Morgan Lewis

GLOBAL SPONSOR FORUM

Privacy and Security Updates For Fund Managers

Ezra D. Church, Christopher J. Dlutowski, Elizabeth S. Goldberg, Kristin M. Hadgis, Martin Hirschsprung, Todd Liao, and Pulina Whitaker

April 28, 2022

Speakers

Ezra D. Church
+1.215.963.5710
ezra.church@
morganlewis.com

Christopher J. Dlutowski
+1.212.309.6046
chris.dlutowski@
morganlewis.com

Elizabeth S. Goldberg
+1.412.560.7428
elizabeth.goldberg@
morganlewis.com

Kristin M. Hadgis
+1.215.963.5563
kristin.hadgis@
morganlewis.com

Martin Hirschprung
+1.212.309.6837
martin.hirschprung@
morganlewis.com

Todd Liao
+86.21.8022.8799
todd.liao@
morganlewis.com

Pulina Whitaker
+44.20.3201.5550
pulina.whitaker@
morganlewis.com

Morgan Lewis

Agenda

- Overview and Current Landscape For Fund Managers
- Proposed New Rules
- DOL Guidance
- SEC Enforcement Actions
- Chinese Update
- European Update
- Ransomware Attacks

Overview and Current Landscape For Fund Managers

Morgan Lewis

US Privacy Law – Sector Specific

Financial	Health	Education
• Gramm-Leach-Bliley Act; Reg. S-P; Reg. P • Fair Credit Reporting Act (FCRA) • State laws	• Health Insurance Portability & Accountability Act (HIPAA)	•Federal Educational Rights & Privacy Act (FERPA) • Children's Online Privacy Protection Act (COPPA) • State laws

Regulation S-P (2000)

- Privacy Rule: Notice and opt-out requirements for “nonpublic personal information.” 17 C.F.R. 248.1 et seq.
- Safeguards Rule: Requires (a) adoption of written policies and procedures for the protection of customer information and records, including administrative, technical, and physical aspects; and (b) protection against anticipated threatrs or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information. 17 C.F.R. § 248.30.
- Similar rules apply to non-SEC regulated financial insitututions under Regulation P (Consumer Financial Protection Bureau) and the Safeguards Rule (FTC).

Other Laws

- Breach notification laws
  - First enacted in CA in 2002, now exist in all 50 states
  - Apply based on location of individual's residence
- State information security laws (about 30 states)
  - Most well-known and detailed are the MA Cybersecurity Regulations
  - NY DFS Cybersecurity Regulations
- State consumer privacy laws—limited application
  - California Consumer Privacy Act (CCPA)
  - Other states, Virginia, Colorado, Utah
- Comprehensive privacy laws in jurisdictions around the world
  - EU General Data Protection Regulations (GDPR)
  - Chinese Personal Information Protection Law (PIPL)

Proposed New Rules

Overview of Proposed Cybersecurity Rules

Applicability	• Registered investment advisers • Registered investment companies • Closed-end funds that have elected to be treated as business development companies
Background	• Growing number of cybersecurity risks for advisers and funds • No existing, Securities and Exchange Commission (SEC) rules requiring comprehensive cybersecurity risk management programs • Clients and investors may not be receiving sufficient information on cybersecurity incidents
Proposal Elements	• Adopt and implement cybersecurity risk-management policies and procedures • Report significant cybersecurity incidents to the SEC • Disclose information about cybersecurity risks and significant incidents • Prepare and maintain related records
Comment Period	• The comment period ended on April 11, 2022

Cybersecurity Risk-Management Policies and Procedures

Proposed Rule 206(4)-9 and Proposed Rule 38a-2. Cybersecurity policies and procedures would be required to include the following elements:

- Periodic risk assessments;
- User security and access;
- Information protection (including oversight of third parties);
- Cybersecurity threat and vulnerability management; and
- Cybersecurity incident detection, response, and recovery.

Annual Reviews and Written Reports

- At least annually, advisers and funds would be required to (1) review the effectiveness of their policies and procedures and (2) prepare a written report.

Board Oversight and Reporting

- Fund boards would be required to initially approve the policies and procedures and review the annual written report.
- Board oversight should be conducted proactively.

Reporting of Cybersecurity Incidents to the SEC

Proposed Rule 204-6

- Advisers would be required to submit proposed Form ADV-C to the SEC promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that a significant adviser cybersecurity incident or a significant fund cybersecurity incident has occurred or is occurring.
- Advisers would be required to amend any previously filed Form ADV-C within 48 hours:
  - (1) After information previously reported becomes materially inaccurate;
  - (2) If additional or new material information about a previously reported incident is discovered; or
  - (3) After resolving a previously reported incident or closing an internal investigation relating to a previously reported incident.

Proposed Form ADV-C

- Structured as a series of check-the-box and fill-in-the-blank questions.
- Captures, among other things, identifying information about the adviser as well as details about the nature and scope of the incident, whether law enforcement or other government agencies have been notified, and whether the incident is covered under a cybersecurity insurance policy.

Disclosure of Cybersecurity Risks and Incidents

Amended Form ADV

- Proposed Item 20 of Form ADV Part 2A would require advisers to describe:
  - (1) Any cybersecurity risks that could materially affect the advisory services they offer and how they assess, prioritize, and address cybersecurity risks; and
  - (2) Any cybersecurity incidents that have occurred in the last two fiscal years that have significantly disrupted or degraded the adviser's ability to maintain critical operations or led to the unauthorized access or use of adviser information, resulting in substantial harm to the adviser or its clients.
- Proposed Rule 204-3(b) would require an adviser to promptly deliver interim brochure amendments to existing clients if the adviser adds the disclosure of a cybersecurity incident to its brochure or materially revises information already disclosed in its brochure pertaining to such an incident.

Amended Fund Registration Statements

- The proposal would also require funds to disclose, in their registration statements, any significant fund cybersecurity incidents that have occurred in the last two fiscal years.
- Disclosure must include (1) entity or entities affected; (2) when the incident was discovered and whether it is ongoing; (3) whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; (4) the effect on the fund's operations; and (5) whether the fund/service provider has remediated or is currently remediating the incident.

DOL Guidance

Morgan Lewis

ERISA and Fund Managers 101

- ERISA regulates private employee benefit plans and assets.
- ERISA imposes fiduciary duties of loyalty and prudence.
- Fiduciary duties apply to:
  - “Plan sponsor” fiduciaries
  - Asset managers that accept ERISA fiduciary status by contract or in their actions
- However, ERISA’s standards can impact asset managers that are not ERISA fiduciaries

Benefit Plans and Assets Are Attractive Targets

General Cybersecurity Risks

Cyberattacks are the fastest growing crime in the United States with a global cost of more than $6 trillion annually.

Increasing Incidents of Data Theft

For example, Social Security theft and ransomware attacks.

Increasing Reports of Plan Asset Theft

Public report of plan participants' accounts being accessed and unauthorized distributions being made (e.g., $245K, $400K, $99K).

Increasing Litigation and Regulatory Risks

General Cybersecurity Risks

Plaintiffs' bar continues to find novel theories of fiduciary liability.

US Department of Labor (DOL) Focused on Issue

On April 14, 2021, the DOL issued three pieces of subregulatory guidance.

Also conducting enforcement investigations.

DOL Guidance: Tips for Hiring a Service Provider

Guidance to Plan Sponsors: Tips for plan fiduciaries when hiring a service provider; largely focused on hiring recordkeepers and custodians/trustees.

Tips 1–3

1. Ask about the service provider's data security standards, practices, policies, and audit results and benchmark those against industry standards.
2. Analyze the service provider's security standards and security validation practices.
3. Evaluate the service provider's track record in the industry.

Tips 4–6

4. Ask about past security events and responses.
5. Confirm that the service provider has adequate insurance coverage for losses relating to cybersecurity and identity theft events.
6. Ensure that the services agreement between the plan fiduciary and the service provider includes provisions requiring ongoing compliance with cybersecurity standards.

DOL Guidance: Service Provider Best Practices

Guidance to Service Providers: Practices that plan service providers "should" implement to mitigate risks. Largely directed to recordkeepers and custodians/trustees.

Practices 1–6

1. Have a formal well-documented cybersecurity program
2. Conduct prudent annual risk assessments
3. Have a reliable annual third-party audit of security controls
4. Clearly define and assign information security roles and responsibilities
5. Have strong access-control procedures
6. Ensure that any assets or data stored in a cloud or managed by a third party are subject to appropriate safeguards

Practices 7–12

7. Conduct periodic cybersecurity training
8. Implement and manage an SDLC program
9. Have an effective business resiliency program addressing BCDR and incident response
10. Encrypt sensitive data, stored and in transit
11. Implement strong technical controls in accordance with best practices
12. Appropriately respond to any past cybersecurity incidents

What Might this Mean for Asset Managers

- **What might this mean for asset managers**
  - Asset managers that are ERISA fiduciaries might be subject to DOL guidance and/or face litigation and investigation risks.
  - ERISA plans likely to seek contract/side letter representations.
  - ERISA assets and data can be target even if manager is not a fiduciary.
- **How can we help?**
  - Help with navigating the DOL guidance and enforcement and litigation risks.
  - Help in the event of a breach or incident involving ERISA assets or data.
  - Help with contract/side letter negotiations.

SEC Enforcement Landscape For Fund Managers

Morgan Lewis

SEC Focus on Cybersecurity

- SEC Division of Examination 2022 Priorities
- SEC Risk Alerts
- Enforcement Actions

Three Recent Actions Charging Deficient Cybersecurity Procedures (August 2021)

- Eight firms were charged in three actions for failures in their cybersecurity policies and procedures that resulted in email account takeovers exposing the personal information of thousands of customers and clients at each firm.
- Two of the firms also sent breach notifications to clients that included misleading language suggesting that the notifications had been issued much sooner after discovery of the incidents than they actually were.
- The firms settled with the SEC for fines ranging from $200,000 to $300,000.

Previous Significant Enforcement Actions

Investment Adviser (Sept. 2015)

- First SEC cybersecurity enforcement case.
- The SEC found that investment adviser failed to establish required cyber policies and procedures under Regulation S-P in advance of a breach that exposed PII of approximately 100,0000 individuals.
- $75,000 penalty.

Global Financial Institution (June 2016)

- The SEC concluded that a global financial institutional had failed to adopt written policies and procedures reasonably designed to protect customer data and the company paid a $1 million penalty.
- A former employee improperly accessed and transferred data from more than 700,000 accounts to his personal server, which was then hacked by a third party, conduct for which he was criminally convicted.

Financial, Retirement, Investment and Insurance Company (Sept. 2018)

- The SEC charged this broker-dealer and investment adviser, with violation of the Safeguards Rule in connection with a massive data breach in 2016.
- The company was fined $1 million.

Enforcement Actions Against Public Companies for Disclosure Violations

Title Insurance Company

- 2021
- The company failed to maintain disclosure procedures designed to ensure that the company's senior management received relevant information about the identified vulnerability or lack of remediation.
- The company agreed to a cease-and-desist order and a $487,616 civil monetary penalty.

Media Company

- 2021
- In a media statement, the company referred to the breach as hypothetical when the breach had in fact occurred and claimed that it had “strict protections” in place to prevent such a breach when it had known for six months about the vulnerability that led to the breach.
- The company agreed to cease and desist from committing violations of these provisions and was asked to pay a $1 million civil penalty.

Chinese Update

Morgan Lewis

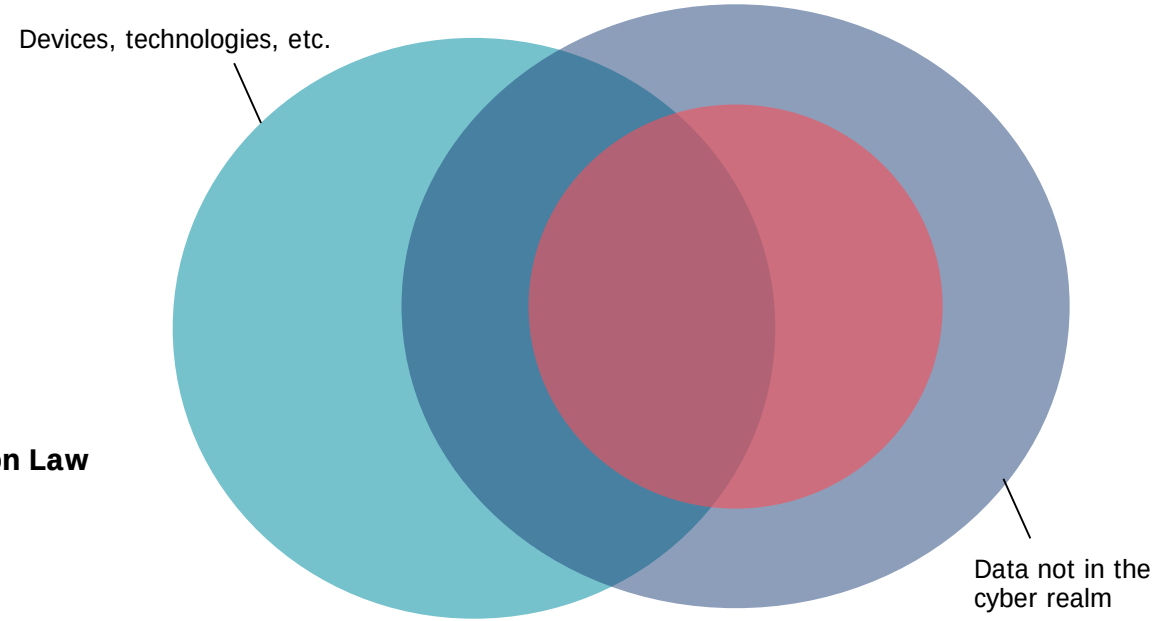
Legal Framework for Data Protection in China

VENN DIAGRAM

Cybersecurity Law

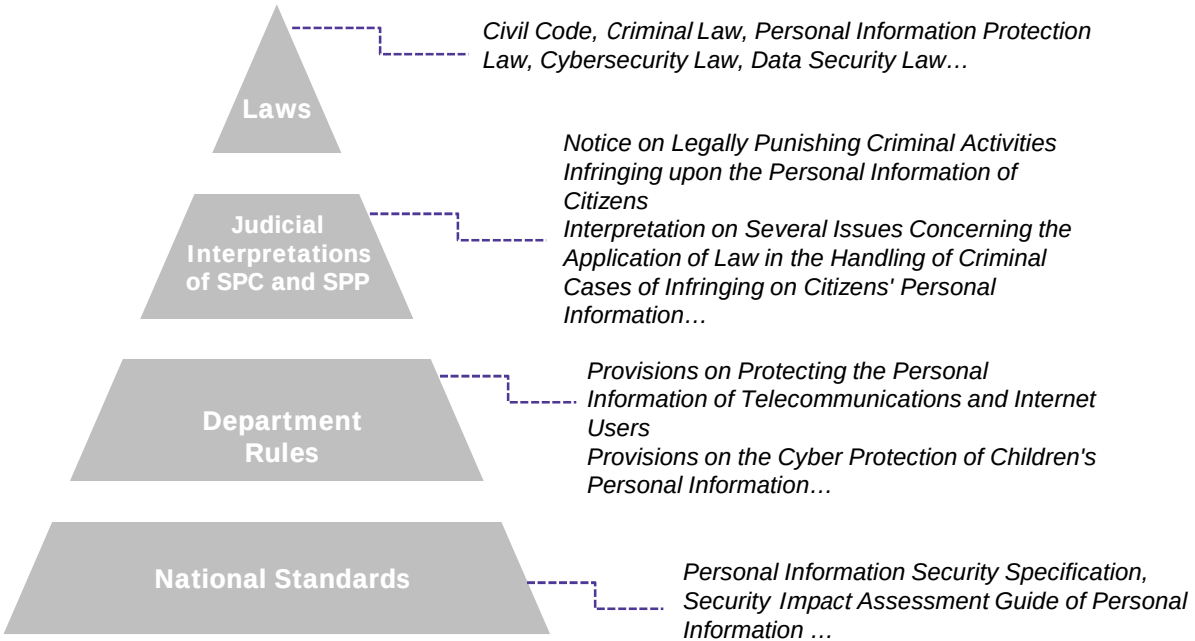
Data Security Law

Personal Information Protection Law



Legal Framework for Data Protection in China

LEGAL FRAMEWORK



Specific Rules in Finance Sector

e.g., Implementation Measures issued by the People's Bank of China for the protection of the rights of financial consumers which came into force on 1 November 2020

e.g., Personal Financial Information Protection Technical Specifications effective from February 2020

e.g., Notice by the People's Bank of China regarding the Effective Protection of Personal Financial Information by Banking Institutions which came into force on 5 January 2011

e.g., Financial Data Lifecycle Guidelines" which came into force on 8 April 2021

……

Legislative Updates

Milestone Legislation

- Cybersecurity Law (“CSL”)
- Data Security Law (“DSL”)
- Personal Information Protection Law (“PIPL”)
- Sector-specific regulations in the finance industry

Legislative Updates – Data Security Law (Sept. 1, 2021)

Application scope and jurisdiction

Data

Art. 3 (1) **Data** refers to any information recorded in electronic or other form.

Data processing

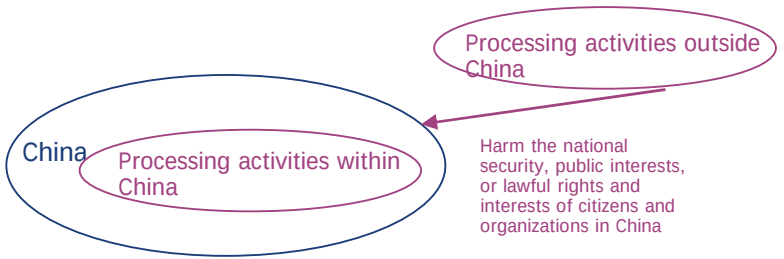
Art. 3 (2) **Data processing** includes collection, storage, use, processing, transmission, provision and disclosure of data.

Data security

Art. 3 (3) **Data security** refers to ensuring that data is in a state of effective protection and lawful use through adopting necessary measures, and to possessing the capacity to ensure a persistent state of security.

Territorial scope – Extraterritorial jurisdiction

Art. 2
(1) Data processing activities within China; and
(2) Data processing activities outside China that harm the national security, public interests, or lawful rights and interests of citizens and organizations in China



Legislative Updates – Data Security Law

Data categorization and protection

Data categorization

Art. 21 China will establish a "categorical and hierarchical system" based on the "importance of the data in economic and social development as well as the extent of harm to national security, public interests, or lawful rights and interests of individuals or organizations that would be caused once the data is tampered, destroyed, leaked, or illegally obtained or used."

Important Data
Data related to national security, economic development and social public interests.

→ **Risk assessment**

National Core Data
Data related to national security, the lifeline of the national economy, important aspects of people's livelihoods, and major public interests.

→ **Stricter management system**
A fine of up to RMB 10 million, cancellation of business licenses, and even criminal penalties

Legislative Updates – Personal Information Protection Law

Definition of key terms

Personal information

Art. 4 **Personal information** is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization processing.

Sensitive personal information

Art. 28 **Sensitive personal information** means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons, grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.

Legislative Updates – Personal Information Protection Law

Legal bases for processing

consent	Art. 13 (1) obtaining individuals' consent – separate consent required for certain situations, e.g. processing sensitive PI
HR functions	Art. 13 (2) necessary to conclude or fulfill a contract, or necessary to conduct human resources management;
legal obligation	Art. 13 (3) necessary to fulfill statutory duties and responsibilities or statutory obligations;
health and safety	Art. 13 (4) necessary to respond to a public health emergency, or in an emergency to protect the safety of individuals' health and property;
news/media reporting	Art. 13 (5) for purposes of carrying out news reporting and media monitoring for public interests;
disclosed already	Art. 13 (6) processing of personal information that is already disclosed;
miscellaneous	Art. 13 (7) other circumstances as required by laws.

Legislative Updates – Personal Information Protection Law

Personal information rights

- Right to information
- Right to access
- Right to correction/rectification
- Right to erasure/deletion
- Right to object to and restrict the processing of an individual's data
- Right to data portability (but needs to satisfy conditions stipulated by the Cyberspace Administration of China (CAC))
- Right to choose whether to be subject to automated decision-making
- Right to withdraw consent
- Right to raise a complaint with the regulator

Legislative Updates – Personal Information Protection Law

Cross-border Transfer of Personal Data

- Obtain separate consent
- Carry out an internal risk assessment prior to cross-border transfer, and keeping records of such transfers (Art. 55)
- Choose one of the following mechanisms to transfer personal information abroad (Art. 38)
  - ✓ undergo a security assessment administered by the CAC (requirements for CII operators and processing entities that transfer a large volume of personal information);
  - ✓ obtain certification from "professional institutions" in accordance with the rules of the CAC;
  - ✓ enter into a transfer agreement with the overseas recipient based on a "standard contract" to be published by the CAC; or
  - ✓ transfer mechanisms in other laws and regulations (or the CAC presumably through implementing regulations).

Legislative Updates – Personal Information Protection Law

Legal liabilities and penalties

Administrative Penalties	Art. 66 of the PIPL a fine of not more than 50 million CNY, or 5% of annual revenue
Civil Liabilities	Art. 69 of the PIPL Where the processing of personal information infringes upon personal information rights and interests and results in harm, and personal information processors fail to prove they are not at fault, they shall take responsibility for the infringement through compensation, etc.
Criminal Liabilities	Art. 253 of the Criminal Law Infringement of Citizen's Personal Information
Public Interest Lawsuit	Art. 70 of the PIPL If the processing entities infringe the rights and interests of a large number of individuals, the People's Procuratorate and other designated organizations may file public interest lawsuits.

Hot Issues Affecting Finance Industry

- Financial personal information protection
- Data localization and cross-border transfer
- Multi-Level Protection Scheme (MLPS)
- Companies planning foreign IPO may be subject to cybersecurity review

Financial personal information protection

Finance sector specific regulations follow the general personal information protection principles under the PIPL framework, but they imposes additional privacy and cybersecurity obligations.

- *Personal Financial Information Protection Technical Specification* ("**Specification**") dictates that personal financial information should be classification into 3 levels and 7 categories.
  - 3 Levels by sensitivity—User identification information (C3), information that can identify personal identity and financial status (C2) and internal information assets (C1)
  - 7 Categories—Account information, identification information, financial transaction information, personal identity information, property information, loan information and other information reflecting certain situations of specific financial information subject.
- The Specification affirms the fundamental principles of fairness, transparency, opt-in consent, minimum use, security and participation by data subjects in handling personal financial information. Specification lays down detailed security requirements in respect of collection, transfer, sharing, storage, use, retention and deletion of personal financial information for its entire life cycle.

Data localization and cross-border transfer

Critical information infrastructure operators (CIIO)	• Personal information and important data should be stored within China; cross-border data transfers are subject to a government-led security assessment (and are not permitted if they bring risks to the national security, public interests, or data subjects' rights). • Under the *Critical Information Infrastructure Security Protection Regulation*, entities in finance industry may fall within the category of CIIO and as a general principle, personal financial information collected or generated in China must be stored and processed in China.
Non-CIIOs	The following data should be stored in China and subject to security assessment for cross-border transfer: • Personal information exceeding an amount threshold designated by CAC. • Important data.
Sector-specific regulation	The storage, processing and analysis of personal financial information collected in China shall be carried out within China.

Data localization and cross-border transfer

Triggering Criteria for Mandatory Government-led Security Assessment under the draft Security Assessment Measures

Key Factors	Triggering Criteria
Based on the "**special identity**" of the data controller	CIIO
	Operators who possess personal information of over a million users
Based on the "**sensitivity and scale**" of the data to be transferred abroad	The data to be transferred includes "important data"
	Cross-border transfer of personal information of over 100,000 individuals or sensitive personal information of over 10,000 individuals
Other factors	Other situations to be determined by the CAC

Regardless of whether the data transfer by a data processor triggers a CAC-led security assessment, the data processor is required to conduct a risk self-assessment on its data export before transferring any data outside of the PRC.

Important data in the finance industry

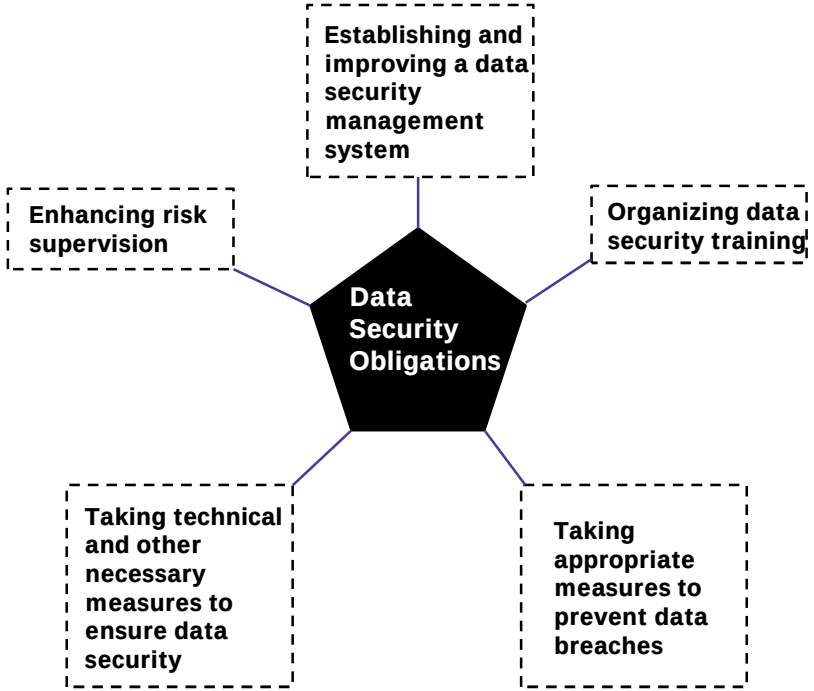
The DSL did not offer a clear definition of "important data," but empowered regional and industry authorities to formulate specific catalogs.

Cyberspace Administration of China ***Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Exposure Draft)***	Art. 17 "**Important data**" refers to the data closely related to national security, economic development, and social and public interests. Refer to relevant national standards and important data identification guidelines for its specific scope.
National Information Security Standardization Technical Committee ***Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment***	Appendix A "**Important data**" refers to the data (including original data and derived data) collected or generated by the government, enterprises and individuals within the territory of the People's Republic of China that do not involve state secrets but are closely related to national security, economic development and public interests, once unauthorized disclosure, loss, misuse, alteration or destruction, or convergence, integration, analysis, may result in the following consequences. A 19.1 Financial Institution Security Information A 19.2 Financial Information of Natural Persons, Legal Persons and Other Organizations
The People's Bank of China ***Financial Data Security - Guides of Data Security Classification***	Art. 5.3 Financial Data Classification Financial Industry Institutions should classify their financial data into Levels 5, 4, 3, 2 and 1, in descending order of importance, by evaluating the "impacted areas" and the "degree of impact" in the event of data leakage or destruction. Appendix C "**Important data**"

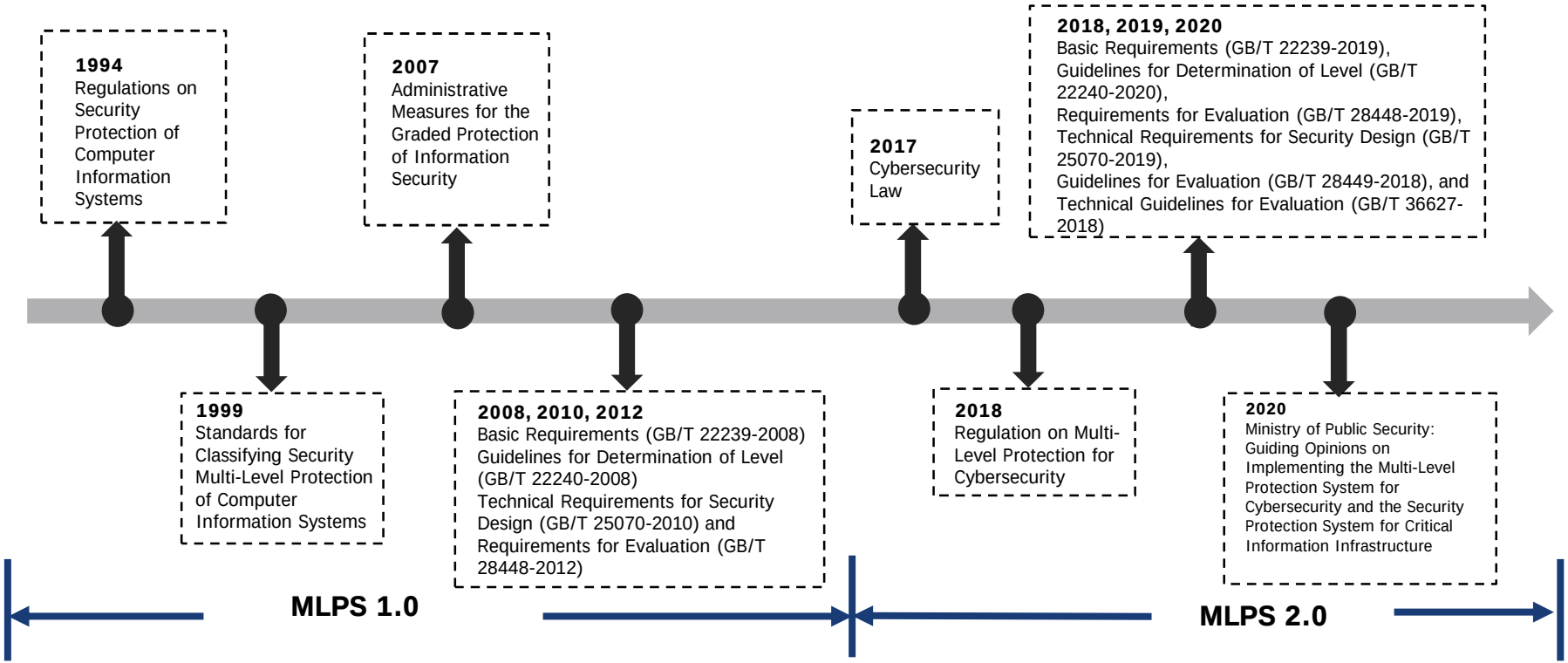
MLPS requirements and data security obligations

Multi-Level Protection Scheme

- Article 21 of the CSL provides that the country shall implement the rules for graded protection of cybersecurity.
- Article 27 of the DSL reemphasizes the importance of the MLPS by requiring all entities in China to carry out data processing activities in compliance with the data security requirements under the MLPS.



Multi-Level Protection Scheme



Multi-Level Protection Scheme

Definition

Multi-level protection scheme for cybersecurity refers to the multi-level protection and multi-level supervision and administration of networks (including information systems and data), the multi-level management of cybersecurity products, and the multi-level response to and disposal of security incidents occurring in the network.

Targets

The targets in the multi-level protection for cybersecurity are the systems that are composed of computers or other terminals and relevant equipment to collect, store, transmit, exchange and process information in accordance with certain rules and procedures, mainly including basic information networks, cloud computing platforms/systems and big data applications/platforms/funds, IoT, industry control system and systems employing mobile interconnection technology, etc. (Article 5.1 of Basic Requirements for Multi-Level Protection for Cybersecurity)

Procedures

Self-assessment

↓

Preliminary determination of Level

↓

Expert verification

↓

Filing with local PSB

↓

An official MLPS certification is issued

Multi-Level Protection Scheme

Determining the Steps for MLPS

Step 1

Prerequisite

- The system should be physically located in mainland China (including systems deployed on the cloud)

Type of server	Location
Application Server	Should be deployed in China
Database Server	Should be deployed in China

Step 2

Determine impact level of business information security

- Impact of data breach is based on the volume of personal information and sensitive personal information stored in the system
- Includes systems that cause social impact in case of problems, such as downtime or loss of sensitive information other than personal information

Level	Total amount of sensitive PII	Total amount of PII
Level 1	0-1,000	0-10,000
Level 2	1,000-10,000	10,000-100,000
Level 3	10,000-100,000	100,000-1,000,000
Level 4	≥100,000	≥1,000,000
Level 5		

Step 3

Determine impact level of system service security

- Impact of system failure to business operation is based on the importance of the system

Level	Importance of the system
Level 1	Low important system
Level 2	Medium important system
Level 3	High important system
Level 4	Extremely important system (only applicable to systems owned by State-owned enterprise or financial institution)
Level 5	

Multi-Level Protection Scheme

Proposed Compliance Path for MLPS 2.0

- Enterprises should identify systems and generate a system inventory based on the enterprises' operations and plans.
- Based on the identified grading objects and their levels, enterprises should perform gap analysis with reference to the MLPS requirements and produce self-assessment reports.
- Prepare grading documentation, arrange external expert reviews (level 2 or above), obtain approvals from authorities (where applicable), and submit filings to the relevant public security organs.
- Formulate security plans and determine cybersecurity tasks and their priorities, costs, and resources based on cybersecurity governance goals and findings from the MLPS assessment.

Companies seeking listing overseas may be subject to cybersecurity review

- Companies seeking to list outside of China and Hong Kong may be subject to a cybersecurity review if they hold data of more than one million people.
  - Under the *Cybersecurity Review Measure*, Chinese network platform operators (NPOs) holding personal information of more than one million users must apply for a cybersecurity review from the Cyberspace Administration of China (CAC) before being "publicly listed abroad."
  - Under the draft *Regulations for the Administration of Network Data Security*, the cybersecurity review is required when, among others, (1) the data handler processing the personal information of more than one million individuals is seeking to go public overseas; (2) the data handler is seeking to go public in Hong Kong, which will or may impact national security.
- The CAC can initiate a cybersecurity review, presumably against any entity, if it deems that the entity's data processing activities or products and services will or may affect national security.
- The cybersecurity review may take 70 working days or, in exceptional cases, 160 working days or even longer.

Companies seeking listing overseas may be subject to additional requirements under draft rules

- On April 2, 2022, China Securities Regulatory Commission published the draft *Provisions on Strengthening Confidentiality and Archives Administration of Overseas Securities Offering and Listing by Domestic Companies* for public consultation.

Application Scope	
1.	**PRC domestic enterprises seeking listing overseas**, including: • domestic joint stock companies seeking directly listing overseas; • domestic operating entities that indirectly list overseas through non-PRC incorporated listing vehicles (such as VIE)
2.	**Securities companies and securities service agencies helping PRC companies list on overseas stock exchanges**, including: • domestic and overseas securities companies and securities service agencies; • their member organizations, representative offices, joint venture organizations, cooperative organizations and other related organizations in the Mainland.
3.	**Accounting firms servicing PRC listed companies**

Companies seeking listing overseas may be subject to additional requirements under draft rules

- Major restrictions under the draft rule include:
  - When domestic enterprises are required to share certain data with securities firms, securities service firms ("**third-party intermediaries**") and overseas regulators, to the extent that such shared data constitute State secrets or are otherwise confidential from a governmental perspective, or the leakage of such data may adversely affect national security or public interest, domestic enterprises are required to complete the relevant procedures, including obtaining an approval, making a filing and/or consulting with relevant authorities;
  - Domestic enterprises should provide a written record in respect of the implementation of the abovementioned procedural requirements and enter into a proper non-disclosure agreement with third-party intermediaries;
  - Any working paper of the listing project and/or any archive file generated by third-party intermediaries in mainland China when providing services to domestic enterprises should be stored in mainland China, and the export of which is subject to governmental approvals.

Key Take-Aways

Proactive steps to mitigate the compliance risks that MNCs may face:

1. Perform data mapping to understand categories and location of data and identify important data, personal information, and sensitive personal information that the company is processing.
2. Perform a gap analysis of the current data-related policies, both internal employee notice and external-facing privacy notices and policies, to comply with the informed consent requirements.
3. Establish a risk assessment process for major data processing activities, covering the processing of important data, (sensitive) personal information, and cross-border data transfer, including the internal assessment and government reporting obligations.
4. Conduct the MLPS as soon as possible.
5. Understand the localization requirements and (if required) implement localized storage within China.

European Update

Morgan Lewis

European Data Protection Laws

- **UK Framework:**
  - UK GDPR
  - EU GDPR – extraterritorial processing
  - DPA 2018
  - PECR
- **Rest of Europe:**
  - EU GDPR
  - UK GDPR – extraterritorial processing
  - Local laws supplementing the GDPR
  - Local laws implementing 2002 ePrivacy Directive

Data Protection Framework – Key Requirements

- Data-subject rights of access, rights to restrict or erase data, and rights of portability: within one month (or up to three months), no fee
- Stricter processing requirements for special categories of data, e.g., health information and biometrics:
  - express, informed, freely given consent
  - employment laws
  - assessment of working capacity
- Data protection impact assessment: required prior to processing if high risk for individuals
- Penalties for breach of GDPR; up to 4% global turnover or €20m/£17.5m, whichever is higher (depends on nature and extent of breach)
- Controllers and processors directly liable under GDPR
- Processor audit rights required by controllers
- Recordkeeping requirements
- DPO requirement for some companies processing large amounts of special categories or criminal record data
- Appointed representative for non-EU/non-UK organizations

Key GDPR Issues

- **Data-subject rights:**
  - one month to respond; how to extend to three months?
  - charging a fee or refusing to respond
  - managing regulatory/data-subject/third-party privacy claims or complaints
  - redactions and exemptions
- **Data breaches:**
  - management and remediation
  - investigations
  - notices

Data Privacy Documents

- Employee privacy notices: candidates and employees
- Investor privacy notices
- DPAs with administrators
- DSAR process and response templates for legal/HR
- DPIA
- Processing clauses for supplier and commercial contracts
- New EU SCCs now in force
- New UK IDTA and UK Addendum now also in force

Fine Factors

- **Gravity and nature** — The overall picture of the infringement. What happened, how it happened, why it happened, the number of people affected, the damage they suffered, and how long it took to resolve.
- **Intention** — Whether the infringement was intentional or the result of negligence.
- **Mitigation** — Whether the firm took any actions to mitigate the damage suffered by people affected by the infringement.
- **Precautionary measures** — The amount of technical and organizational preparation the firm had previously implemented in order to be in compliance with the GDPR.
- **History** — Any relevant previous infringements, including infringements under the Data Protection Directive (not just the GDPR), as well as compliance with past administrative corrective actions under the GDPR.
- **Cooperation** — Whether the firm cooperated with the supervisory authority to discover and remedy the infringement.
- **Data category** — What type of personal data the infringement involves.
- **Notification** — Whether the firm, or a designated third party, proactively reported the infringement to the supervisory authority.
- **Certification** — Whether the firm followed approved codes of conduct or was previously certified.
- **Aggravating / mitigating factors** — Any other issues arising from the circumstances of the case, including financial benefits gained or losses avoided as a result of the infringement.

Data breaches

- What is reportable?
- All personal-data misuse or loss is a data breach; assess risk of harm for reporting
- Different authorities take different approach to “harm”
- Best to be cautious and report if unsure

Data Transfers under UK and EU GDPR

- General restriction on transferring personal data outside EEA to a “third country”
- European Commission list of adequate countries: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, and Uruguay – and now the United Kingdom
- United Kingdom is looking at its own list, possibly to include the United States in one shape or form, e.g., a type of certification arrangement or by State
- Proposed new EU-US transatlantic framework
- GDPR-permitted data transfer options (DTO) (safeguards):
  - Binding corporate rules
  - Standard contractual clauses: importer controller/processors based in the third country; exporter controller must be based in Europe – these will be replaced shortly (this month or next?)
  - Importer subject to an approved code of conduct
  - Importer subject to an approved certification mechanism
- GDPR-permitted derogations:
  - Explicit consent
  - Transfer is “necessary” for performance of contract; to establish, exercise, or defend legal claims; from a public register
  - Where the transfer is not repetitive, concerns a limited number of data subjects, is necessary for compelling legitimate interests of controller (not overridden by data-subject rights) and safeguards in place to protect the data

Which DTO?

- EU SCCs and UK IDTA: easy to execute, not so easy to implement
  - Need to consider legal framework in importer's country;
  - Consider additional safeguards, e.g., encryption in transit and at rest;
  - Importer to notify exporter if it cannot comply with SCC/IDTA obligations
  - Exporter or supervisory authority can suspend data flow pending EDPB approval
  - UK Addendum to EU SCCs or stand-alone IDTA for UK transfers
- BCRs – time and expense to get approval; now need UK and EU authority approval post-Brexit
- Consent – GDPR standard of explicit consent
- Legitimate interests – for one-off limited transfers; notify supervisory authority first
- Other new options: code of conduct, privacy seals – details awaited from supervisory authorities
- Give notice to data subjects of the transfers

Ransomware Attacks

Morgan Lewis

Ransomware Attacks – What Are They?

- The increase in ransomware attacks is big news in privacy and cyber fields.
- 700% increase in ransomware attacks for 2020, even more in 2021.
- What are they?
  - A threat actor enters a system and uses malware to encrypt the system to shut it down
  - The threat actor sends a ransom note demanding payment in cryptocurrency in exchange for the key needed to decrypt the system
  - Launched by organized criminal groups, typically located in Russia, China, or North Korea, with Darkside, Nightwalker, and Revil
  - Dual threat—exfiltration of sensitive data

Ransomware Attacks – What Is Causing Them?

- **Change in business model—traditional attacks focused on exfiltration are more difficult to perpetrate and less lucrative.**
  - Companies avoid storing sensitive data, use encryption and multifactor.
  - Payment network has evolved with chip technology and other changes
  - Your data is already out there!
- **Fueled by the rise in remote work and distraction due to COVID-19 over the last years, which has made companies more vulnerable.**
  - Use of remote-access tools such as outdated VPNs and equipment, personal devices, and unsecure Wi-Fi
  - In May 2020 Microsoft found that the level of overall cyberattacks reached an all-time high in the three months immediately after the World Health Organization (WHO) announced that COVID-19 was a global pandemic.

Ransomware Attacks – How to Respond When They Occur

- Convene the incident response team
- Outside counsel's role
- Outside cybersecurity expertise
- Insurance
- PR and crisis communications
- Contacting law enforcement
- Negotiating a ransom payment
- Data mining
- Notification obligations

Ransomware Attacks – Is It Alright to Pay?

- The US Department of the Treasury's Office of Foreign Assets Control (OFAC) recently issued an updated advisory on potential sanctions risks for companies facilitating payments in connection with ransomware attacks.
- In September 2021, OFAC for the first time sanctioned a cryptocurrency exchange for its part in facilitating financial transactions for ransomware actors, and it will continue to impose sanctions on those who provide financial, material, or technological support to perpetrators of ransomware activities.
- Violations of OFAC regulations may result in civil penalties based on strict liability.
- OFAC strongly discourages companies from making ransomware payments and instead recommends focusing on strengthening defensive measures and reporting to/cooperating with authorities—actions that OFAC would consider to be "mitigating factors" in any related enforcement action.

Ransomware Attacks – How Can You Prevent Them?

- Focus on backups—ensure they are regular, complete, and segregated.
- Know your system and endpoints—inventory and data map are critical.
- Consider vulnerabilities created in remote work environment.
- Maintain good, consistent cyber hygiene:
  - Regular patches
  - Updated antivirus
  - Authentication protocols (passwords and multifactor)
- The buck stops with your incident response team and planning process.

Attorney Biographies

Morgan Lewis

Ezra D. Church

Philadelphia

T +1.215.963.5710

ezra.church@morganlewis.com

Ezra D. Church counsels and defends companies in privacy, cybersecurity, and other consumer protection matters. He helps clients manage data security and other crisis incidents and represents them in high-profile privacy and other class actions. Focused particularly on retail, ecommerce, and other consumer-facing firms, his practice is at the forefront of issues such as biometrics, artificial intelligence, location tracking, ad tech, and blockchain. Ezra is a Certified Information Privacy Professional (CIPP) and co-chair of the firm's Class Action Working Group.

Ezra advises clients on compliance with data privacy and cybersecurity requirements such as the California Consumer Privacy Act (CCPA), the Gramm-Leach Bliley Act (GLBA), including Regulation S-P, Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) laws, the Telephone Consumer Protection Act (TCPA), the Fair Credit Reporting Act (FCRA), the Illinois Biometric Privacy Act (BIPA), the EU's General Data Protection Regulation (GDPR), and state data breach notification laws. He has particular experience with children's privacy issues and has worked extensively with on educational technology firms and mobile app and game developers in connection with the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA), and numerous state law regarding education privacy. Ezra has assisted hundreds of multinational companies with advice, planning and connections with GDPR and the Privacy Shield for data transfers to and from the United States to EU countries. He has advised on privacy and security issues related to cutting-edge technologies including facial recognition, voice recognition, iris and retinal scanning, artificial intelligent and machine learning, ad tech, location tracking and employee monitoring, and blockchain. He is a Certified Information Privacy Professional with the International Association of Privacy Professionals. He writes and speaks frequently on privacy and data security and has lectured on privacy law at Rutgers University Law School.

Ezra has worked with hundreds of companies facing data breaches, counseling them in the critical hours after an incident occurs, helping them understand and investigate the issues, and crafting an effective and appropriate notice program for affected individuals and government regulators. He also works with companies to anticipate and prepare for cybersecurity incidents before they occur, developing breach response plans to help prevent and mitigate future breaches. Ezra is a member of Morgan Lewis's Crisis Management Practice, with a focus on the management of the crises involved in cybersecurity incidents.

Beyond his counseling practice, Ezra has experience handling complex and unusual class action litigation, including some of the largest privacy and data security class actions in the United States. This includes the defense of major national retailers facing data security litigation and the representation of consumer-facing companies facing large class actions filed under the TCPA and other privacy statutes. He has handled all aspects of such cases from inception through trial and appeal and has rare experience litigation class actions all the way through class trial. He is the co-leader of the Firm's Class Action Working Group and regularly writes and speaks on class action issues. He is a contributor to the Firm's chapter on class action litigation in the leading treatise Business and Commercial Litigation in Federal Courts and co-author of a chapter in A Practitioner's Guide to Class Actions, among others.

Ezra has spent over 10 years advising and defending retailers and ecommerce companies, focused on helping them find practical ways to address the unique legal challenges they face. He has counseled and defended clients on matters related to privacy and data security, credit cards, gift cards, employee background checks, anti-money laundering, advertising and sales issues, vendor and supplier issues, return policies, marketing practices, loyalty programs, layaway, and unclaimed property.

Christopher J. Dlutowski

New York

T +1.212.309.6046

christopher.dlutowski@morganlewis.com

Christopher J. Dlutowski represents institutional investors—including public and private pension plans, family offices, sovereign wealth plans, universities, endowments, and funds of funds—on their investments in private equity, hedge, venture capital, private debt, real estate, infrastructure, hybrid, and other private funds, funds-of-funds, managed accounts, co-investments, and direct investments, and on governance and compliance issues. Christopher also counsels private investment funds—including US domestic and offshore private equity funds, hedge funds, and funds-of-funds—and investment management firms on the formation and structuring of funds, trading and other investment activities, capital raising, registration and other regulatory issues, and ongoing operations.

Christopher has more than 25 years of experience in customized investment products, including strategic partnerships, captive funds, and co-investment funds, in all asset classes.

Christopher has presented on private investment funds topics at numerous investment management conferences and training programs. Prior to re-joining Morgan Lewis, Christopher was vice president and corporate counsel at Prudential Financial, Inc. where he advised investment management clients on their hedge funds and other alternative investment products, US and foreign institutional investor mandates, trading activities (including securities, derivatives, lending, and financing transactions), marketing efforts, domestic and foreign registration, and other regulatory issues.

Christopher is the chair of the firm's institutional investors working group, a co-leader of the firm's education industry team, and a member of the New York office's recruiting committee.

Elizabeth S. Goldberg

Pittsburgh
T +1.415.560.7428
elizabeth.goldberg@morganlewis.com

Elizabeth (Liz) Goldberg advises employee benefit plan sponsors and service providers to those plans (including financial service firms) on ERISA US Department of Labor (DOL) enforcement investigations, DOL ERISA regulatory matters, and ERISA fiduciary counseling and compliance.

Liz has broad experience representing both plan and service provider clients in DOL ERISA investigations. Liz has worked on more than 30 such DOL investigations including matters that have involved significant monetary disputes or enterprise risk. In assisting in such matters, Liz draws on her prior work experience that includes six years at the DOL's Office of the Solicitor, primarily as an ERISA litigator. Liz also works with clients to perform internal audits to minimize any potential liability related to DOL investigations or ERISA litigation.

Liz's experience also includes other matters before the DOL, including prohibited transaction exemption applications and representing clients in other DOL regulatory processes (such as ERISA rulemaking).

Liz advises fiduciaries and related parties and service providers on ERISA fiduciary compliance including on ERISA's fiduciary rules, governance issues, and prohibited transaction exemptions. This includes her work with fiduciaries on governance issues, such as setting up fiduciary committees and drafting investment policies. She also provides related counseling on general employee benefit plan issues, such as tax qualification rules.

Kristin M. Hadgis

Philadelphia

T +1.215.963.5563

kristin.hadgis@morganlewis.com

Kristin M. Hadgis counsels and defends retail and other consumer-facing companies in matters relating to privacy and cybersecurity, class actions, Attorney General investigations and enforcement actions, the California Consumer Privacy Act, consumer protection laws, retail operations, loyalty and gift card programs, and commercial disputes. Kristin also handles data security incident response crisis management, including any resulting litigation or government investigations.

Kristin has advised hundreds of companies in connection with privacy and cybersecurity compliance issues such as privacy policies, information security policies, incident response plans, and protocols for data collection, storage, and transfer. Her experience includes the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), state data security laws, the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transactions Act (FACTA), US federal and state CAN-SPAM laws, the Telephone Consumer Protection Act (TCPA), Federal Trade Commission (FTC) rules, the Securities and Exchange Commission privacy regulations (Reg. S-P), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA). Kristin has advised on more than 250 data breaches in her career, counseling clients on how best to give notice to affected individuals or government and consumer reporting entities, following proper compliance protocol. Kristin also represents these companies on any class action and other litigation stemming from the incidents, and instructs them on implementing policies and procedures to prevent and mitigate future breaches.

Kristin also understands the unique issues and challenges facing retail, e-commerce and other consumer-facing companies, and routinely advises these clients on a variety of legal, regulatory, and operational matters. She works closely with clients on retail operations and compliance, including the launch of bricks and mortar stores across the United States and e-commerce platforms. She also counsels retail and consumer-facing clients on loyalty programs, gift cards, marketing and advertising, social media, price comparison, fraud prevention, online contracting and website terms, and privacy and data security compliance.

She is a member of the firm's retail and privacy and cybersecurity practices as well as its class action working group. Kristin routinely writes articles on developments in the law on consumer and data privacy matters

In her pro bono practice, Kristin represents children in dependency proceedings through the Support Center for Child Advocates.

Prior to joining Morgan Lewis, Kristin clerked for Judge Timothy R. Rice of the US District Court for the Eastern District of Pennsylvania. While attending law school, she was a legal extern for Judge Juan R. Sanchez in the same court.

Martin Hirschsprung

New York

T +1.617.951.8833

martin.hirschprung@morganlewis.com

Martin Hirschprung's practice involves counseling US and international banks and non-bank financial services companies on corporate, regulatory, and compliance matters. He advises clients on major state and federal financial services statutes and regulations, including data protection, anti-money laundering, fiduciary duties, consumer lending, licensing, and transactional matters. Martin is a member of the firm's Privacy and Cybersecurity practice and a Certified Information Privacy Professional/United States (CIPP/US). He works with companies on designing and building aspects of their privacy programs, including internal policies, procedures, and guidelines that incorporate best practices and legal requirements.

Martin also represents mutual fund complexes, their independent trustees and investment advisers in a number of areas, including SEC filings, and regulatory and compliance issues.

Before joining Morgan Lewis, Martin served as associate counsel at JPMorgan Chase through the firm's Chase Honors Program. At Chase, Martin worked with the Regulatory, Operations & Controls group to identify and correct the root causes of customer complaints. He also supported privacy and cybersecurity initiatives.

Todd Liao

Shanghai
T +86.21.8022.8799
todd.liao@morganlewis.com

Todd Liao works with clients on a wide range of financial transactions and legal issues involving China. He frequently works with multinational corporations on cross-border mergers and acquisitions, foreign direct investment and investment financing, disposal of Sino-foreign joint ventures and assets, and the structuring of complex commercial transactions. Todd also handles intellectual property (IP) work, specifically assisting clients with managing their trademark portfolios. He is admitted in New York only.

In addition, Todd counsels on matters related to the US Foreign Corrupt Practices Act (FCPA) practice in China and throughout the Asia-Pacific region. He advises multinational corporations regarding compliance with the FCPA and other regulatory compliance matters including policies and practices, gifts, travel and entertainment policies and violations, third-party due diligence issues, managing and conducting investigations of alleged FCPA violations, whistleblower investigations, and employee disciplinary actions. He also conducts FCPA training in multiple languages.

Todd was a recent speaker at the Anti-Corruption China Summit conference hosted by Beacon. He is fluent in Mandarin Chinese, English, Shanghainese, and Cantonese.

Pulina Whitaker

London

T +44.20.3201.5550

pulina.whitaker@morganlewis.com

Pulina Whitaker's practice encompasses data privacy and cybersecurity as well as employment matters. Co-head of the firm's global privacy and cybersecurity practice, she manages employment and data privacy issues on an advisory basis and in sales and acquisitions, commercial outsourcings, and restructurings. Pulina manages international employee misconduct investigations as well as cross-border data breach investigations. She has been appointed as a Compliance Monitor for the United Nations and has completed a three-year Monitor engagement of a UK charity for USAID. She is also a trustee of Hostage International.

Pulina is often appointed to conduct independent misconduct investigations, including most recently for UNICEF UK in response to bullying allegations. She acts for employers in defending against employment and data privacy allegations and claims, including for bullying/harassment, unfair dismissal, discrimination, whistleblowing, breach of data processing, and employment contract claims. She has experience working with international and European clients to help them comply with the EU General Data Protection Regulation, including advising on audits of data processing activities and data security incidents.

Pulina advises on cross-border commercial outsourcing and corporate reorganizations, negotiating warranty and indemnity provisions and disclosures in transactional documentation, and conducting global redundancy and furlough projects. She is skilled at navigating individual and collective consultation requirements in multiple jurisdictions, including dealing with trade unions and works councils. She also advises on the automatic transfer of employment requirements and related information and consultation obligations in the United Kingdom and across other European jurisdictions.

Pulina's practice spans internationally, and she speaks French and Italian.

She has been described by clients in *The Legal 500* as "extremely knowledgeable with a practical approach" and is noted as being "a key name for issues covering employment and data privacy work." Also named as a *Legal 500* leading practitioner, they go on to note Pulina "is head and shoulders above the data protection and privacy pack on her command of law, requirements, and implementation."

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.