Our Privacy Objective

CyberGRX's privacy assessment streamlines third party cyber risk management by assessing privacy risk and prioritizing mitigation. Built from prominent privacy standards and regulations, the CyberGRX privacy assessment identifies multi-party compliance and information security gaps embedded in third-party relationships. The following captures CyberGRX's approach and terminology that define the privacy assessment.

Background & Initial Analysis:

We used the following 13 privacy regulations to develop the control families:

- GDPR
- Privacy Shield US-EU
- Privacy Shield US-Swiss
- HIPAA
- GLBA
- NYDFS
- CCPA
- Coppa
- CalOPPA
- EU Cookie Directive
- PIPEDA
- FIPPs
- NIST 80-53 Privacy Controls

Principles, Terms and Definitions

These terms commonly occur in the CyberGRX questionnaire.

TRANSPARENCY

The individual's right to know which of your personal data are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed.

OPENNESS

An organization shall make its policies and procedures about how it manages personal information readily available. When providing the information, it should be available in a form that's generally understandable.

FAIRNESS

An organization considers how the processing may affect the individuals concerned and can justify any adverse impact. Organizations do not deceive or mislead people when personal data is collected.

LAWFULNESS

Organization identifies an appropriate lawful basis for our processing. If an organization processes special category data or criminal offense data, conditions for processing this data are identified.

AVALABILITY

Data is "available" if it is accessible when needed by the organization or data subject. The General Data Protection Regulation (GDPR) requires that a business be able to ensure the availability of personal data and have the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incidents.

Data Specific Definitions:

SENSITIVE PERSONAL DATA

Generally, personal health data, financial data, credit worthiness data, student data, biometric data, personal information collected online from children under 13, and information that can be used to carry out identity theft or fraud are considered sensitive.

OPENNESS

The FTC now considers information that is linked or reasonably linkable to a specific individual, which could include IP addresses and device identifiers, as personal data.

The CCPA defines personal information as any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The definition specifically includes contact information, government IDs, biometrics, genetic data, location data, account numbers, education history, purchase history, online and device IDs, and search and browsing history and other online activities, if such information is linked or linkable with a particular consumer or household. Under the law, consumer is broadly defined as any resident of California.

In contrast, state breach notification laws and data security laws typically define personal information more narrowly focusing on more sensitive categories of information

DATA SUBJECT

Refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

CONSUMER

The CCPA defines "consumer" as "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations . . ., however identified, including by any unique identifier." According to the referenced state regulations, a California resident is any individual who is (1) "in the state of California for other than a temporary or transitory purpose," or (2) "domiciled in the state" of California and "outside of the state for a temporary or transitory purpose."

Notably, the CCPA does not define "consumer" in terms of an individual's relationship with a business. The act applies to every California resident, whether or not they are a customer of the covered business. Accordingly, employees of a business or a business's vendors could be consumers. The broad definition of "consumer" also serves to extend the CCPA's reach beyond state borders, as on its face it applies to California residents regardless of whether they are physically in the state.

The CyberGRX Privacy Control Group is:

A set of privacy-focused controls based on industry standards

A tool that can be used to assess the maturity and effectiveness of an organization's privacy controls

A tool that can be used to identify risks associated with an organization's privacy control implementation

These areas are covered in the privacy group within the Tier 1 CyberGRX assessment.

GOVERNANCE

- Enforcement/Redress
- General Policies and Procedures
- Incident Response Plan
- Individual Rights
- Audit Trail
- Privacy Authorization Policy and Procedures
- Recourse, Enforcement and Liability
- Risk Assessments
- Safeguards
- Security
- De-Identification
- Business Associate Contracts
- Integrity and confidentiality (security)
- Integrity/security
- De-Identification
- Challenging Compliance
- Integrity and confidentiality (security)
- Integrity/security

INTEGRITY and PURPOSE

- Data Integrity and Purpose Limitation
- Data minimization
- Accuracy
- Purpose limitation
- Purpose Specification
- Integrity and confidentiality (security)
- Integrity/security
- Identifying Purposes
- Authority to Collect
- Use and Disclosure
- Use Limitation
- Usage Restrictions of Personally Identifiable Information
- Storage limitation

ACCESS

- Access Privileges
- Access/Participation
- Individual Access

ACCOUNTABILILTY

- Accountability for Onward Transfer
- Accountability for Onward Transfer

CHOICE and CONSENT

- Sale and Marketing
- Choice/Consent
- Informed, specific, voluntary consent being received before cookies are used
- Consent
- Consumer rights/controls
- Authority to Collect
- Individual Rights
- The choice for users to opt-out
- Authority to Collect

Privacy Assessment Structure

DATA GOVERNANCE

Accountability

- Leadership and Oversight
- Risk Assessment
- Policies and Procedures
- Transparency
- Training & Awareness
- Monitoring & Verification
- Response & Enforcement

Responsibility, Collection, and Policy

- Data management
- Breach Response
- Communication Plan
- Response Plan
- Containment
- Analysis Plan
- Mitigation Plan
- Complaints Response Policy
- Continuous Improvement

DATA STORAGE AND MAINTENANCE

- Data Security
- Availability
- Confidentiality
- Integrity
- Anonymization
- Deification
- Pseudonymization
- Encryption
- Backup
- Data Mapping
- Data Tagging
- Data Destruction

DATA SUBJECT ACCESS AND MANAGEMENT

- Subject Access
- Right to be forgotten (Consumer Rights)
- Purpose of Processing
- Collection Limitations (Scope)

DATA PROCESSING

Records of processing

- Purpose of processing
- Name/Contact of Controller
  - Joint Controller
  - DPO
- Categories of data subjects
- Categories of Personal data
- Recipient of personal data
- Data Transfer
  - Documentation of Suitable Safeguards
- Consent & Consent Management
- Opt-in/Opt-out
- Use & Disclosure (Sale)
- Data Transfers
- Profiling
- Data Protection Impact Assessment
- Automated Processing
- Data Security
- Encryption in Transit

DATA PROCESSING (CONTINUED)

Organization's approach to accountability may include:

- 2 or less individuals solely responsible for organizational compliance with privacy and data protection principles
- 4 or more individuals responsible for organizational compliance with privacy and data protection principles
- Defined privacy processes, policies, and procedures with the ability to demonstrate compliance to internal and external requirements
- Organizational measures to demonstrate compliance
- Technological measure to demonstrate compliance

Examples of transparency and reporting in regards to privacy obligations

- Internal Reporting
- Self-attestation of compliance to Accountability requirements
- Internal Audit of Accountability requirements
- External Audit of Accountability requirements
- No reporting – we don't care about privacy

Lawfulness and Consent:

1. How to you obtain consent prior to collecting [personal data]?
2. What type of consent do you obtain prior to collecting [personal data]
3. What is communicated to the [data subjects] prior to obtaining consent?
4. How are [data subjects] informed of their rights while obtaining consent?
5. What rights do [data subjects] have?
    i. Purpose of processing
    ii. Duration of processing
    iii. Information regarding data transfers
    iv. Information regarding the security of personal data
    v. Right to erasure
    vi. Right to limit processing
    vii. Right to rectification
    viii. Right to withdraw consent
    ix. The existence/use of automated decision making/profiling.

Fairness in Data Processing

- Written policy documents
- Ensuring data is collected lawfully
- Data tagging
- Allowing [data subjects] to exercise their rights (i.e right to be forgotten, request copies of personal data, right to rectification)

For more information on the CyberGRX privacy objectives, please visit our website at:

www.CyberGRX.com

CyberGRX