Compliance Check List: Required Data Processing Agreements

This checklist is designed to help MSPs identify which data privacy and security laws apply to their business and integrate the required data processing terms into their contracts. It includes jurisdictional nuances, threshold criteria, and actionable steps.

1 General Data Protection Regulation (GDPR)

Jurisdiction:

- Applies to companies anywhere in the world if they process personal data of EU or UK residents.

Threshold Criteria:

- You collect or process data about individuals located in the EU or UK.
- You offer goods or services to EU/UK residents (e.g., a website targeting EU/UK customers).
- You monitor the behavior of individuals in the EU/UK (e.g., tracking cookies).

Required Data Processing Terms:

- Include a Data Processing Addendum (DPA) with provisions for:
    1. Data transfer mechanisms (e.g., Standard Contractual Clauses).
    2. Obligations for breach notification within 72 hours.
    3. Rights of data subjects (access, deletion, rectification).

Does this regulation apply to your MSP?

☐ Yes ☐ No

2 Health Insurance Portability and Accountability Act (HIPAA)

Jurisdiction:

- Applies to entities operating in the U.S. that handle protected health information (PHI).

Threshold Criteria:

- You provide services to healthcare providers, insurers, or other "covered entities."
- You handle PHI, such as patient records or billing information, on behalf of these entities.

Required Data Processing Terms:

- Include a Business Associate Agreement (BAA) specifying:
    1. MSP's responsibility to protect PHI.
    2. Breach reporting requirements.
    3. Permitted and prohibited uses of PHI.

Does this regulation apply to your MSP?

☐ Yes ☐ No

3 Gramm-Leach-Bliley Act (GLBA)

Jurisdiction:

- Applies to financial institutions in the U.S. and companies handling sensitive financial data.

Threshold Criteria:

- You provide IT services to banks, credit unions, mortgage brokers, or other financial institutions.
- You access or store customer financial information.

Required Data Processing Terms:

- Include a clause in your agreements specifying:
    1. Safeguards for protecting customer financial data.
    2. Responsibilities for identifying and mitigating security risks.

Does this regulation apply to your MSP?

☐ Yes ☐ No

4 Cybersecurity Maturity Model Certification (CMMC)

Jurisdiction:

- Applies to companies providing services to the U.S. Department of Defense (DoD) or handling Controlled Unclassified Information (CUI).

Threshold Criteria:

- You subcontract for DoD contractors or handle DoD-sensitive data.
- You provide IT services that involve CUI.

Required Data Processing Terms:

- Include a CMMC Compliance Addendum detailing:
    1. Certification levels required for data handled.
    2. Breach reporting obligations.
    3. Periodic audit requirements.

Does this regulation apply to your MSP?

☐ Yes ☐ No

5 U.S. State Privacy Laws

Jurisdiction:

- Applies to companies operating in states with comprehensive privacy laws, such as California (CCPA/CPRA), Virginia (VCDPA), Colorado (CPA), Utah (UCPA), and Connecticut (CTDPA).

Threshold Criteria by State:

- **California (CCPA/CPRA):**
    1. Annual gross revenue exceeds $25 million.
    2. You process personal data of 100,000+ California residents annually.
    3. You derive 50%+ of revenue from selling California residents' data.

Does this regulation apply to your MSP?

☐ Yes ☐ No

- **Virginia (VCDPA):**
    1. Process personal data of 100,000+ Virginia residents annually.
    2. Process data of 25,000+ residents and derive 50%+ of revenue from data sales.

Does this regulation apply to your MSP?

☐ Yes ☐ No

- **Colorado (CPA):**
    1. Process personal data of 100,000+ Colorado residents annually.
    2. Process data of 25,000+ residents and derive revenue from data sales.

Does this regulation apply to your MSP?

☐ Yes ☐ No

- **Utah (UCPA):**
    1. Process data of 100,000+ Utah residents annually.
    2. Process data of 25,000+ residents and derive revenue from data sales.

Does this regulation apply to your MSP?

☐ Yes ☐ No

- **Connecticut (CTDPA):**
    1. Process personal data of 75,000+ Connecticut residents annually.

Does this regulation apply to your MSP?

☐ Yes ☐ No

Required Data Processing Terms:

- Include a **Data Processing Addendum (DPA)** specifying:
  1. Consumer rights to access, delete, and opt out of data collection.
  2. Prohibition of data use beyond agreed purposes.
  3. Compliance with state-specific notification and processing rules.

Does this regulation apply to your MSP?

☐ Yes ☐ No

Next Steps

- **Determine which regulations apply to your MSP using this checklist.**
- **Update your contracts to include the necessary data processing terms.**
- **Consult legal counsel to ensure compliance.**