GRC Illustrated

What are the elements of privacy risk management and compliance?

Organizations that handle personal information face increasingly complex challenges to effectively manage privacy risk and compliance. The impact of these challenges covers the entire information life cycle.

DEVELOPED BY

OCEG®

ERNST & YOUNG
Quality In Everything We Do

SUBJECTS

An individual, usually living, who is the subject of the personal information. We often call them customers, consumers, employees, and citizens. They are people.

CUSTOMERS

CITIZENS

DATA BROKERS

BUSINESS PARTNERS

EMPLOYEES

PARTNERS

What are they going to do with this data?

Can I trust them?

PRODUCTS AND SERVICES

COLLECT

Personal information is collected from a variety of sources – directly from the individual data subjects, from business partners, and from other parts of the information economy – nearly every time an individual interacts with the organization. The collection of personal information should be limited to what is needed.

ACCESS

NOTICE

CONSENT

Do we have a privacy statement?

Did we get consent if needed?

Are we collecting too much?

COLLECT

TRANSFER

Personal information is transferred to other parties to support the processing for the organization, or perhaps for other purposes entirely. Transfer should be made only to organizations that will protect the data and use it only as agreed.

Is this going offshore?

What are our risks? Can we trust them to use the data securely?

TRANSFER

LEGITIMACY

DATA

PURPOSE

JURISDICTION

Does our contract address privacy?

Are we allowed to transfer it?

GOVERNMENT AGENCIES

Any of the numerous organizations that interact with citizens, such as a tax authority, law enforcement, regulator, or social services. Often, transfers to Government Agencies are mandated by law or regulation.

PROCESSORS

A Processor is an entity that processes personal information on behalf of a Controller. A Processor may be performing a variety of services for the Controller, including hosting, aggregation, collection, retention, destruction, etc.

CONTROLLERS

A Controller is an entity who (either alone or jointly with others) determines the purposes for which and the manner in which any Personal Information is to be processed. They are in charge.

INFORMATION DISPOSAL

Information should be disposed of in a thoughtful way. Be sure that all hardware is properly wiped before tossing it in the trash. Ensure that backups and archives are included in the process.

Are our controls effective?

What are the leading practices?

Are we doing what we need to comply?

OVERSIGHT

How do we govern access?

I want all of this information locked down.

REGULATORS AND AUDITORS

How may I use the data?

CO-LOCATED AFFILIATE

OFFSHORE AFFILIATE

NEAR-SHORE AFFILIATE

COMPLIANCE ENVIRONMENT

CONTRACT

Do we have controls in place?

USE

Are we using the data as we said we would?

USE

Personal information is often used to fulfill a request from the individual (such as to provide a product or service), to perform research, and even to market other products and services to the individual. It should not be used for purposes not described in the privacy statement without the permission of the individual.

STORE

Personal information may be stored or retained by the organization in systems, databases, electronic media, and paper records. It should be stored for no longer than is necessary to maintain the business relationship with the individual, or as required by law or regulation.

STORE

How long will we keep it?

What will we do with it afterwards?

RECORDS MANAGEMENT

Records Management involves the maintenance of official business records. Personal Information related to customer transactions and accounts, marketing campaigns, customer relationship management, and human resources management also needs to be maintained for appropriate periods and securely disposed afterwards.

SECURITY

Securing the personal information requires numerous measures – including administrative, technical, and physical techniques – for the data when it is at rest and in motion. For example, the networks and operating systems need to be kept up to date and configured so they are not vulnerable to attack. Likewise, databases, laptops, and portable electronic media need to be protected, and communications between systems and between organizations need to be secured.

contact info@oceg.org for comments, reprints or licensing requests

XPLANATIONS™ by XPLANE® ©2007 OCEG®