# Data Privacy

We assist organizations to meet current industry and organizational privacy goals. Our experience helps organizations futureproof against potential legal, regulatory, and market changes driven by ongoing pressure from consumers to protect their personal and sensitive information.

### Incident Response

Quickly respond to breaches with proven workflows and expertise.

### Incident Response Planning

Having a plan can help mitigate the costs associated with data incidents.

### Data Privacy Risk Assessment

Good data policy begins with understanding an organization's risk profile.

### Data Mapping

Locate all your data to understand the risks & build a response plan.

### Compliance & Privacy

Our consultants bring a comprehensive approach to compliance.

## An Evolving Landscape

The data privacy industry is rapidly growing and developing. Authorities are adopting and implementing new data protection and privacy laws, alongside the evolving corresponding regulations. These regulatory updates can disproportionately impact industries and business sectors according to the volume and sensitivity of the information they produce.

Organizations and users of personal or sensitive information experience difficulty maintaining the necessary actions to conform to the evolving data protection landscape. Compounding the difficulty of developing and implementing new compliance programs for data protection and privacy is a shortage of privacy professionals, with vendors only offering limited services that fulfill only a part of an organization's data privacy needs.

## Incident Response – Notification and data exposure analysis

Various data protection laws require notification for certain types of breached data, most commonly Personally Identifiable Information (PII) or Protected Health Information (PHI) for data based in the United States and Personal or Sensitive Information for data based in the European Union and other locations.

Once a data incident is known, organizations likely need to notify the affected individuals or data subjects that personal information was exposed.

Trustpoint.One Incident Response

## Our Approach

Trustpoint Cyber Services uses textual searches, metadata searches, and analytical tools to programmatically data mine the exposed information to determine a document review population. We collaborate with Counsel and Client to reduce the review population as much as reasonably possible, including segmenting parts of the review population for custom extraction workflows. We also engage Counsel and Client to draft a review protocol to govern our efforts in capturing the necessary information for the Client to meet their notification obligations in a cost and time-effective manner.

Once a review population and protocol are finalized, we engage a review team to manually extract necessary information from the documents, process any queued automated extraction documents, and generate a notification report.

The notification report is the final deliverable allowing Client's Counsel to perform their analysis and identify the individuals that ultimately will require notice per governing laws and regulations or require follow-up investigation.

Following the notification report, we also offer post review assessment based on exposure types, metadata of documents exposed, and other information learned during the manual review phase and provide guidance for exposure remediation, future mitigation, and aid the Client to comply with the changing privacy and data regulatory environment.

## Incident Response Plan

The first time an organization experiences a data security incident, it often reacts without a plan or tabletop practice. This can lead to unecessary employee stress, may result in dramatically increased costs, is most likely more damaging to the organization's reputation, and may result in ancillary data loss, continuation of the data breach, loss of customer trust, or abuse of resources.

Incident Response Plans help an organization respond quickly and uniformly to any type of external threat, including data security incidents. They ensure that responses are as effective and efficient as possible. Understandably, most organizations don't have the resources or know-how to begin making a proper IRP and to react appropriately to a data security incident. This is where experts are needed to help guide an organization in developing the proper approach in developing their IRP.

### Our Approach

We work with our clients to develop a customized Incident Response Plan, following industry standards such as the Incident Response Cycle. Once established, our experts will lead tabletop exercises with organization stakeholders and practice the plan, making sure the organization is ready to handle and act expeditiously to reported data security incidents when they arise.

## Data Mapping

Without understanding where data is located and what it is, organizations can't comply with certain data protection laws. They may also face legal problems outside of data protection laws if they don't understand what type of data they have and where it is- otherwise known as Data Mapping.

Not all Data Mapping is the same.  A data map is frequently included when an organization engages a vendor to perform a data assessment. The end-product is usually a basic list of files and network paths, devoid of any additional information other than location or custodian and without regard to the type of data or the possible ramifications of owning certain data. This style of data map leaves much to be desired, potentially failing to convey enough information for decision-making or creating a blind spot in the compliance scheme.

### Our Approach

Trustpoint Cyber Services offers a thorough approach to Data Mapping. Our privacy professionals leverage technology to help find personal & sensitive information and map it out accordingly, with actionable information. We also help determine the next steps once the Data Mapping exercise is complete.

## Compliance and Privacy Consulting:

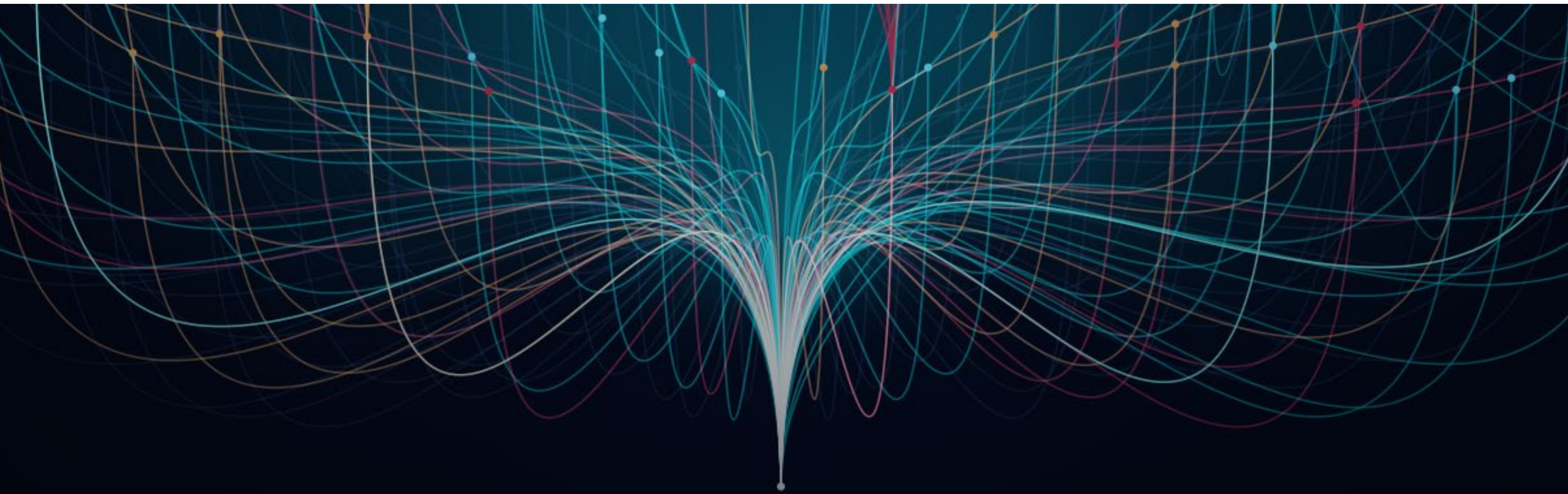
Data protection laws and regulations are ever-changing and more comprehensive, with rising monetary and reputational costs for privacy failures. Organizations need to assess what data protection laws apply to them and comply with seemingly moving regulation targets. Additionally, they need to take specific steps to comply with the existing General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), and other regulatory schemes domestically and globally.

**Our Approach**
Trustpoint Cyber Services privacy professionals bring an organization into compliance with data protection laws and regulations. Our consultants handle engagements focused on data privacy with a comprehensive to meet an organization's goals.

## Data Privacy Risk Assessment:

Many organizations don't know where to begin in assessing their risk profile when dealing with data privacy. If they hold any personal information, not just Personally Identifiable Information (PII), it's subject to data protection laws and regulations. Understanding the risk is a part of the analysis to inform the next steps to protect personal information.

**Our Approach**
Trustpoint Cyber Services leverages various Data Privacy Risk Assessment software and unique approaches. We help organizations determine their risk levels and consult on any needed actions to protect personal or sensitive information.



## Let's Talk

Our team of experts is here to walk you through any and all of your privacy & compliance questions: Reach us at cyberservices@trustpoint.one