PII TOOLS

Why You're Overpaying for Data Breach Responses

Technical whitepaper

PII TOOLS

Why You're Overpaying for Data Breach Responses

And How to Reduce Cost After the Alarm Goes Off

PII TOOLS

Introduction

It is no secret that data privacy regulations and software are playing a never-ending game of catch-up. And, unfortunately, they are trying to catch up to an exponentially growing and constantly evolving **datasphere set to jump up by** 200% by 2028. How can modern organizations possibly hope to keep up with the estimated **400 zettabytes of annual data generation**?

This white paper explores the unfortunate reality of what happens when even a small fraction of that overall data is breached, and how organizations are consistently overpaying in their response efforts.

It also details the most helpful solutions, including Person Cards®, an eDiscovery turning point that **automatically aggregates every instance of a data subject's information** in an easily employed and massively beneficial "report card".

Person Cards®

Why Data Breaches Happen

Data breaches are all too common. Within only a three-month period in 2024, it was estimated that 422 million data records **were leaked in data breaches**. How have we gotten to this point?

Data breaches happen for a variety of reasons, but the #1 factor might surprise you. **Human error is the leading cause of data breaches** worldwide. All too often, employees fall for phishing scams, bogus email requests, shady links,

or simply forget to log out of an important terminal, leaving the backdoor figuratively wide open.

Weak passwords, stolen devices, malware, ransomware, and more. Like a bucket overfilling with water, so much daily information generation can only lead to eventual data breaches. But just because they are commonplace, doesn't mean regulatory bodies take data breaches any less seriously.
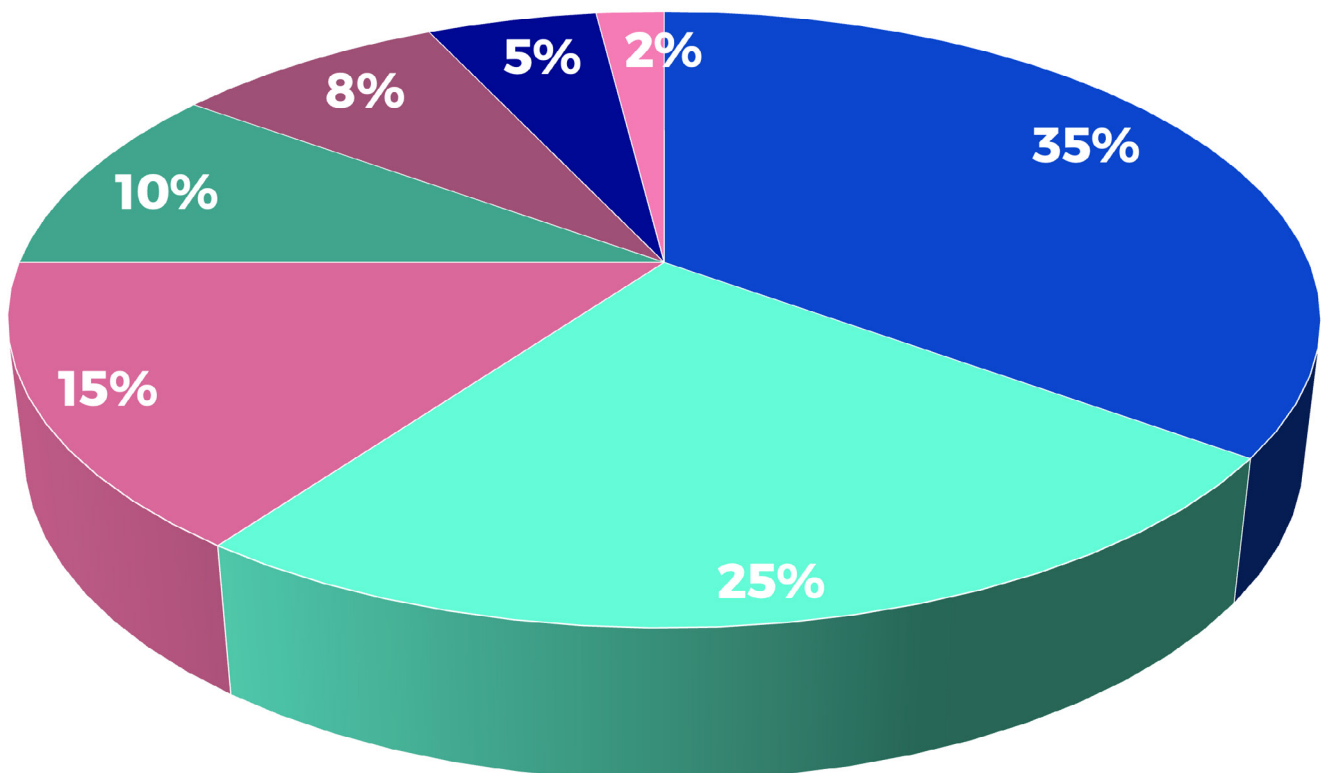
- Human Error / Mistakes — 35%
- Phishing & Social Engineering — 25%
- Malware / Ransomware — 15%
- Stolen / Lost Devices — 10%
- Misconfigured Systems / Cloud — 8%
- Insider Threat (malicious) — 5%
- Other — 2%

The Rise of Data Privacy Regulations

The world's first data privacy legislation actually dates back to the 1970s, when the German state of Hessia defined what was known then as "informational self-determination". But fast-forward 40 years, and the General Data Protection Regulation (GDPR) set the standard for information protection in the 21st century.

Since then, countries around the globe have introduced regulations that determine how organizations can gather, store, use, and transfer Personally Identifiable Information (PII). Some focus primarily on their region or country (CCPA, LGPD, etc.), while others deal with specific types of data (HIPAA, PCI DSS, etc.).

Just as each regulation lays out its own data protection framework, they also provide rules and repercussions for data breaches. For instance, the GDPR mandates that breached organizations **notify authorities within 72 hours,** while HIPAA affords a 60-day window.

But simply informing the relevant individuals and people affected about the breached data is not enough. Involved organizations will also have to dedicate a great amount of time and effort to the "clean-up" process. Not to mention the **potential fines reaching over €1 billion** in some noteworthy cases.

Global Data Privacy Regulation Comparison

Regulation	Country / Region	Focus	Breach Notification Deadline	Maximum Fine
GDPR	EU	General personal data	Within **72 hours**	€ 20 million or **4% of global annual revenue** (whichever is higher)
HIPAA	USA	Healthcare / PHI	Within **60 days**	$ 1.5 million **per violation category, per year**
CCPA	California	Consumer data	**No specific deadline**, but must notify "without unreasonable delay"	$2,500 per unintentional violation, $7,500 per intentional violation
LGPD	Brazil	General personal data	"In a **reasonable time**" (typically interpreted as days, not weeks)	Up to **2% of Brazilian revenue**, max BRL 50 million (~$10M USD)
PIPEDA	Canada	General personal data	As soon as feasible after breach is confirmed	No fixed maximum; enforcement by Privacy Commissioner (can lead to litigation)
PIPL	China	Broad personal data	**Promptly**, no fixed timeline	Up to **¥50 million** or **5% of annual revenue**
PDPA	Singapore	General personal data	As soon as practicable, within **3 calendar days**	Up to **SGD 1 million** or **10% of annual turnover** in Singapore
POPIA	South Africa	Consumer employee data	As soon as reasonably possible	Up to **ZAR 10 million** or criminal liability

The Expensive Problem with Breach Investigations

There is a lot that goes into resolving a data breach, everything from the initial identification of the problem to ensuring it never happens again. And in between those two steps, we have the **costly discovery phase**.

If an organization suffers a data breach, it first needs to:

1. Locate the affected data;
2. Determine whether that compromised data holds PII.

In other words, if 100 company emails are leaked, how many of those emails include person names or addresses or even talk about a patient's medical history? And the only way to figure that out is to individually review every email. Now, multiply this scenario by 10,000, 100,000, or even +1 million.

Organizations are often forced to turn to "breach investigation experts", or lawyers with set prices per examined document, by the hour, or some other metric. It is been estimated that **most companies charge approx. €1 per document**, so it is in the organization's best interest to limit the amount of GB under investigation. On the contrary, the investigator will strive to review as much data as possible to maximize profits.

PII Tools Pays for Itself — and Then Some.

Automated discovery, built-in compliance, and faster response times save our customers more than €150,000 in the first 3 years.

Year	Compliance savings	Audit savings	Time saved	Breach response	Total
1	€ 15,000	€ 10,000	€ 8,000	€ 7,000	€ 40,000
2	€ 20,000	€ 12,000	€ 9,000	€ 10,000	€ 51,000
3	€ 25,000	€ 14,000	€ 10,000	€ 12,000	€ 61,000
Total 3-Year Savings: € 152,000					

Based on estimated time, compliance, and legal savings modeled from typical mid-size organizations handling sensitive data under GDPR, HIPAA, or PCI DSS.

It is at this point that organizations suffering a data breach reach a proverbial balance act between **reducing the amount of data being reviewed** while also **ensuring zero affected information** slips through the cracks. So, what are their options?

Avoiding False Positives with Data Discovery Tools

For a standard data breach dealing with corporate emails, only between **10-20% of documents** actually contain a reportable form of PII. However, many breach investigators will insist on reviewing upwards of **50-70% of documents**, meaning potentially hundreds of GB of data go needlessly under the microscope, leaving the affected organization (and its insurer) to foot the bill.

The best way to avoid this expensive scenario is to deploy a data discovery tool that **automatically scans the affected data for reportable PII.** Using sophisticated machine learning and discovery algorithms, such software is specially positioned to flag PII where it stands while removing uncompromised data from the pool.

But not all data discovery tools are created equal. Some have a much harder time telling the difference between reportable PII and an email signature featuring a non-PII name, for example. This is what is known as a **"false positive"**. The system flags an email as containing PII simply because it features a well-known brand name, sports team, product title, etc. And that document then goes under human review, where it is cleared instantly, despite costing the same as its actually problematic counterpart.

Standard Tools
Documents flagged: 70%

Actual PII present: 15%

PII Tools:
Documents flagged: 15%

Actual PII present: 15%

Smart filtering cuts review size by 3–5x — and costs even more.

Choosing the Right Data Discovery Tool

The benefit of using the right data discovery tool is two-fold:

1. Avoid data breaches before they happen;
2. React quickly and efficiently to data breaches.

The best way to deal with data breaches is to avoid them altogether. PII Tools is sensitive data discovery software that deploys a fast and accurate **on-prem solution to automatically scan data BEFORE it ever reaches an organization's storages.** It allows users to perform regular in-house audits while also being specifically tailored to help reach compliance with all major data privacy regulations worldwide.

**Replace days of billable hours with one scan.
PII Tools automates the hard part.**

Manual Review
Identify data
Manually open + read docs
Tag PII
Bill hours
Legal review
Final summary

With PII Tools
Scan data → auto-detect PII
Generate report
Review edge cases only
Done

Must-Have Feature: Person Cards®

PII Tools also offers a highly specialized and completely unique tool: Person Cards®. Built with legal and forensics teams in mind, this feature allows users to **automatically link up all forms of PII discovered by its AI detectors for each individual person**. It then takes that data subject's information, ranging from their name, email, DOB, credit card information, both structured and unstructured data, files, emails, databases, and more, and generates an easy-to-read, easy-to-export Person Cards®.

This marks a considerable leap forward in data breach response and breach investigation processes. Person Cards® also **streamlines importing the gathered data into helpful eDiscovery platforms** like Relativity and others. And, of course, unassigned PII (considered 'non-risk') is also included in each Person Card®, providing that extra assurance with additional quality control options.

And Person Cards® come in handy in non-urgent instances, too. The ability to automatically aggregate an individual's relevant data makes **DSAR requests a matter of seconds instead of a time-consuming obstacle.**

PII TOOLS

A Better and More Cost-Effective Data Breach Response

The best kind of data breach is one that never happens. Even despite one's best efforts, however, humans can still make mistakes, and data breaches are never 100% off the table. That is why PII Tools provides instant insights during the investigation process, **effectively streamlining the response and recovery phase with automated scanning and reporting, backed by effective manual review options to boot.**

Analyze millions of breached files or emails for all forms of PII in seconds, generate detailed, interactive reports, and then use them to take actionable steps to prevent data breaches from happening again in the future.

Data breaches cause an array of problems. Substantial cleanup costs, a loss in company reputation, potential regulatory fines, and more. If you want to avoid this critical issue from ever arising, then visit the **PII Tools Data Discovery** homepage to learn how you can secure your data storages before it's too late. Or if you are already dealing with a data breach, then avoid the overpriced breach investigators and resolve the issue on your own with PII Tools' Person Cards® as part of the same software.

PII TOOLS

About PII Tools

Our mission

The mission of PII Tools is to bring modern automation technology into the world of data privacy.

We equip infosec, legal and data protection teams with accurate and easy-to-use software for discovery and remediation of sensitive data.

What PII Tools brings to the game is clarity and quality, both in technology and in the business model. Our context-aware PII detectors come from years of cutting edge research into Artificial Intelligence.

Why did we start PII Tools?

- Clarity and honesty. AI is quickly becoming a vacuous buzzword. As an AI-first company and world-leading PhD experts in machine learning, we think the cyber security world deserves better.

- Focus on technology. Intelligent automation doesn't have to be a marketing after-thought. We bring over a decade of research excellence, award-winning open source software used by thousands of companies world-wide, and over a thousand peer-reviewed citations.

- Passion for pragmatic solutions. With a strong background in IT services, we know how to listen to customers and combine quality engineering with cutting edge research.

Our history

- **MARCH 2010**
  First public release of Gensim, our open source NLP software.

- **MAY 2014**
  Incorporated UK office in Bristol, UK

- **OCTOBER 2015**
  Launch of corporate Machine Learning and NLP trainings

- **JANUARY 2017**
  Office opening in Brno, CZ

- **JANUARY 2018**
  Launch of PII Tools

- **AUGUST 2024**
  PII Tools redeveloped and sold by PII Tools Limited, a Cyprus company

- **NOW**
  Serving customers

Contact us

Email:
info@pii-tools.com

Website:
https://pii-tools.com

Address:
25 Spyrou Araouzou, Berengaria 25, 3036 Limassol, Cyprus