

PRIVACY READINESS ASSESSMENT

Evaluate Preparedness for Privacy Regulations

REGULATIONS ARE HERE

The clock has struck midnight with the new General Data Protection Regulation (GDPR), a law affecting any organization that processes or handles the information of European Union (EU) citizens. However, it has started ticking again for new privacy regulations such as the California Consumer Privacy Act (CCPA), Brazil's version of GDPR and more on the horizon.

Data privacy has moved from being a niche topic to something discussed in almost every corporation's boardroom. These regulations apply to any personal information, whether it belongs to a customer, an employee or other relationship with the organization.

With potential fines as high as 4% of global revenue for non-compliance, it is good business practice to proactively achieve compliance with current and future privacy laws.

PROACTIVE GUIDANCE

At **CRITICALSTART**, we know compliance failures can risk your organization's future revenues and reputation. That's why we're committed to helping your organization assess, identify and develop strategic roadmaps to fit your needs. Our Privacy Readiness Assessment seeks to identify key areas of risk in relation to privacy and information rights in preparation for current and upcoming data protection laws going into effect.

We can help assess your environment against privacy laws that affect you and provide guidance and remediation advice for any identified risks.

WHAT'S INCLUDED?

A clear understanding of your organization's ability to comply with current and upcoming regulations

A snapshot of status in relation to the privacy framework requirements

Identification of various locations of privacy data and how the information is used

Key risks of non-compliance and a roadmap to achieve compliance to the requirements

Understanding of how to continually monitor, measure and manage compliance to privacy framework requirements



KEY GDPR PRIVACY REQUIREMENTS

- Ensure GDPR compliance with these key capabilities and controls
- Obtain unambiguous consent from the user when collecting personal information
- Allow individuals to delete their personal information or request a copy of all personal information that a company possesses for that individual
- Appoint a Data Protection Officer (DPO) where necessary
- Provide breach notification to supervisory authorities (including data users) within 72 hours upon discovery
- Know where personal data is stored on your system, especially in unstructured formats in documents, presentations and spreadsheets.

COMPARISON WITH UPCOMING PRIVACY REQUIREMENTS (CCPA)

	GDPR	CCPA
Consent	Opt-in	Opt-out
Which entities are responsible?	Any organization capturing EU citizen's personal data	For profit organizations that process California citizen's data Along with one of the following: <ul style="list-style-type: none"> ▪ \$24M in revenue ▪ Hold over 50K unique records ▪ 50% of revenue from sale of personal data
Individual rights	Access to data Right to correct, erase, object to auto processing Right to notification upon data breach	GDPR rights plus Object to whom data is sold
Type of law	Regulation	Statutes added to Civil Code
Substantive provisions	99 Articles, most with several sub-articles	19 Sections, most with several (some with numerous) sub-sections

CONTACT US TODAY

To learn more about how **CRITICALSTART** can support your Privacy Readiness efforts, call **877.684.2077** or email info@criticalstart.com.

