Legal Data Intelligence

Data Breach Response

Updated: May 6, 2024

The actions taken by an organization following the discovery or suspicion of unauthorized access, disclosure, or loss of sensitive information, aimed at mitigating harm, complying with legal obligations, and restoring security and trust.

USE CASE IN PRACTICE

Data Breach Impact Assessment

Following a data breach, a school board engaged a Legal Data Intelligence leader to identify impacted data and compile a list of affected individuals. Leveraging AI and LDI practices to analyze intricate data belonging to students, faculty, and parents, the breach's scope was accurately assessed, enabling the school board to take necessary next steps.

PII Filtering for Review Management

After a company's email server was breached, exposing hundreds of thousands of emails, a Legal Data Intelligence leader leveraged AI to assess the compromised data. By ruling out personally identifiable information in over 90% of the emails, the review burden was effectively reduced to a manageable dataset.

MODEL WORKFLOW

Initiate

Scope Project and Set Goals

Some common goals include:

1) Gathering information sufficient to notify affected individuals whose personal information was impacted

2) Identifying the number of affected individuals by jurisdiction and the information types that were compromised for communication to privacy regulators

3) Identifying sensitive information not typically considered personal information, such as business confidential information and financial information of vendors

4) Identifying the plaintiff class for a proposed class action arising from the breach

Identify Potentially Compromised Data

Work with data forensics team to identify potentially impacted data

Upload Potentially Compromised Data

Once compromised data has been identified, upload to a review tool for assessment

How Technology Can Assist

Pulls data from sources into a platform for processing

Carry Out Initial Assessment

Identify groups of documents that are not likely to contain personal information (PI) or sensitive information

Identify key groupings of documents (the ""Review Set"") that are likely to be rich in personal information

How Technology Can Assist

Provides a variety of functionalities to conduct the initial assessment, including search terms, regular expressions, Boolean operators, AI, and analyses and categorization of document types, titles, sizes, and subject matter

Investigate

Search

Once the Review Set has been narrowed down, create search parameters depending on the specific types of PI, personal health information (PHI), and personal sensitive information (PSI) that are likely to appear in the data set

How Technology Can Assist

A variety of functionalities – ranging from search terms, regular expressions, Boolean operators, and AI – may be chosen to carry out this process.

Develop a Review Protocol

Develop a detailed protocol to maximize consistency, accuracy, and efficiency in the data analysis. At a minimum, the protocol should include:

1) A description of the affected organization's business and the types of data likely to be included in the Review Set

2) A detailed description of each type of personal information that should be recorded

3) Coding instructions

How Technology Can Assist

Identifies sample documents from the Review Set to provide as appendices to the Protocol to demonstrate the nature of the information reviewers are likely to come across and how to treat different information types

Review Data

Identify PI, PHI, and PSI and record the affected individuals

Associate the PI, PHI, and PSI to the affected individuals

How Technology Can Assist

AI enables the quick extraction of personal information and the association of entities (affected individuals) with linked PI, PHI, and PSI

Implement

Create a Notification List

Create a report containing the following information:

1) Those who are impacted including specific information about what types of information are implicated

2) The affected individuals for whom there is no contact information

3) Privacy regulators having jurisdiction over the affected individuals

How Technology Can Assist

AI tools populate the affected individuals in a column and all their associated PI traces in rows

AI easily normalizes duplicate records belonging to the same individual

Notify Individuals and Regulators

Inform affected individuals

Apprise privacy regulators with details on how many individuals were impacted, along with the types of information impacted in the breach

How Technology Can Assist

AI helps prevent duplicate notifications to the same affected individual and consolidates all notifications