

5 Ways Companies Can Protect Personally Identifiable Information

TechRounder PDF Edition

Live article:

<https://www.techrounder.com/business/few-ways-companies-can-protect-personally-identifiable-information/>

By Vipin PG | Published October 8, 2022 | Updated January 13, 2024 | Format: Article | 3 min read

In brief

Companies can protect Personally Identifiable Information (PII) by creating tailored safeguards, following applicable privacy regulations like CCPA, HIPAA, and GDPR, regularly reviewing data privacy policies, safely storing and destroying unnecessary PII, and conducting ongoing risk assessments.

Personally Identifiable Information (PII) helps identify one individual from another and includes names, social security numbers, phone numbers, passport numbers, driver's license numbers, credit cards, etc. Since companies collect, process, and hold such information for their customers and employees, they need to implement measures to ensure security, which can otherwise lead to hefty penalties and loss of reputation. For example, investing in strong data mapping tools by ZenData can significantly help you keep track of PII, so you can take immediate appropriate actions when required. Nevertheless, this article will discuss 5 ways companies can protect PII. Read below to learn!

1. Create Safeguards for PII Protection

Different threats require different safeguards. Therefore, you need to evaluate the level of risk each possible threat carries in your company and create safeguards accordingly. You should always have a policies and procedures manual handed over to onboarding employees so they know how to collect, hold, disclose, and destroy PII. In addition to encrypting sensitive data, you should provide training to all your employees. Regularly training them on cybersecurity protocols and new technological updates can help you ward off security breaches.

2. Know What Regulations You're Required to Follow

Regulations may vary from industry to industry. However, adhering to applicable privacy laws for your business will keep you in compliance and mitigate any risk of hefty penalties and loss of goodwill. Furthermore, since you will know which rules to follow regarding the processing, storage, and handling of PII, you will be able to protect sensitive and confidential information better. Some of the most common compliance mandates are California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), and General Data Protection Regulation (GDPR). Within the area of healthcare, email archiving plays a important role in upholding HIPAA compliance. By employing secure email archiving practices, organizations can meticulously track and store electronic communications containing protected health information (PHI). This both facilitates swift retrieval during audits and establishes a secure record-keeping system, mitigating the risk of unauthorized access or inadvertent data breaches.

3. Review Your Data Privacy Policies and Procedures

You must always keep track of your current data privacy policies and procedures and adjust them accordingly. For instance, you should assess if there were any near-misses or failures in recent events to implement better future strategies. Awareness of any new external and internal threats will also facilitate keeping the PII of your customers and employees secure while ensuring all the controls are practical and efficient.

4. Safely Store and Destroy Unnecessary PII

Most businesses may urge to collect as much information as possible from their customers to keep them updated regarding new product releases or boost overall sales. However, doing so will only make you more liable for any data breach. Thus, you should always limit the amount of PII you obtain from your customers and employees to prevent the risk of breach. Only collect information that is important for you and store it in a secure location with advanced security controls. When you no longer need PII, you must delete it properly to prevent cyber perpetrators from getting their hands on it.

5. Conduct a PII Risk Assessment

To develop the most accurate risk strategies, you must regularly conduct risk assessments based on the likelihood and severity of risks. This way, you can reduce or eliminate the impact of risk. While conducting a PII risk assessment, you should consider the worst-case scenarios too. For example, let's say who will be harmed, and are you currently adhering to data privacy laws? Asking such questions will lead to an adequate data protection plan.

References

1. cloudficient.com - blog / ultimate-guide-to-email-archives - <https://www.cloudficient.com/blog/ultimate-guide-to-email-archives>