CCPA vs GDPR Compliance

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It's primary aim is to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. GDPR also addresses the transfer of personal data outside the EU and EEA areas.

The California Consumer Privacy Act (CCPA) of 2018 aims to protect the personal information of consumers in California. Personal information is defined as anyting identifying, relating to, or associated with a consumer or a household. CCPA applies to entities that do business in California and meet at least one of the following: gross revenue over $25M; hold data of 50k or more California consumers, households or devices; derives 50% or more of annual revenue from selling PII.

CCPA vs GDPR Distinguishing Traits

	GDPR	CCPA
Scope	EU and EEA	USA/California
Data Impact Assessment Required?	Yes	No
Data Protection Officer Required?	Yes	No
Privacy Requirements?	Yes	Yes
Consumer Rights?	Yes	Yes
Data Collection Limits?	Yes	No
Steep Fines for Legal liability?	Yes	Yes
Verification required	No	Yes

CCPA vs GDPR COMPLIANCE CHECKLIST

GDPR Domains

- [ ] Have you done a data impact assessment?
- [ ] Do you have a designated data protection officer?
- [ ] Do you have the following security controls in place:
  - [ ] Asset & Vulnerability Management
  - [ ] Data Management
  - [ ] Logical Access
  - [ ] Physical Access
  - [ ] Risk Assessment
  - [ ] Policy Management
  - [ ] Third Party Management
  - [ ] Incident Management
- [ ] Do you have a rights management program?
- [ ] Do you have a privacy management program?
- [ ] Do you have breach notification procedures?
- [ ] Have you tested your breach notification procedures?

CCPA Domains

- [ ] Do you have reasonable security measures in place?
  - [ ] Asset & Vulnerability Management
  - [ ] Data Management
  - [ ] Logical Access
  - [ ] Physical Access
  - [ ] Risk Assessment
  - [ ] Policy Management
  - [ ] Third Party Management
  - [ ] Incident Management
- [ ] Do you verify the identity of petitioner?
- [ ] Do you ensure you are not storing data as part of the petitioner identification process?
- [ ] Do you have a privacy management program?
- [ ] Do you have a rights management program that includes:
  - [ ] The right to KNOW
  - [ ] The right to ACCESS
  - [ ] The right to DELETE
  - [ ] The right to OPT OUT
- [ ] Does your program provide annual notice updates?

ABOUT CONTROLCASE:

ControlCase is a global provider of technology-driven compliance and security solutions. ControlCase is committed to partnering with clients to develop strategic information security and compliance programs that are simplified, cost effective and comprehensive in both on-premise and cloud environments.

ControlCase provides the best experts, customer experience and technology for regulations including PCI DSS, GDPR, CCPA, SOC2, HIPAA, ISO 27001/2, CCPA, SWIFT, Microsoft SSPA, CSA STAR, SCA, PA DSS, PCI P2PE, PCI PIN, PCI 3DS, PCI Secure Software, PCI Secure SLC.

For more information email contact@controlcase.com www.controlcase.com