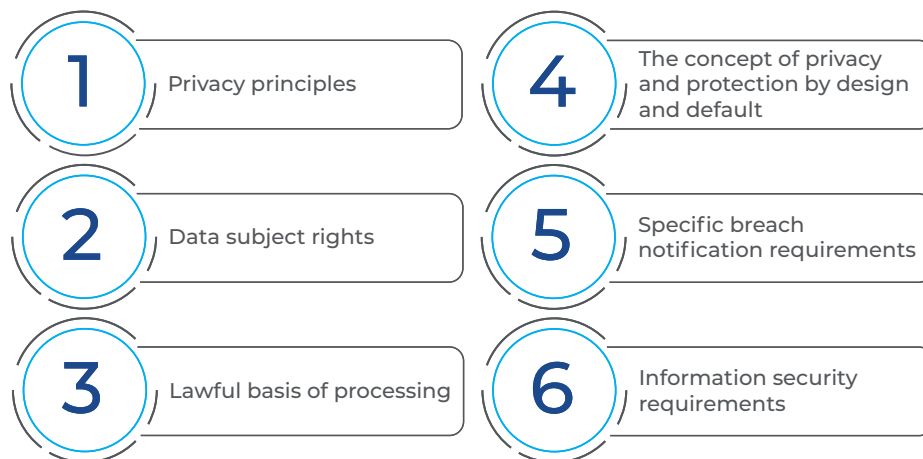


GDPR Readiness Checklist

What is the GDPR?

The General Data Protection Regulation (GDPR) is a comprehensive privacy regulations intended to strengthen data protection for individuals within European Union (EU) countries. The GDPR expands consumer rights surrounding the use of their data, places the responsibility of compliance on Controllers and Processors, spells out specific breach notification requirements, and sets large fines for non-compliance. The GDPR also provides one common regulation for all EU member states to follow. The GDPR applies to any organization that has a presence in the EU and is processing personal data of EU data subjects and organizations outside the EU that target EU data subjects to offer goods or services.

The goal of the GDPR is to provide more power and control to the people regarding how organizations collect and use their personal data. The regulation includes:

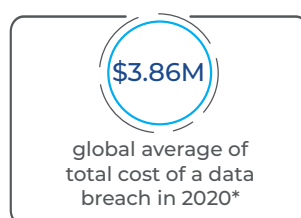


Why is it Important?

Information security is no longer tied to avoiding a breach, it is a requirement under the GDPR. Organizations must ensure personal information is collected for a disclosed and specific purpose to avoid large fines and public scrutiny over data handling practices. Fines for non-compliance can reach up to 4% of total global revenue or up to €20 Million, whichever is higher. And the impact to revenue surrounding the damage to an organization's public image and loss of consumer trust can be devastating.



4% or €20M
fines of up to 4% of total global revenue or €20M, whichever is higher



\$3.86M
global average of total cost of a data breach in 2020*

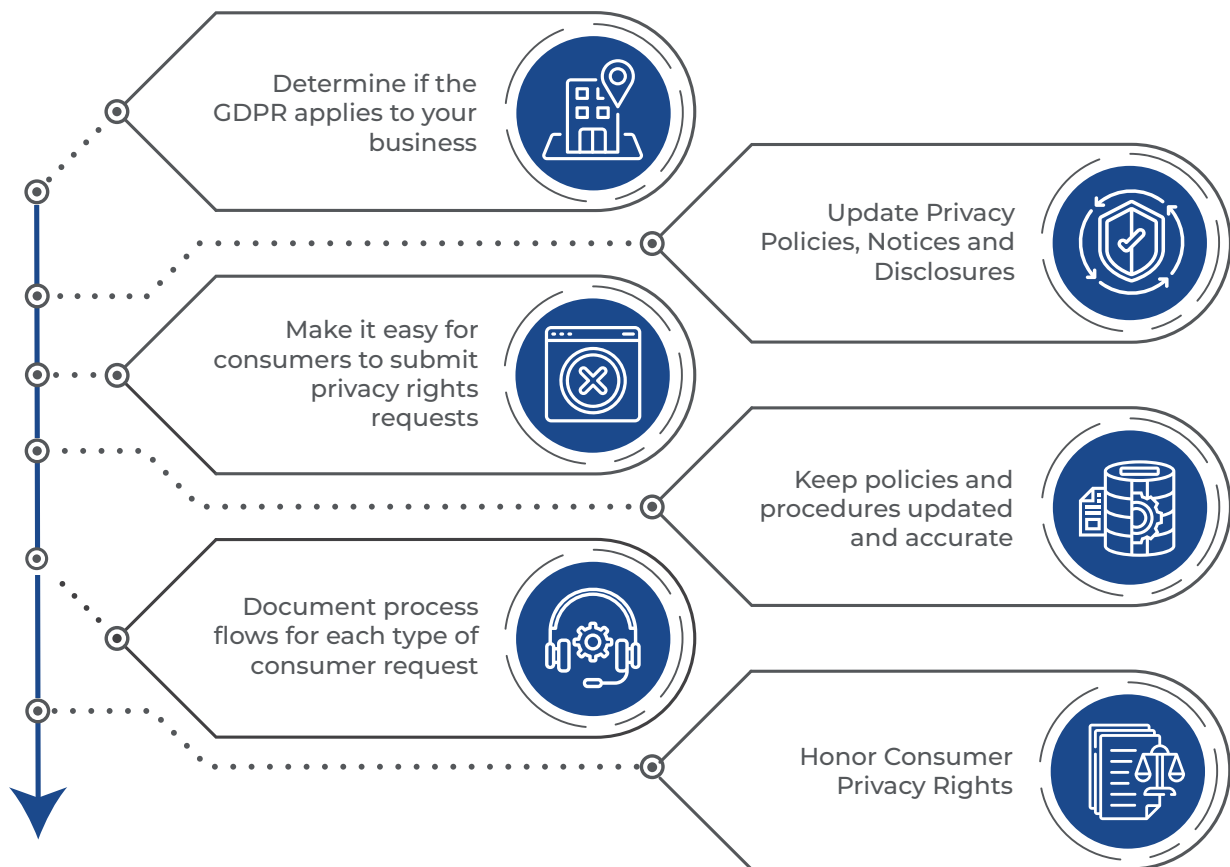
Mitigating risk in data privacy and with the GDPR involves the organization understanding the personal data they are processing, and ensuring they are honoring consumer privacy rights, making transparent notices available, and protecting personal information appropriately. By building and having processes around the GDPR requirements and a solid governance layer, an organization can reduce the likelihood of consumer complaints and the likelihood of a data breach, reducing risk of GDPR investigation or enforcement.

What Does it Mean to Be Compliant?

Demonstrating compliance with GDPR means that you have the appropriate privacy controls implemented to honor consumer rights, address proper disclosure requirements, and maintain records of processing. Implementing these requirements is most easily broken into 3 main areas: 1) Governance, 2) Operations and 3) Technology. Compliance with GDPR is complicated, with hundreds of regulatory requirements that could apply. To address all areas impacted by GDPR, create a cross-functional team that can reach across the entire organization. The applicable controls that could apply to an individual organization are beyond the scope of this document. We recommend you reach out to us at connect@compliancepoint.com to consult with one of our privacy experts and better understand how this regulation applies to your specific organization.

What Does the Compliance Process Look Like?

Organizations should begin their data privacy journey with a risk assessment to determine their obligations under the various privacy regulations as well as to establish their risk exposure and how their current controls measure up for compliance. Following the risk assessment, organizations will have a roadmap to work from. Further, the risk assessment will help establish priorities and assist in determining the level of input and workload for the cross-functional teams often needed to solve for GDPR.




GDPR Readiness Checklist

The checklist below can be used to determine your organization's GDPR compliance posture.

GDPR Readiness Checklist	Complete	Incomplete
Determine applicability		
Make sure someone in your organization is responsible for GDPR compliance		
Appoint a Data Protection Officer and EU Representative if required		
Determine the scope of the personal data you process through a Data Inventory exercise		
Document data flows and any sharing through a Data Mapping exercise		
Update your privacy policy and employee policies to include how personal data is processed and the legal justification for doing so		
Establish policies and procedures to honor data subjects' access, modify and delete requests		
Ensure appropriate technical and security controls are in place to protect data		
Establish policies and procedures to ensure data security and protection		
Update your Incident Response Plan to include notification of data breaches		
Update contracts with vendors to include third party processor requirements under the GDPR		
Implement approved data transfer mechanism(s)		
Train employees on obligations under the GDPR on at least an annual basis		

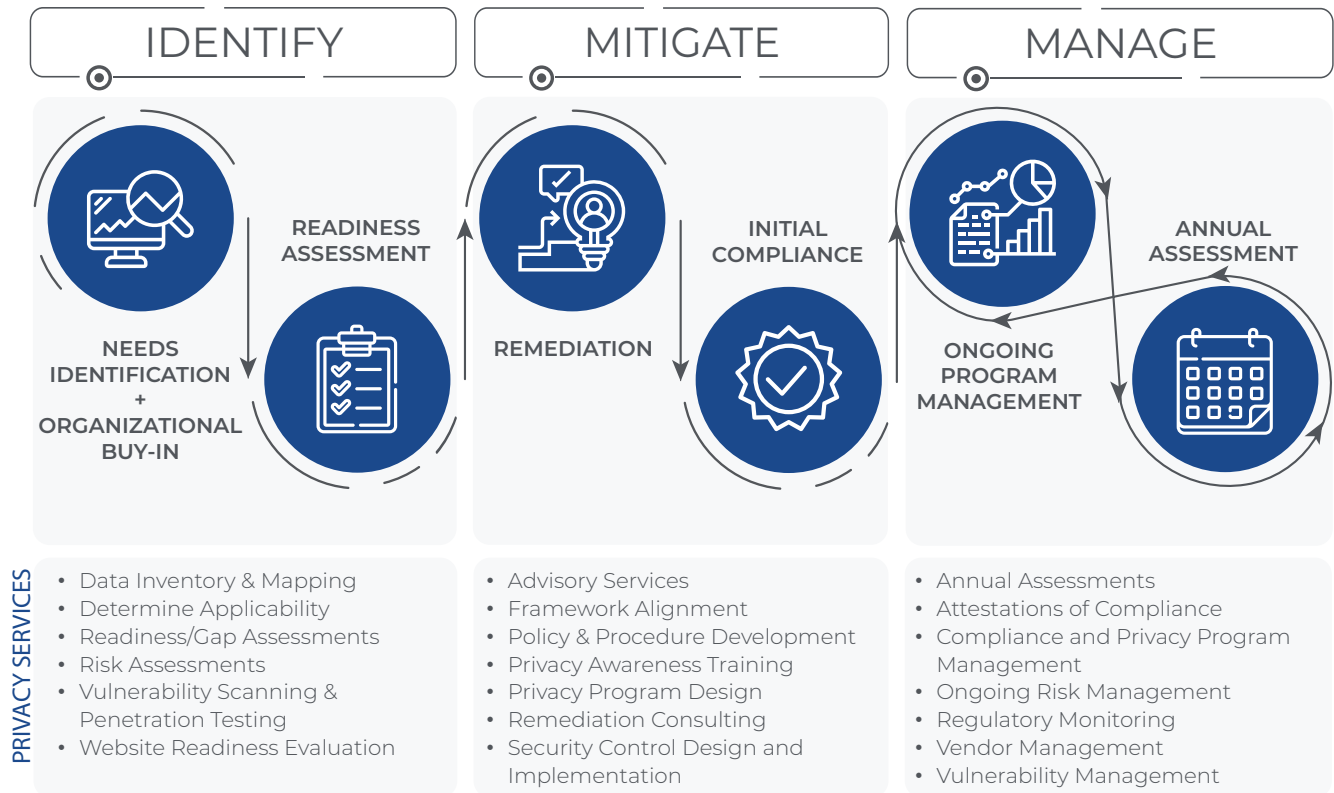
Got questions about your business?
Click here to [speak with a privacy expert!](#)

NEED HELP?

 Depending on the size of the organization, it may be necessary to designate a privacy department and appoint a Data Protection Officer

How CompliancePoint Can Help







CompliancePoint provides a full suite of services that help organizations manage and respond effectively to privacy requirements. Using our **IDENTIFY, MITIGATE + MANAGE** approach, we help organizations proactively identify their gaps, build out frameworks to meet compliance requirements and help manage long term programs to maintain this posture.



About CompliancePoint

CompliancePoint is a leading provider of risk management services focused on information security, data privacy, and compliance. Organizations face many risks associated with engaging their marketplace including how they process information internally and with whom they share information downstream. Our mission is to help our clients interact responsibly with their customers and the marketplace.

The difference is simple – data privacy, security and compliance have been at the core of our service offering for almost two decades. We provide our clients with a broad view of industry best practices and benchmarking that allows our customers to make informed business decisions, helping to minimize impact to business operations and maximize return on investment.

-  Business-centric approach
-  True practitioners with hands-on experience
-  Full lifecycle support
-  Over 2,500 companies assessed
-  Company-specific recommendations
-  Net Promoter Score (NPS) of 92 – our customers love us!

For more information about the GDPR or other privacy regulations and how they apply to your specific organization, contact us at connect@compliancepoint.com

* Ponemon Institute – Cost of a Data Breach Report (<https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>)

**CompliancePoint 2019 GDPR Survey (https://info.compliancepoint.com/hubfs/Surveys/CompliancePoint_2019-GDPR-Survey.pdf)