeichert werden (oder die Kriterien, mit denen dieser Zeitraum bestimmt wird);
- Informationen über Ihr Recht auf Löschung, Berichtigung oder Einschränkung der Verarbeitung und Widerspruch gegen die Verarbeitung;
- Informationen über Ihr Recht, Beschwerde bei der relevanten EU-Datenschutzbehörde einzureichen;
- Falls Daten nicht direkt von Ihnen erhoben wurden, Informationen zur Quelle der Daten; und
- Informationen über das Vorhandensein von automatischer Verarbeitung und eine Erklärung dazu, wie Ihre Daten mittels automatischer Verarbeitung verarbeitet werden und/oder wie Entscheidungen zu Ihnen oder Ihren Daten ausschließlich auf der Basis von automatischer Verarbeitung getroffen werden.

Sie können eine Kopie der persönlichen Daten anfordern, die verarbeitet werden. Kopien werden in einem strukturierten, gebräuchlichen und maschinenlesbaren Format bereitgestellt, das wiederverwendbar ist. Bei zumutbarer Anfrage wird Lydall Ihre persönlichen Daten von einem Datenverantwortlichen zu einem anderen übertragen, Ihre persönlichen Daten zur weiteren persönlichen Verwendung auf einem privaten Gerät speichern und/oder Ihre persönlichen Daten ohne Behinderung direkt von Lydall zu einem anderen Datenverantwortlichen übertragen lassen. Dies gilt nicht für persönliche Daten, die Sie Lydall nicht direkt zur Verfügung gestellt haben, und Lydall ist nicht verpflichtet, Ihre persönlichen Daten länger als nötig aufzubewahren.

In der Regel erhebt Lydall für derartige Anfragen keine Gebühren. Im gesetzlichen Rahmen behalten wir uns jedoch das Recht vor, eine angemessene Gebühr für wiederholte, übermäßige oder unbegründete Anfragen sowie für zusätzliche Kopien zu erheben.

Lydall unternimmt alle angemessenen Schritte, um sicherzustellen, dass ungenaue oder unvollständige persönliche Daten gelöscht oder berichtigt werden. Sie haben das Recht,

Lydall über Abweichungen oder Ungenauigkeiten zu informieren und ungenaue persönliche Daten zu berichtigen.

Sie haben das Recht, die weitere Verarbeitung Ihrer persönlichen Daten zu begrenzen, falls:

- Sie die Richtigkeit Ihrer Daten bestreiten (und nur so lange, wie für die Bestätigung und Korrektur der Richtigkeit Ihrer Daten erforderlich);
- die Verarbeitung unrechtmäßig ist und Sie eine Beschränkung anfordern (im Gegensatz zum Recht auf Löschung);
- Lydall die Daten nicht mehr zum ursprünglichen Zweck benötigt, diese jedoch weiterhin zur Wahrung, Ausübung oder Verteidigung der Rechte Lydalls erforderlich sind; oder
- Sie die Löschung oder Vernichtung Ihrer Daten ordnungsgemäß angefordert haben, aber Lydall andere vorrangige Gründe für die Beibehaltung und Verarbeitung Ihrer Daten untersucht.
- Lydall löscht Ihre persönliche Daten oder macht sie anderweitig unzugänglich, wenn:
  - Ihre Daten nicht mehr für ihren ursprünglichen Zweck gebraucht werden (und kein neuer rechtmäßiger Zweck besteht);
  - die rechtliche Basis für die Verarbeitung Ihre Einwilligung ist, Sie diese Einwilligung zurückziehen und kein weiterer rechtmäßiger Grund besteht;
  - Sie Ihr Recht ausüben, der weiteren Verarbeitung Ihrer Daten durch Lydall zu widersprechen und das Unternehmen keine vorrangigen Gründe für die weitere Verarbeitung hat;
  - Ihre Daten unrechtmäßig verarbeitet wurden; oder
  - die Löschung für die Einhaltung von EU-Gesetzen oder die Gesetze des relevanten EU-Mitgliedslandes, denen Sie unterliegen, notwendig ist.

Wenn Lydall Ihre persönlichen Daten gegenüber Dritten offengelegt hat und Sie eines der obigen Rechte ausüben, benachrichtigt Lydall diese Dritten, soweit dies nicht unmöglich ist oder unverhältnismäßigen Aufwand erfordert. Sie sind berechtigt, die Identität dieser Dritten anzufordern. In Ausnahmefällen, in denen Lydall Ihre Daten veröffentlicht hat, unternimmt Lydall angemessene Schritte (unter Beachtung der Kosten), um relevante Dritte zu informieren.

Fragen zur Umsetzung dieser Anforderungen sollten gemäß der Beschreibung an anderer Stelle in dieser Richtlinie eingesandt werden.