Robinson+Cole

COMPLIANCE STRATEGIES FOR EVOLVING DATA PRIVACY LAWS

Moderated Peer Discussion

BENJAMIN JENSEN – ROBINSON+COLE
WILLIAM PIOTROWSKI – LYDALL
NOELLE SLIFKA – SLIFKA LAW
JULIE WADE – BARNES GROUP

Please Note

The presentations and discussions today are designed to provide accurate information about the subject matter. However, it only provides general information and does not constitute legal advice. No attorney-client relationship has been created. If legal advice or other assistance is required, let us know directly.

Preliminary Considerations

- This platform should not be used for activities prohibited by antitrust law.
- Avoid discussions leading to a restriction, or coordination, of competition between or among attendees.
- Attendees should not share information, have discussions, and/or make arrangements on, among other things, pricing, market conduct, terms of sale, individual manufacturing costs and costs of sale, output, or supplier or customer relations/allocation.

Agenda

- Overview of data privacy landscape
  - United States
  - Europe
  - Trend toward European model
  - Department of Defense Cybersecurity Regulation (DFARS)
- In-house perspective on compliance
  - Designing and implementing a compliance program
  - Contractual protections – third party and inter-company
  - Data security incident response/disclosures
- Open discussion

Data Privacy in the United States

- Patchwork of federal and state laws
  - Federal: focused on specific industries / categories of data
    - Financial services – Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801–6809)
    - Healthcare – Health Information Portability and Accountability Act (42 U.S.C. § 1320d)
    - Credit information – Fair Credit Reporting Act (15 U.S.C. § 1681)
    - Information about minors – Children's Online Privacy Protection Act (15 U.S.C. §§ 6501–6506)
  - State: focused on security of consumer information
    - Obligation to protect information from unauthorized access
    - Data breach notification procedures

Data Privacy in Europe

- EU approach: data protection is a fundamental right of individuals
- E.U. General Data Protection Regulation 2016/679 (GDPR), effective May 25, 2018
- Applies to all EEA Member States (E.U. plus Iceland, Liechtenstein & Norway)
- Potential Brexit implications for application in UK
- Extraterritorial application
  - Establishment in Europe?
  - Marketing goods and services to Europe?
  - Monitoring behavior of data subjects in Europe?

GDPR Key Concepts

- Individual rights to control over personal data
  - Right of access
  - Right to withdraw consent
  - Right of erasure / to be forgotten
- Broad definition of “Personal Data”
  - Information relating to an identified or identifiable natural person
  - Name, photo, email, social media posts, IP address, etc.
- Must have a lawful basis to process personal data
  - High standard for consent
  - Every processing activity requires its own lawful basis
- Third-party processors must comply
- Penalties
  - Maximum fines up to 20 million Euros or 4% of global annual turnover

U.S. Trend Toward European Model

- California Consumer Privacy Act (Cal. Civ. Code § 1798.100 – 1798.199)
- Effective January 1, 2020 (with 12 month lookback)
- Applies to companies doing business in California that collect consumer personal information and that meet 1 of 3 criteria:
  - At least $25 million in annual revenue
  - Buy, sell, or share personal information on at least 50,000 California consumers;
  - Derive more than half of annual revenue from sale of personal information

CCPA Key Concepts

- Broad definition of personal information (PI)
- Disclosure requirements
  - Automatic disclosure of practices concerning PI at, or before, collection
  - Disclosure on consumer request of categories of data collected, sources of data, and sales or disclosures to third parties
- Consumer rights
  - Request deletion of PI
  - Opt out of sale of PI
  - Non-discrimination (business may not charge consumers for exercising rights or charge different rates to consumers who opt-out)
- Private right of action for data breaches

International Trend Toward European Model

- Brazil: General Data Privacy Law (LGPD)
- Japan: amendments to Act on the Protection of Personal Information
- Driver of international trend: adequacy determinations
  - Facilitates cross-border data transfers
  - Personal data can flow from EU to that third country without additional safeguards
  - Countries recognized to date:
    - Argentina, Canada, Israel, New Zealand, Switzerland, Uruguay and USA (limited to the Privacy Shield framework)
    - Japan is currently applying for adequacy determination
- Without an adequacy determination, cross-border data transfers may require contractual agreement

Department of Defense Cybersecurity Regulation

- DFARS: Safeguarding Covered Defense Information and Cyber Incident Reporting (48 CFR § 252.204-7012)
- Adequate security on all covered contractor information systems
  - Contractor IT systems used to process, store or transmit information subject to safeguarding or dissemination controls under federal law, regulation or policy
    - Export-controlled information
  - Follow 110 security requirements of NIST SP 800-171
  - Create and maintain written system security plan (SSP)
  - Additional requirements if supplying an IT system or cloud computing for government use, or using external cloud for storing covered information

Department of Defense Cybersecurity Regulation

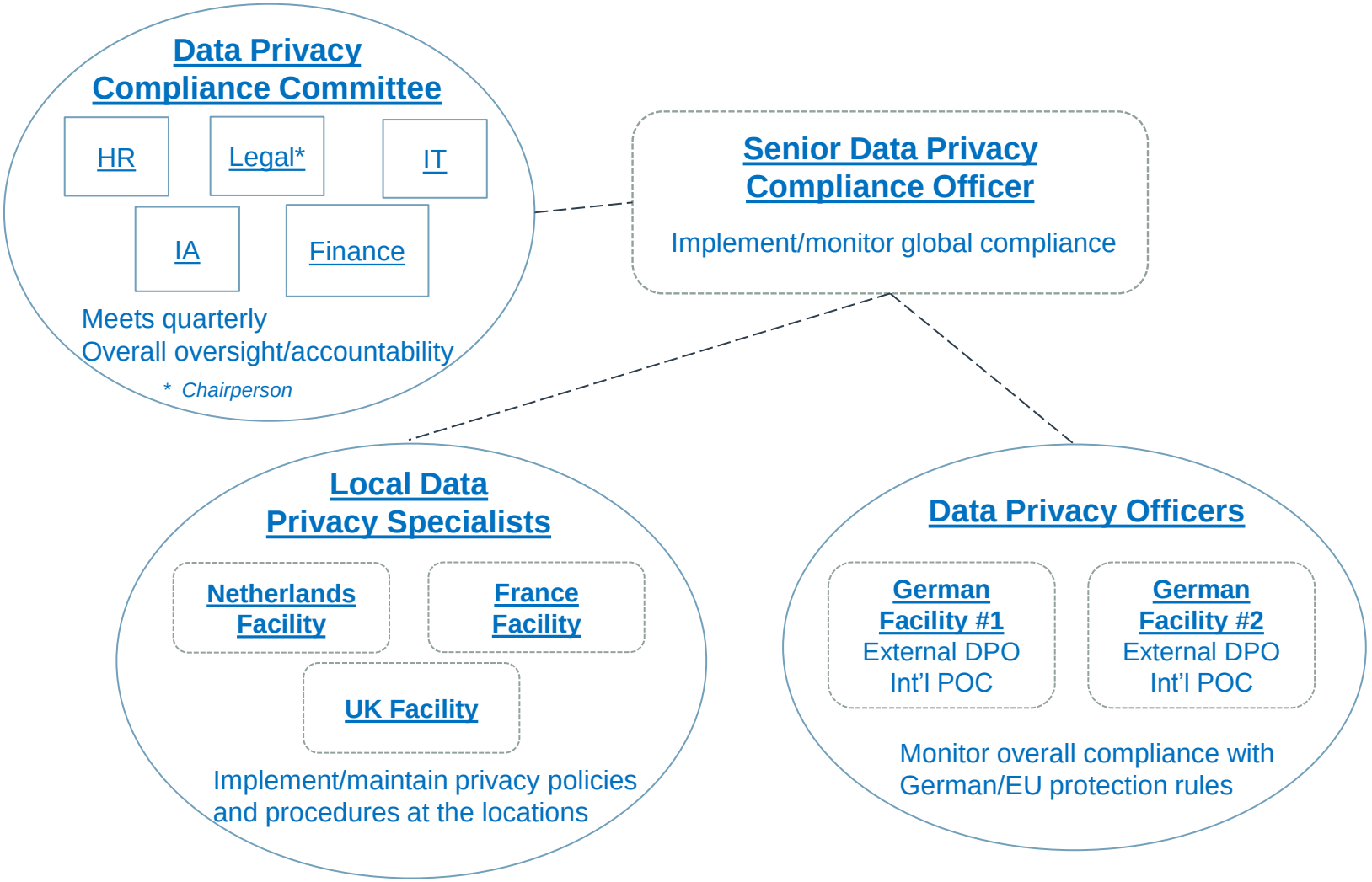
- Report cyber incidents to DoD within 72 hours of discovery
  - Cyber incident: information disclosure to unauthorized persons or violation of security policy resulting in intentional or unintentional disclosure, modification, destruction or loss of information
- Clause applies to almost all DoD prime contracts, plus subcontracts involving covered information
- DoD will review prime contractor's oversight of subcontractors during purchasing system audits
- Expect demands for compliance certification, copy of SSP, possibly future audits/testing

Privacy Program Design and Implementation

Key Program Elements:

- Establish formal governance structure
- Complete personal data inventories
- Publish Data Privacy policies and notices
- Embed Data Privacy protections into operational processes
- Implement a training and awareness program
- Manage information security risk
- Manage third-party risk
- Establish procedure for inquiries and complaints
- Monitor for new operational best practices and legal developments
- Establish Data Privacy breach management program

GOVERNANCE STRUCTURE EXAMPLE: LYDALL



GDPR Project Phases

Project Launch & Team Established

Outside Consultant Engaged

Prepared surveys / standard inventory form data collection

Surveyed all sites/processes

Identified gaps

Created remediation plans

Established/ updated Governance documents, policies, notices, 3rd party contracts

Identify DPOs & EU-based Team Members

Launch Privacy Governance Structure

Sign the model clauses/ agreements with 3rd party & Lydall entities

EU-US Privacy Shield filing

W/C Consults

Program Cadence

Create privacy audit Process

Implement remediation plan at the EU locations

Support on-going GDPR Privacy compliance

Employee Training

Privacy Impact Assessments

Privacy Audit in-place

Phase I

Phase II

Phase III

GDPR Prep Key Activities Example: Barnes

Data Mapping & Legal Basis

✓EU-U.S. Privacy Shield Certified

✓High-Level Data Mapping to Identify Data Ingress and Egress

✓Creation of Record of Processing Activities
- HR info systems and platforms
- Non-HR info systems and platforms
- Annual Process for Review and Update

✓Finalize Data Export Contracts
- Standard Contractual Clauses
- Global DTA – ongoing

Process & Training

✓ Create Standard Data Protection Clause for 3rd Party Processors

✓ Develop Data Protection Due Diligence Questionnaire

✓ Deploy/train on standard tools and process – partner with IT on cyber/privacy diligence process

✓ Training Program
- GDPR for HR: 4/25
- GDPR for Leadership: 4/27
- GDPR for IT: 5/1
- Privacy: General Awareness: 5/2
- Annually Deployed through LMS System and Targeted by Employee Function: Platform and Modules Selected for remainder 2018

✓ Breach Notification Response Plan

✓ Data Subject Access and Portability

Policies

✓ Policy 207 Updated

✓ Internal Privacy Notices
- Update Internally Facing Privacy Notices
- Update Templates for European Employment Agreements

✓ External Privacy Notices
- Harmonize Cookie and Privacy Notices
- Develop Customer Privacy Statement

Framework & Governance

✓ Establish relationship with German DPO

✓ Accountability Assessment Report – 5/25 and annual

✓ Adopt Internal Privacy Framework Model for Ongoing Compliance

✓ Identify EU Privacy Points of Contact

✓ New Data Privacy SharePoint Site containing:
- Record of Processing Activities
- Privacy Notices and Procedures
- Privacy Training

DATA PRIVACY – GDPR COMPLIANCE

Transferring Personal Data

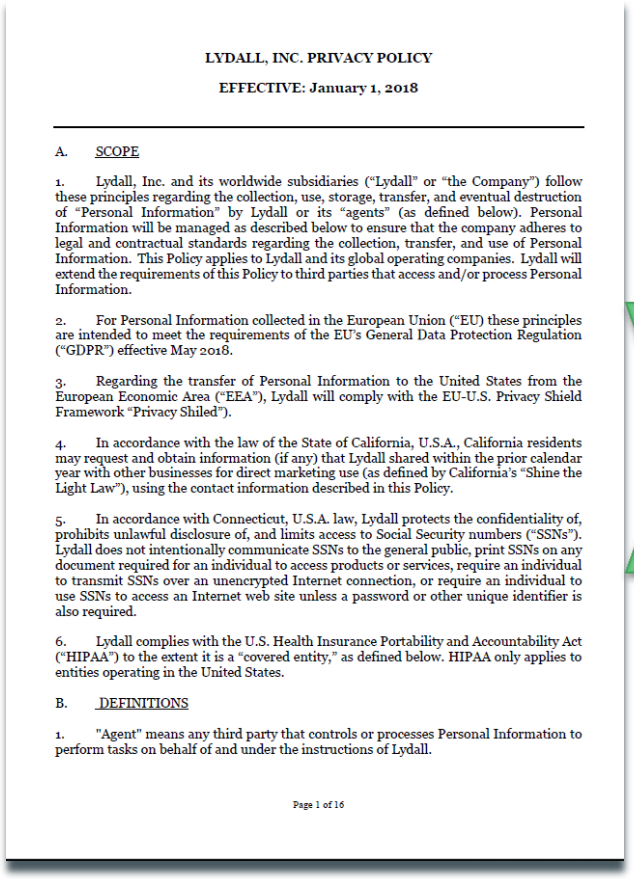
Options to comply when transferring personal data to a third party

- The third party must:
  - Subscribe to Safe Harbor Principles; or
  - Be subject to GDPR; i.e., located in the European Union (EU); or
  - Be located in a place recognized by the EU as providing an adequate level of privacy protection (e.g., Canada);

OR

- The parties can enter a written agreement requiring the third party to provide at least the same level of protections required by GDPR; frequently, the “model clauses”

Contractual Controls



LYDALL, INC. PRIVACY POLICY

EFFECTIVE: January 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. Regarding the transfer of Personal Information to the United States from the European Economic Area ("EEA"), Lydall will comply with the EU-U.S. Privacy Shield Framework "Privacy Shiled").

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 identifier 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.

Page 1 of 16

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.), 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

1

Page 6 of 16

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.

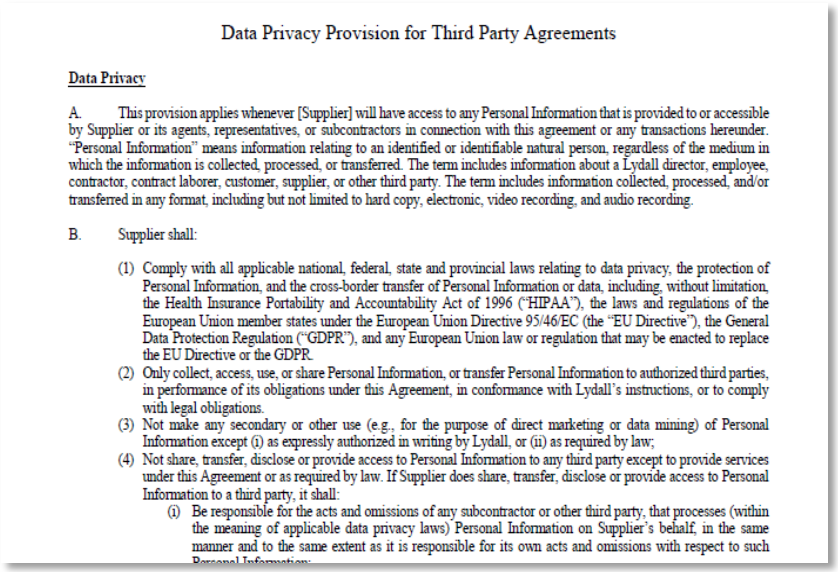
2

Contractual Controls

"Controllers" determine the purpose and means of processing personal data
"Processors" perform operations on personal data (e.g., record, collect, use)

Who, What, Why, How

1 Third party terms



Data Privacy Provision for Third Party Agreements

Data Privacy

A. This provision applies whenever [Supplier] will have access to any Personal Information that is provided to or accessible by Supplier or its agents, representatives, or subcontractors in connection with this agreement or any transactions hereunder. "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 information about a Lydall director, employee, contractor, contract laborer, customer, supplier, or other third party. 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.

B. Supplier shall:

(1) Comply with all applicable national, federal, state and provincial laws relating to data privacy, the protection of Personal Information, and the cross-border transfer of Personal Information or data, including, without limitation, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the laws and regulations of the European Union member states under the European Union Directive 95/46/EC (the "EU Directive"), the General Data Protection Regulation ("GDPR"), and any European Union law or regulation that may be enacted to replace the EU Directive or the GDPR.

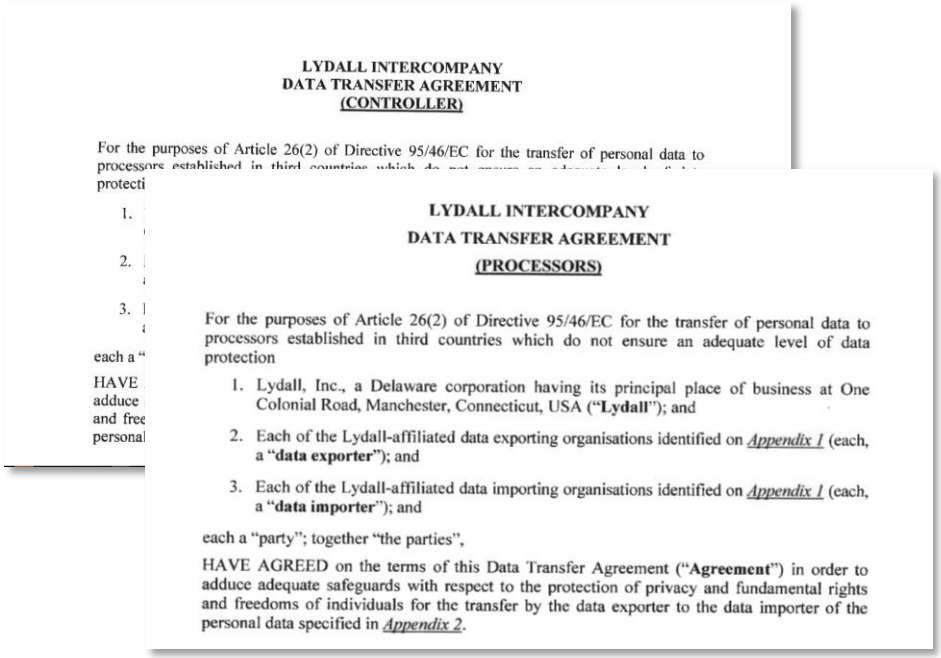
(2) Only collect, access, use, or share Personal Information, or transfer Personal Information to authorized third parties, in performance of its obligations under this Agreement, in conformance with Lydall's instructions, or to comply with legal obligations.

(3) Not make any secondary or other use (e.g., for the purpose of direct marketing or data mining) of Personal Information except (i) as expressly authorized in writing by Lydall, or (ii) as required by law;

(4) Not share, transfer, disclose or provide access to Personal Information to any third party except to provide services under this Agreement or as required by law. If Supplier does share, transfer, disclose or provide access to Personal Information to a third party, it shall:

(i) Be responsible for the acts and omissions of any subcontractor or other third party, that processes (within the meaning of applicable data privacy laws) Personal Information on Supplier's behalf, in the same manner and to the same extent as it is responsible for its own acts and omissions with respect to such Personal Information;

2 Cross-border transfers/Model Clauses



LYDALL INTERCOMPANY
DATA TRANSFER AGREEMENT
(CONTROLLER)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protecti

1.

2.

3.

each a "

HAVE

adduce

and free

personal

LYDALL INTERCOMPANY
DATA TRANSFER AGREEMENT
(PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

1. Lydall, Inc., a Delaware corporation having its principal place of business at One Colonial Road, Manchester, Connecticut, USA (**"Lydall"**); and
2. Each of the Lydall-affiliated data exporting organisations identified on *Appendix 1* (each, a **"data exporter"**); and
3. Each of the Lydall-affiliated data importing organisations identified on *Appendix 1* (each, a **"data importer"**); and

each a "party"; together "the parties",

HAVE AGREED on the terms of this Data Transfer Agreement (**"Agreement"**) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in *Appendix 2*.

Responding to a Data Security Incident
Hypothetical: Business Email Compromise

Detection – could be internal or external

- Have we prepared in advance? Incident Response Plan, insurance, what else
- Who is on the Response Team?

  Internal: Legal/Compliance/Privacy, Risk, IT, HR, ?

  External: Outside Counsel, Forensics, ?

Containment – to prevent further exposure

Analysis – who, what, when, where, why, how

Notification – central coordination, timing, regulators/individuals, law enforcement, DPO…

Data Breach Notifications

GDPR: EU data subjects

- Different harm thresholds
  - Notifying regulators (Article 33) = within 72 hours after the entity has "become aware" of a personal data breach that is likely to result in a "risk to the rights and freedoms of natural persons"
  - Notifying individuals (Article 34) = likely to result in a **high** risk to the rights and freedoms…
- Definitions of "personal data" and "personal data breach" are broader than those in the U.S.
- Which DPA? Notification procedure? Close-out expectation?

In addition, have we triggered:

- State or other jurisdiction data breach notification rules?
- Contractual obligations to notify customers?
- Other Federal notification laws?
  - Financial, health, export-controlled data…
- SEC notice requirements?
- Internal communications/messaging?

Conclusion

Questions?