Document Name: Relevant Laws, Regulations, and Contractual Requirements

|  |  |
| --- | --- |
| Company Name: | [Company Name] |
| Policy Owner(s): | [Policy Owner] |
| Effective Date: | XX/XX/XXXX |

1. Purpose

The purpose of this workbook is to identify, update, and maintain a current list of all relevant laws, regulations, and contractual requirements and [Company Name]'s approach to meeting these requirements.

1. Relevant Laws, Regulations, and Contractual Requirements

| **Relevant Laws, Regulations, and Contractual Requirements** | **[Company Name] as Data Controller** | **Approach to Meeting Requirements** | **[Company Name] as Data Processor** | **Approach to Meeting Requirements** |
| --- | --- | --- | --- | --- |
| California SB 1386 Security of Non-encrypted Customer Information of 2003 (State of California) and progeny | Yes | See [Company Name]'s Information Security Policy. | No. All customer data is encrypted. | Not Applicable |
| The Californian Online Privacy Protection Act of 2004 | Yes | [Company Name] has a Privacy Notice on our website. We support DNT, our privacy notice covers all notice requirements under CalOPPA. [Company Name] ensures transparency and accountability in its use of PII. | Yes | [Company Name] has a Privacy Notice on our website. We support DNT, our privacy notice covers all notice requirements under CalOPPA. |
| California Consumer Privacy Act (CCPA) | Yes | To the extent that [Company Name] has PII belonging to CA residents, we will protect such PII in accordance with our Information Security Policies. | No | To the extent that [Company Name] has PII belonging to CA residents, we will protect such PII in accordance with our Information Security Policies. |
| Computer Fraud and Abuse Act (CFAA) of 1986 (FTC – Federal Trade Commission) | Yes | See [Company Name]'s Acceptable Use Policy. | Yes | Customers are contractually prohibited from using the services in violation of any law, see also [Company Name]'s Acceptable Use Policy attached to all contracts. |
| New York Data Security Law (Name: New York State Information Security Breach and Notification Act) | Yes | To the extent that [Company Name] has PII belonging to NY residents, we will protect such PII in accordance with our Information Security Policies and will notify the state AG in the event of a breach of such data. | No |  |
| 23 NYCRR 500 (NYCS) | Yes | To the extent that [Company Name] has PII belonging to NY residents, we will protect such PII in accordance with our Information Security Policies and will notify the state AG in the event of a breach of such data. | No |  |
| General Data Protection Regulation (GDPR) | Yes | In its role as a data controller, [Company Name] complies with the requirements of the GDPR. [Company Name] has appointed a DPO and our policies and procedures reflect our compliance efforts. | Yes | In its role as a data processor, [Company Name] complies with the requirements of the GDPR. [Company Name] has appointed a DPO and our policies and procedures reflect our compliance efforts. |
| GLBA |  |  |  |  |
| PCI DSS | No | [Company Name] has outsourced all PCI functions to PCI compliant 3rd parties. [Company Name] does not store, process, or transmit credit card data. | No |  |
| HIPAA | No | [Company Name] does not store patient health data. | No |  |
| Customer contractual requirements | No. Customers are data controllers. | Not Applicable | Yes | [Company Name] has implemented administrative, technical, physical, and organizational controls to protect customer data.  |

# Version History

| **Version** | **Date** | **Description** | **Author** | **Approved by** |
| --- | --- | --- | --- | --- |
| 1.0 | XX/XX/XXXX | Initial policy |  |  |
|  |  |  |  |  |
|  |  |  |  |  |