Overview of CCPA and US Privacy Shield

June 2019

Privacy & data protection drivers

Why privacy and data protection is such a hot topic

REGULATIONS

New privacy and data protection laws and regulations (with teeth) are being drafted and going into effect in the US , EU, and across the world

DATA BREACHES & HACKS

Data breaches & hacks lead to adverse media attention, business disruption, customer trust erosion, goodwill and reputation loss, criminal and civil penalties and costs, complaints and lawsuits, and loss of revenues

INNOVATION

Implementations of Artificial Intelligence, Blockchain, Robotic Process Automation, Internet of Things etc. are bringing about new and different uses of personal data and privacy concerns

Recent changes to data breach and cybersecurity laws

And then there were 50…

April 2018

Arizona toughens data breach notification law. Expands definition of personal information to include biometric, health insurance & login data and private keys to authenticate records. 45 days breach notification deadline.

Arizona

Delaware

April 2018

Delaware broadens and toughens data breach notification law. 60 day breach notification deadline. One (1) year of credit monitoring similar to as CA and CT. Imposes new cybersecurity standards to implement reasonable information security measures on companies.

June 2018

Oregon broadens and toughens data breach notification law. 45 day breach notification deadline. One (1) year of credit monitoring similar to as CA and CT. Imposes new cybersecurity standards to implement reasonable information security measures on companies.

Oregon

South Dakota

July 2018

Becomes the 49th State to adopt a data breach notification law. 60 day breach notification deadline.

June 2018

Becomes 50th State. Includes requirements for an employee to coordinate security measures, identify risks, adopt and assess safeguards to address risks, retain service providers contractually required to maintain safeguards, evaluation of security measures for sensitive PII, and keeping board of directors and leadership informed.

Alabama

California Consumer Privacy Act (CCPA)

600 + State laws and counting…

The CCPA going into effect January 1, 2020, gives Californians the most sweeping, comprehensive and empowering consumer privacy rights in the country. The act sets requirements that regulates and attempts to limit the sale of personal information (PI). Applies to "for profit" businesses that:

- Annual revenues > $25M
- 50% annual revenues from sale of personal information
- Buy, sell, share PI of > 50,000 CA residents

PRIVATE RIGHT OF ACTION AND PER CAPITA FINES UPTO $750 PER RECORD

HIGHLIGHTS

Broad definition of PI includes identity, commercial, professional, electronic, behavioral, inferential, financial, transactional, biometric, and educational data

Enhanced disclosure obligations to consumers how and from whom PI is collected, used, shared, disclosed, or sold to

Enhanced consumer rights including:

1. Right to Know
2. Right to Access
3. Right to Data Portability
4. Right to Say No or Opt-out
5. Right to Equal Service
6. Right to Deletion

The GDPR

A framework to understand the requirements

PRINCIPLES

PRINCIPLES

- Fair, lawful, and transparent
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

DATA SUBJECT RIGHTS

RIGHTS OF THE DATA SUBJECT

- Right to Know
- Right to Access
- Right to Data Portability
- Right to Rectify
- Right to Restrictions
- Right to Object to Automated Decisions
- Right to be Forgotten

CONTROLLER OBLIGATIONS

CONTROLLER OBLIGATIONS

- Written records of processing
- Legal basis for processing
- Cross-border transfer mechanisms
- Transparent notices
- Freely given, specific, informed and unambiguous consent & withdrawal mechanisms
- Privacy by design and by default
- Privacy Impact Assessments (PIA) & Data Protection Impact Assessment (DPIA)
- Constraints and requirements for automated decisioning
- Security obligations
- Obligatory Data Protection Officer (DPO)
- Representatives
- Documented accountability mechanisms

PROCESSOR OBLIGATIONS (OPERATIONS AREAS)

OPERATIONS (PROCESSOR) AREAS

- Contract requirements
- Policies and procedures
- Written records of processing activities
- Technology
- Third-party risk management and vendor accountability
- Information security
- Website activity
- Information governance/records retention
- Breach notifications
- Data Protection Impact Assessment (DPIA)
- Data transfer mechanisms
- Data subject access requests intake, verification, and fulfilment

The CCPA

A framework to understand the requirements

PRINCIPLES

PRINCIPLES

- ~~Fair, lawful, and transparent~~
- ~~Purpose limitation~~
- ~~Data minimization~~
- ~~Accuracy~~
- ~~Storage limitation~~
- ~~Integrity and confidentiality~~
- ~~Accountability~~

CONTROLLER OBLIGATIONS

BUSINESS OBLIGATIONS

- ~~Written records of processing~~
- ~~Legal basis for processing~~
- ~~Cross-border transfer mechanisms~~
- Transparent notices
- ~~Freely given, specific, informed and unambiguous~~ Affirmative consent for children & withdrawal mechanisms
- ~~Privacy by design and by default~~
- ~~Privacy Impact Assessments (PIA) & Data Protection Impact Assessment (DPIA)~~
- ~~Constraints and requirements for automated decisioning~~
- ~~Security obligations~~
- ~~Obligatory Data Protection Officer (DPO)~~
- ~~Representatives~~
- Documented accountability mechanisms

DATA SUBJECT RIGHTS

RIGHTS OF THE DATA SUBJECT

- Right to Know
- Right to Access
- Right to Data Portability
- ~~Right to Rectify~~
- ~~Right to Restrictions~~
- ~~Right to Object to Automated Decisions~~
- Right to be Forgotten

PROCESSOR OBLIGATIONS (OPERATIONS AREAS)

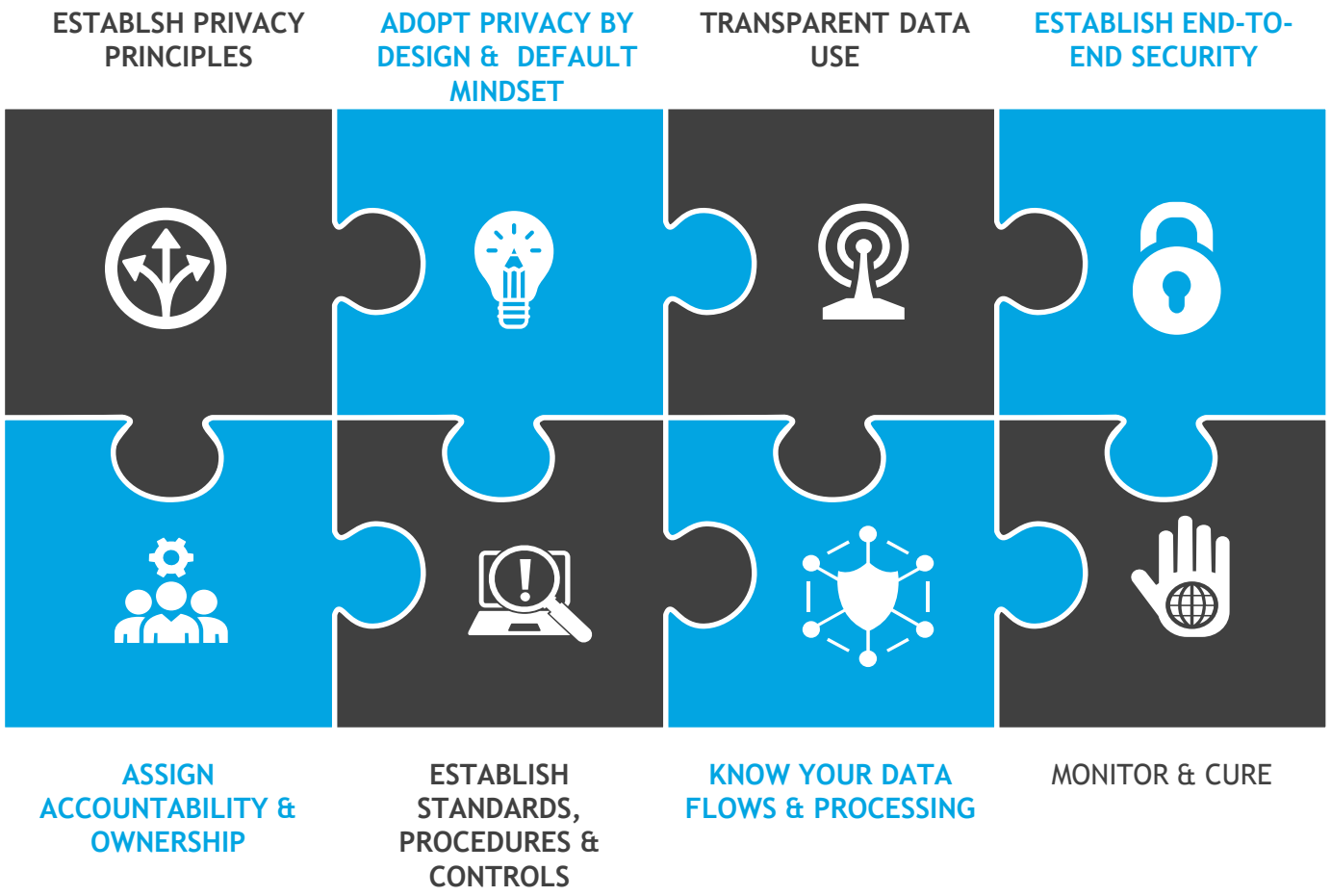
SERVICE PROVIDER AREAS

- Contract requirements
- Policies and procedures
- ~~Written records of processing activities~~
- Technology
- Third-party risk management and vendor accountability
- Information security
- Website activity
- ~~Information governance/records retention~~
- Breach notifications
- ~~Data Protection Impact Assessment (DPIA)~~
- ~~Data transfer mechanisms~~
- ~~Data subject access requests~~ Consumer rights assertion intake, verification, and fulfilment

Future-proofing your privacy program

How to comply

Adopt a framework (GAPP, Privacy Shield, ISO, ISACA or other) and organize the privacy program



BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 80,000 people working out of 1,600 offices across 162 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

www.bdo.com