VOTIRO

GUIDE

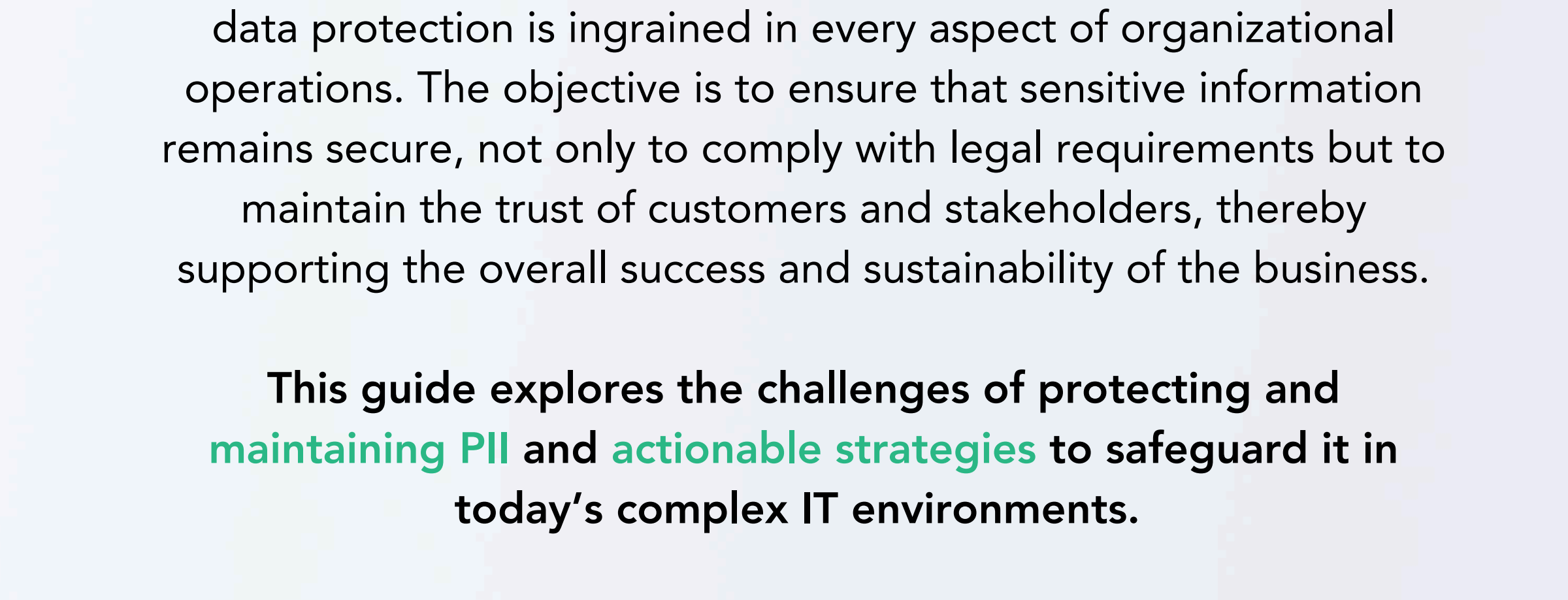
Safeguarding Data for Modern Enterprises

Ensuring **Private Data Protection** & Compliance

Data security isn’t just about breach prevention, it’s about safeguarding sensitive data. As companies accumulate vast amounts of data, including customers’ personally identifiable information (PII) and proprietary business secrets, the focus shifts to implementing robust protection strategies. This involves deploying advanced technical measures such as encryption and access controls while fostering a culture of security awareness among employees.

More than that, it’s about creating a resilient environment where data protection is ingrained in every aspect of organizational operations. The objective is to ensure that sensitive information remains secure, not only to comply with legal requirements but to maintain the trust of customers and stakeholders, thereby supporting the overall success and sustainability of the business.

This guide explores the challenges of protecting and maintaining PII and actionable strategies to safeguard it in today’s complex IT environments.



VOTIRO

The Guide to Personal Identifiable Information (PII)

Straight from the Experts

> In 2023, more than 52 percent of all data breach incidents in global organizations involved customer personal identifiable information (PII), thus making it the most frequently breached type of data."
>
> — Statista

> "In 2023, the average cost per record involved in a data breach was USD 165, a small increase from the 2022 average.
>
> — IBM Report, 2023

What is PII?

Any data identifying an individual directly or indirectly is considered PII. Direct identifiers are explicit details that directly map back to an individual with little effort, such as social security and passport numbers. Indirect identifiers take more effort to map back to an individual, combining data like birth dates and zip codes. Either one taken independently is unlikely to correlate to an individual, but together, they narrow the possibilities enough to make unique identification possible.

When looking at PII, it is essential to distinguish between sensitive PII, which, if disclosed, could harm the individual (e.g., medical records), and non-sensitive PII, which poses less risk (e.g., names). Numerous laws and regulations oversee and define how PII needs to be protected, depending on the data's location, jurisdiction, and origin.

> **"By 2024, modern privacy regulation will blanket the majority of consumer data..."**
>
> — Gartner Security Summit, 2023

PII Can Be a Combination

Indirect PII is the trickiest to discover and manage because it comprises multiple seemingly unrelated data points. However, some well-known correlations, such as birth year and zip code can rapidly narrow down possibilities. Others are more complex, such as Gender, Profession, and Workplace Location, which would allow narrowing down specific individuals in a field.

Similarly, the combination of Race, Educational Institution, and Graduation Year may be used to identify former students from less diverse institutions or specific programs. Techniques such as anonymization and pseudonymization remove the data values or pieces, making it harder to correlate back to individuals.

PII is Universal

How PII is managed and protected varies globally, reflecting cultural norms and legal requirements. For example, the GDPR imposes hefty fines and provides broad privacy rights, including the right to be forgotten, influencing how data is handled in Europe and in any business interacting with European citizens. Other countries have developed their own data protection laws, like Japan's APPI and Brazil's LGPD, which share similarities with GDPR but also contain local nuances.

PII concerns also exist across multiple business sectors and not just in healthcare. For instance, in the finance sector, PII is crucial for managing customer accounts and transactions, safeguarded under frameworks like PCI-DSS, which protects credit card information. In education, student records containing PII are protected under laws like FERPA in the United States. Similarly, workplaces handle PII with regulations such as GDPR.

Why Protecting PII Matters

For many organizations, protecting PII only comes down to a financial decision. They view the direct costs associated with a breach in terms of the cost of litigation from affected individuals, hefty fines from regulatory bodies, and expenses incurred from rectifying breaches. However, this is only part of the picture and not always the most impactful to a business's bottom line.

Consumers have become far more concerned with data privacy and how organizations protect their personal data. Failures to protect PII data undermine the trust customers place in a business and impact their willingness to do further business. Data has shown that **66% of customers** no longer trust a company after a breach, often taking their business elsewhere in the future or avoiding starting any new business with the affected organization.

PII for **Healthcare**

For U.S. healthcare organizations, PII concerns often focus on meeting HIPAA regulations. HIPAA sets rigorous standards for using and protecting PII, emphasizing confidentiality, security, and the necessity for thorough training and awareness among healthcare professionals. HIPAA not only imposes strict compliance requirements but also severe penalties for non-compliance. These penalties can include fines of up to $50,000 per violation with a potential annual maximum of $1.5 million.

For the most egregious violations, HIPAA may mandate a Corrective Action Plan (CAP), which enforces specific fixes with strict timelines, significantly increasing the financial and operational impact on the organization. Rather than slowly planning the best-fit vendor with the most competitive pricing, those under a CAP have a limited timeline to produce solutions, and the need for speed comes with additional costs.

HIPAA security measures include, but are not limited to:

- Implementing a security management process around electronic protected health information (ePHI)
- Implementing procedures to guard against and detect malicious software
- Training users on malicious software protection
- Implementing access controls to limit access to ePHI to only those persons or software requiring access.

— Office for Civil Rights

PII for **GDPR**

One of the most aggressive regulations protecting PII is the General Data Protection Regulation (GDPR). This regulation sets the standards across the E.U. on consumer privacy, granting them extensive rights over their data, such as access, erasure, and portability. Organizations fully complying with GDPR need to start from the design phase, incorporating data protection principles into their processing activities and business practices.

GDPR, unlike many regulations, has a global reach, impacting any entity handling E.U. residents' data, and imposes severe penalties for non-compliance — up to €20 million or 4% of the annual global turnover, whichever is higher. These aggressive fines have made GDPR a focus of many organizations, mapping their data protections around it as a standard because it thoroughly exceeds the requirements of many others.

The rights of personal data owners with GDPR:

- The right to be forgotten
- The right to data portability
- The right to be informed, e.g., in case of a data breach, or to receive an explanation in machine learning systems' automated decision making

— Smarter with Gartner, 2018

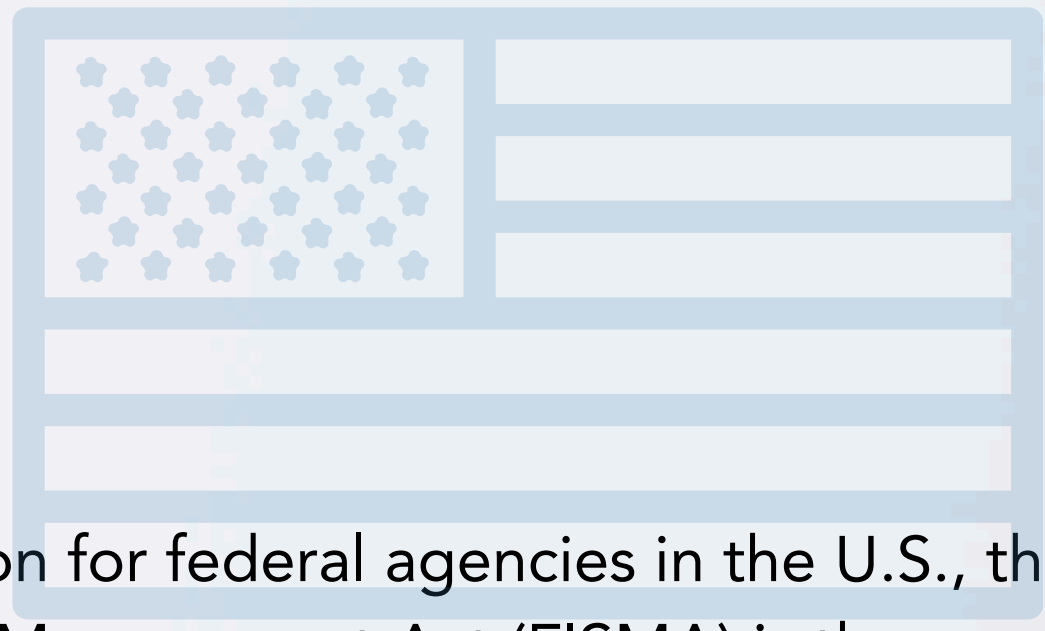
PII for CCPA

Similar to GDPR, the California Consumer Privacy Act (CCPA) also focuses on consumer rights, but it is limited to those of California residents. It promotes transparency in how businesses handle personal information. CCPA mandates that organizations disclose their data collection and management practices, empowering consumers with significant control over their personal data, including the rights to access, delete, and opt out of the sale of their information.

This regulation impacts any business operating within California, setting a precedent for other states. Non-compliance is much less than GDPR, leading to fines of up to $7,500 per intentional violation and $2,500 for unintentional breaches, underscoring the importance of robust data management practices.

> Businesses that are subject to the CCPA have several responsibilities, including responding to consumer requests to exercise these rights and giving consumers certain notices explaining their privacy practices.
>
> — California Department of Justice

PII for FISMA



For those handling information for federal agencies in the U.S., the Federal Information Security Management Act (FISMA) is the primary law to comply with. FISMA protects government information, operations, and assets from natural and man-made threats. It mandates that federal agencies implement a comprehensive risk management framework to safeguard PII and other sensitive data.

FISMA mandates numerous security controls to protect data at all stages of its lifecycle. It covers everything from access controls and authentication to data security monitoring to ensure that federal data and assets are continuously protected against potential threats.

While FISMA does not have a standardized fine structure, non-compliance can result in budget cuts, censure, or other significant organizational penalties. For organizations relying on federal contracts, failures to comply with FISMA can eliminate lucrative funding, significantly damaging their operations.

> [FISMA] requires agencies to report major information security incidents as well as data breaches to Congress as they occur. — CISA

PII for PIPEDA

Even Canada has a specific regulation to protect PII in the Personal Information Protection and Electronic Documents Act (PIPEDA). This act focuses on consumer consent and ensuring the fair handling of personal information. It does this by holding organizations accountable for the personal information they manage, demanding compliance in how this data is treated, especially concerning cross-border data flow.

The act outlines specific obligations for the safe transfer of PII between Canada and other countries and imposes fines of up to CAD 100,000 for each violation.

PII for **PIPL**

As PII protection is genuinely a global interest, China has its own comprehensive data privacy regulation in the Personal Information Protection Law (PIPL). This regulation came into effect in 2021, mirroring many aspects of the GDPR by establishing strict guidelines for personal data processing and granting individuals significant rights over their data. PIPL mandates explicit consent for data collection and requires that organizations handle personal information responsibly, with specific provisions for data security and cross-border data transfers.

With PIPL, the penalties for non-compliance can be severe. Organizations violating PIPL may face fines of up to 50 million yuan or up to 5% of the previous year's turnover. Additionally, responsible personnel can face personal penalties, including fines and restrictions on their future employment in directorial or executive roles.

PII for PDPA

Singapore has its own privacy act for PII, which balances the needs of businesses to collect and use personal data against individuals' rights to privacy. The Personal Data Protection Act (PDPA) sets comprehensive standards and guidelines for organizations' personal data collection, use, and disclosure. It also includes a national Do Not Call (DNC) registry that allows individuals to opt out of receiving marketing communications. These measures cover electronic and non-electronic data, ensuring broad and inclusive protections under the Act.

Non-compliance with the PDPA carries significant consequences, including financial penalties that can be substantial enough to incentivize compliance. The Personal Data Protection Commission (PDPC), the regulatory authority enforcing the PDPA, can issue fines and direct organizations to take corrective actions. These penalties are designed to address various forms of non-compliance, from unauthorized use of personal data to failures in protecting data against security breaches.

PII for **APPs**

Australia's Privacy Principles (APPs) date back to the Privacy Act of 1988, forming the cornerstone of the privacy protection framework, which oversees how personal data is handled within Australia. These principles dictate requirements for the open and transparent management of personal information, ensuring entities maintain clear privacy policies and conduct personal information handling in a secure and accountable manner. They cover various aspects such as the collection, use, and disclosure of personal information, consent, data security, and the rights of individuals to access and correct their information.

Non-compliance can lead to significant consequences, enforced by the Office of the Australian Information Commissioner (OAIC). Entities that fail to adhere to these principles may face regulatory actions, including audits and substantial fines. These fines are similar to GDPR, with the maximum penalties including a fine of up to $50M, three times the value of any benefit obtained through the misuse of information, or 30% of a company's adjusted turnover in the relevant period, whichever is greater.

> APPs continues to evolve, with the Privacy Legislation Amendment Act 2022 enhancing the OAIC's ability to regulate in line with community expectations and protect Australians' privacy in the digital environment. — OAIC

The Current State of PII Protection

When protecting PII, there is no one-size-fits-all security control for every organization. Rather than any specific fix, organizations often employ a selection of controls to detect data, restrict access, and prevent it from being stolen. Despite creating a strong foundation, cybercriminals attempting to access and steal sensitive data keep improving their game, finding new ways to bypass security controls and trick employees into accidentally turning over data.

Encryption

One of the first controls that organizations focus on when protecting sensitive data is encryption. Encryption converts data into a coded format, accessible only through a corresponding decryption key. This process ensures that even if data is intercepted or accessed by unauthorized individuals, it remains unreadable and secure.

Encryption controls are frequently used for data at rest, encrypting entire files for unstructured data or individual fields inside structured data like a database. Used in this way, if an attacker steals the data, it remains unusable without the encryption key, creating a safe harbor defense for many privacy regulations.

Encryption is also used in transit to protect data from being intercepted between systems, which is especially important for cloud or web-based storage as it protects users from having their info intercepted or altered en route. Effectively leveraging encryption requires secure key management to ensure the decryption keys do not fall into the wrong hands.

As you can see, encryption is not a perfect solution as it also introduces risk. Not only can anyone possessing the decryption keys access or modify the data, those already with access can exfiltrate the un-encrypted data and share it as they please, making the act of encryption redundant.

Access Controls

Many organizations focus on access controls to limit access to sensitive info. These controls build on strong authentication restrictions using passwords, biometric scans, tokens, or other forms of multi-factor authentication (MFA), which verify the identity of individuals trying to access various data.

Once users are verified, additional access controls check the authorization levels of individual users. The least advanced versions of this restrict access to members of an organization, while more advanced versions scope access to only what is necessary for users to complete their job, following the principle of least privilege. Strategically limiting access helps limit the risk of unauthorized disclosure, alteration, or destruction of sensitive data.

These controls also come with significant challenges in operations. Attackers frequently exploit weak authentication mechanisms that allow short passwords, reused credentials, or lack MFA. Also, once attackers have achieved access, weak access controls enable attackers to pivot deep within storage, accessing sensitive data.

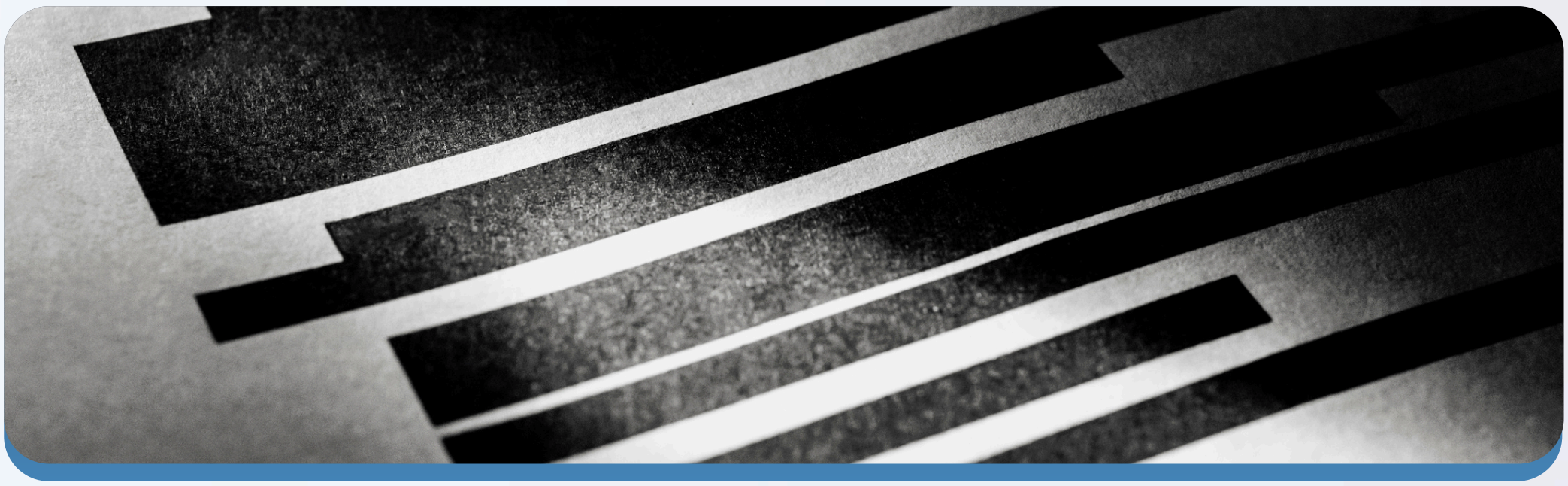
Maintaining appropriate access controls to prevent this is challenging because users are not static and may change roles and projects over time, altering what is appropriate for them to access.

Improving PII Protection

One of the most significant challenges for organizations in protecting PII comes from the technologies that make them more productive. Cloud technologies and collaboration tools have become foundational for organizations in accelerating development and collaborating across geographically diverse locations. These tools transcend traditional security boundaries and controls, making steps to protect PII less effective. Data can easily be transferred and copied—into texts, emails, or documents—making tracking and securing PII outside traditional IT environments challenging.

Protections fall back to access controls, yet attackers with compromised accounts can appear as legitimate users, bypassing initial access restrictions and gaining unfettered access to sensitive data. **Protecting data in these new environments requires a shift from traditional thinking.**

Obscuring PII



Organizations increasingly turn to methods like dynamic redaction and **masking** to adapt to this new environment, allowing them to protect PII while maintaining its utility. Dynamic redaction works by obscuring or removing sensitive information from documents or data sets in real time, adapting based on the context, user permissions, or specific viewing conditions. This automated process ensures that PII is only accessible when necessary and is particularly useful in dynamic environments where access needs to be tightly controlled.

Similarly, masking techniques further enhance privacy by transforming sensitive data in a way that **maintains its operational integrity**. Substitution replaces real data with realistic but fictional alternatives, anonymization removes identifiers linking data to individuals, and tokenization replaces sensitive data with non-sensitive tokens.

Using these techniques allows organizations to use and share data for analysis or operational purposes without risking the exposure of sensitive information.

Blocking PII

Some organizations take a less surgical approach and aim to block or disarm PII from leaving organizational boundaries. Organizations can monitor and control data transfers using Data Loss Prevention (DLP) tools, ensuring sensitive information does not leave the secured environment. Restricted access and egress controls limit data availability to authorized personnel, while real-time blocking mechanisms quickly respond to unauthorized data movements.

While effective for stopping data exfiltration, these tools often fall short of balancing security with productivity. Overly restrictive **DLP measures can hinder operational efficiency**, preventing users from leveraging the data they need when and where they need it, impacting business productivity.

Comparing Solutions

When comparing data protection strategies such as dynamic redaction, data masking, and blocking or disarming, it is essential to understand their optimal applications and limitations. Each method has its strategic use, and choosing the right one depends on the specific data security needs of the organization.

Dynamic redaction is highly effective in real-time environments like online services or document-sharing platforms, where it can selectively hide sensitive information based on user roles and permissions. Dynamic redaction is also contextual aware, meaning it doesn’t just redact sensitive info in motion, but also based on the context in which the data is being used - whether that’s identity, environmental, or by application.

Data masking is more suited for scenarios like software testing and analytics, where data must remain usable but not reveal sensitive details. Meanwhile, blocking or disarming PII is crucial in controlled environments with stringent security needs, such as financial or healthcare institutions, preventing any unauthorized data transmission and significantly reducing the risk of breaches.

Building for Privacy with Votiro's Zero Trust Data Detection & Response

Enhancing your security posture to avoid emerging threats is crucial, especially in protecting PII. To this end, integrating Zero Trust Content Security with Data Detection & Response into a single platform delivers an effective solution. This integration helps organizations proactively defend against file-based threats and manage privacy and compliance in real-time. The Votiro platform also provides insightful data analytics, offering a comprehensive solution to safeguard organizations, their employees, customers, and reputations from digital threats while effectively managing privacy risks.

Votiro's Zero Trust DDR combines advanced malware neutralization with sensitive data protection, creating a strong security solution for all. By emphasizing the early identification and resolution of vulnerabilities to prevent exploitation, organizations can effectively safeguard against security threats while simultaneously protecting sensitive information in real time.

By adopting a proactive stance and integrating a zero-trust approach, Votiro provides a modern defense mechanism that addresses potential vulnerabilities before they can be exploited.

To learn more about Votiro's Data Detection & Response capabilities, sign up for a one-on-one demo of the platform.

You can also try it free for 30 days and see for yourself how Votiro can proactively defend PII and other sensitive data against threat actors and non-compliance fees.

VOTIRO

We make file-borne threats and privacy risks a thing of the past.

Contact Sales

Visit Website