

CCPA ([HTTPS://PRIVACYPILLAR.COM/CATEGORY/CCPA/](https://privacypillar.com/category/ccpa/))

Data Privacy Risk Assessment: Step-by-step Guide for Businesses

02/19/2024 (<https://privacypillar.com/data-privacy-risk-assessment/>)

There has never been a greater need to protect individual privacy than in this digitally connected age.

People are becoming more adept at navigating the digital world, but more complex and pervasive privacy risks come with it.



Concerns about privacy risks have triggered the inception of new privacy regulations now and then.

As per a report by Gartner, by 2023, 65% of the world population will have their data protected by modern privacy laws.

Besides the global push for regulations on privacy, consumers are becoming increasingly aware of their privacy rights and insisting that companies protect their data.

Organizations can address these two complementary criteria with a privacy risk assessment.

A privacy risk assessment becomes essential for understanding, assessing, and mitigating possible risks to people's and companies' data.

Conducting privacy risk assessments is the next step once a business understands its data collecting, usage, and sharing policies.

This helps the company and its customers understand the privacy risks these practices provide, both now and in the future.

Businesses can conduct as many individual or combined reviews as necessary to assess how their procedures may affect privacy.

These Privacy Risk Assessments or Impact Assessments go by various names, but they are commonly called either a Privacy Impact Assessment (PIA) or a Data Protection Impact Assessment (DPIA).

This article delves into understanding the concept of privacy risk management, why your business needs it in today's data-driven world, its



ts, and how to conduct a privacy risk assessment.

What is Privacy risk?

The possibility that people would encounter issues due to data processing and the impacts of such problems, should they occur, are known as privacy risks.

Technical measures lacking suitable protections, social media attacks, mobile malware, third-party access, negligence due to improper configuration, outdated security software, social engineering, and encryption are only a few examples of privacy risks.

Since privacy risks can arise at any point in the data life cycle, properly assessing, managing, and governing data is critical.

Several privacy risk assessment activities can occur throughout the data life cycle.

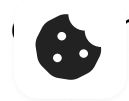
The first step in ensuring data validation and protection, monitoring and controlling data, and complying with every applicable law and regulation is to design a privacy risk assessment framework.

What is a Privacy Risk Assessment?

A risk management framework called a privacy risk assessment is used to assess the risks of storing and managing personally identifiable information (PII).

Organizations can make well-informed decisions to avoid privacy-related mistakes by performing privacy risk assessments.

This ensures that companies abide by privacy laws and can handle consumer and authority demands for data privacy.



Because of this, businesses that carry out privacy risk assessments have a greater chance of avoiding the negative effects of non-compliance on their commercial and legal standing and establishing lasting, reliable relationships with their customers.

PIAs (Privacy Impact Assessments) and DPIAs (Data Protection Impact Assessments) are commonly used to describe privacy risk assessments.

Now, you must wonder what to do in a privacy risk assessment using each type of means.

What is PIA? (Privacy Impact Assessments)

PIAs are risk assessments that assess the privacy controls in a company.

A PIA assesses the degree to which personally identifiable information (PII) is handled and secured, as well as the level of privacy risks that an organization faces when collecting, storing, and circulating PII by keeping an eye on organizational procedures, systems, applications, and products.

Organizations can address any blind spots through the implementation of practical measures, such as mandating data encryption, enabling consumer opt-out, introducing privacy rules, etc., thanks to this internal audit.

What is DPIA? (Data Protection Impact Assessment)

Risk assessments also include DPIAs.



re related to the GDPR, however, in contrast to PIAs.

Businesses must create and conduct DPIAs for high-risk data processing activities following GDPR Article 35.

The following use cases are included in this:

- Profiling and other assessments of personally identifiable aspects.
- Processing personal data and personally identifiable information on a large scale.
- Where data collection and processing are carried out automatically.
- Large-scale surveillance in public spaces.

DPIAs include:

- A thorough description of data processing activities and their purpose
- An analysis of the legal basis for data collection activities.
- An assessment of the personal risk that these data-collecting activities pose.

An explanation of the steps the company must take to reduce these risks and ensure GDPR compliance.

Organizations can avoid the costly legal and economic consequences of violating the GDPR by using the DPIA framework to help comply with the regulation.

Why do businesses need Privacy Risk Assessment?

Businesses can comply with contemporary privacy regulations by using privacy risk assessments.



could be government organizations' compliance obligations,

customers' demands from companies to protect their data, or requirements of internal business stakeholders' who realize the value of privacy.

Let's explore each of these needs in more detail:

Compliance Regulations

Throughout the world, new regulations are emerging.

Legal requirements such as the GDPR, CCPA, PIPEDA, and CPA require many levels of personal information management, maintenance, and control.

Businesses can find compliance gaps, analyze the risks associated with those gaps, and take appropriate action before facing the negative financial and legal consequences of non-compliance by carrying out a privacy risk assessment.

Customer needs

People are far more aware of their privacy now than in the past.

They know disclosing their personal information could lead to financial losses, embarrassment, discrimination, and physical risks.

They, therefore, hope that companies will protect their personal information.

A privacy risk assessment can help businesses establish a trustworthy, long-term relationship with their customers.

Needs for Internal Security



Businesses constantly fear privacy data breaches, primarily due to difficulty containing the blast radius.

Even if a breach results from a “silly” security mistake or an accidental employee leak, the consequences could still be disastrous when made public.

Using a privacy risk assessment, the company actively works to lower such risk by identifying security and compliance risks to take timely action.

Businesses can reposition themselves as a privacy-first organization and do the right thing for their consumers and business by doing a privacy risk assessment.

Benefits of Privacy Risk Assessment

While performing a privacy risk assessment can seem like a difficult and time-consuming process, there are several advantages for companies that involve it, such as:

Being prepared for anything and everything

To avoid unpleasant surprises, privacy risk assessments are strategic initiatives that help the organization plan privacy activities and prepare for compliance audits and customer requests.

By managing them, the business can make sure they are always prepared for any privacy curveball that may come their way.

Put otherwise, a privacy risk assessment can save unnecessary stress.

Making Informed Decisions

The first step in a privacy risk assessment is to find any privacy gaps in how the company collects, handles, and protects sensitive data such as credit numbers, addresses, contact information, and credentials.



Next, the evaluation assesses the potential risk of these gaps and makes informed decisions.

Businesses can deal with privacy gaps and blind spots in an informed and economical manner using this data-driven and precise approach.

The benefits of the decisions to the company can be supported and proven.

Communicating with Customers and Staff

Businesses are under a lot of pressure these days.

The Great Resignation, fierce competition, technological advancements, and geopolitical tectonic shifts are just a few of the changes that keep business owners up at night.

Protecting their privacy is critical in keeping an ongoing and trustworthy relationship with customers and staff throughout this period of uncertainty.

Businesses that protect employee and customer privacy indicate that safeguarding their data is their top priority.

Although not many businesses have the resources to launch extensive marketing campaigns highlighting their commitment to privacy, as Apple did, a simple pop-up notification on the website, an email or text message, or a social network post can have the same effect.

This will have a positive, lasting impact.

Getting Ready for Audits of Compliance



The criteria for compliance are strict, mandatory, and very important.

A privacy risk assessment makes sure that no standards about privacy are overlooked.

It offers a thorough picture of all the processes that require attention and allows the company to address them before they become a liability.

Furthermore, a privacy risk assessment provides the company with evidence that it took all the necessary steps to maintain compliance and later show it to authorities.

How to conduct a privacy risk assessment?

Although privacy risk assessments are valuable and essential, there is no set procedure or checklist to follow when conducting one.

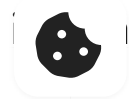
The business does, however, use a variety of tools. The primary ones are:

Data mapping

The process of analyzing, matching, and correlating data fields to produce a uniform, transparent, and comprehensive overview of the locations, uses, and flow of data inside an organization's systems is known as data mapping.

Businesses can use data mapping to ensure their data is high-quality and consistent across all sources.

They can identify possible privacy and compliance issues with this
ation.



The remediation procedure can be carried out if gaps are found.

By doing this, businesses can reduce privacy risks, meet legal requirements, and regain control over their data.

Data accuracy, data quality, structure, number of data sources, data type, data types, data access, data quality, and more may all be found in a data map.

Developing an automated RoPA

An organization's privacy policies and maintenance are documented in a Record of Processing Activities (RoPA).

A RoPA makes all data sources visible and understandable, revealing up to 100% of them.


An automated RoPA program will use data mapping to map data flows about collecting, processing, storing, and erasing PII.

After that, the tool will create the RoPA report automatically and make sure it is updated.

Businesses can use the RoPA to understand their privacy practices better, find and close gaps, and prepare for audits.

Manual Assessments

A more traditional way of privacy risk assessment involves collecting data manually.

This includes distributing questionnaires, going through spreadsheets, and  ing the findings.

FAIR Privacy and NIST PRAM assessments

Using the FAIR Privacy or NIST PRAM frameworks is a more advanced but manual assessment method.

Fair Privacy: Using a spreadsheet and a supplementary PowerPoint for risk calculation based on the Monte Carlo simulation, Fair Privacy is based on the FAIR (Factors Analysis in Information Risk) approach.

NIST PRAM: The Privacy Risk Assessment Methodology, or PRAM, is a set of worksheets that NIST created to help companies in “analyzing, assessing, and prioritizing privacy risks to decide how to respond and choose appropriate solutions.

External Assessments


The organization may relieve itself of the burden of conducting an independent privacy risk assessment by hiring a consulting firm.

The vendor will visit, evaluate all privacy measures, and give suggestions for the company’s next step.

Analyzing the return on investment (ROI) is essential when performing an external assessment.

This covers the process’s expenses and the long-term effects of disclosing private information to an external company.

It’s also advisable to understand the data mapping process that the vendor will carry out.

Will they use automated tools and procedures or continue a labor-
 iver, error-prone manual process?

When the seller leaves the property, what happens to your data?

How frequently is the assessment updated? And more.

Conclusion: Next step for businesses

Businesses may prevent costly and embarrassing errors by using privacy risk assessments as an early warning system regarding privacy gaps and their effects.

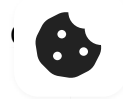
To begin, we advise selecting a workable solution that relieves you of the tedious duties and gives an accurate and efficient outcome you can promptly implement.




Businesses can obtain insights into their data collecting and management with an efficient and privacy-aware solution from automated data mapping and RoPA report generation.

These insights may then be converted into practical measures that close privacy gaps, allowing companies to comply with laws, fulfill customer requests, and meet internal security standards.

Furthermore, an automated solution gives companies authority over the assessment process and their data.

SHARE



 (<https://www.facebook.com/sharer/sharer.php?u=https://privacypillar.com/data-privacy-risk-assessment/>)
 (<https://twitter.com/intent/tweet?text=Data%20Privacy%20Risk%20Assessment:%20Step-by-step%20Guide%20for%20Businesses&url=https://privacypillar.com/data-privacy-risk-assessment/>)
 (<https://pinterest.com/pin/create/button/?url=https://privacypillar.com/wp-content/uploads/2024/02/Privacy-Risk-Assessment.webp&description=Data+Privacy+Risk+Assessment%3A+Step-by-step+Guide+for+Businesses>)

[in\(https://www.linkedin.com/shareArticle?mini=true&url=https://privacypillar.com/data-privacy-risk-assessment/&title=Data%20Privacy%20Risk%20Assessment:%20Step-by-step%20Guide%20for%20Businesses&source=PrivacyPillar\)](https://www.linkedin.com/shareArticle?mini=true&url=https://privacypillar.com/data-privacy-risk-assessment/&title=Data%20Privacy%20Risk%20Assessment:%20Step-by-step%20Guide%20for%20Businesses&source=PrivacyPillar)

← PREVIOUS ARTICLE

NEXT ARTICLE →

What are Consent and Preference Management: The Ultimate Business Guide
(<https://privacypillar.com/what-is-consent-and-preference-management/>)

What is a consent management platform, and why does your business need it?
(<https://privacypillar.com/what-is-a-consent-management-platform-and-why-does-your-business-need-it/>)

You may also like

(<https://privacypillar.com/maryland-online-data-privacy-act/>)



Maryland Online Data Privacy Act: A Comprehensive Guide (<https://>

privacypillar.com/maryland-online-data-privacy-act/)

(<https://privacypillar.com/global-privacy-platform-gpp-iab-tech-lab/>)

1 WEEK AGO

IAB Tech Lab's Global Privacy Platform (GPP): A Step Towards Streamlined User Consent in Online Advertising (<https://privacypillar.com/global-privacy-platform-gpp-iab-tech-lab/>)

(<https://privacypillar.com/data-privacy-for-automotive-companies/>)



2 WEEKS AGO

Data Protection in the Automotive Company: Ensuring Customer Trust and Compliance (<https://privacypillar.com/data-privacy-for-automotive-companies/>)

Search

Search

Recent Posts

Privacy Compliance Challenges for Global Companies (<https://privacypillar.com/privacy-compliance-for-global-companies/>)

Maryland Online Data Privacy Act: A Comprehensive Guide (<https://privacypillar.com/maryland-online-data-privacy-act/>)

IAB Tech Lab's Global Privacy Platform (GPP): A Step Towards Streamlined User Consent in Online Advertising (<https://privacypillar.com/global-privacy-platform-gpp-iab-tech-lab/>)

Data Protection in the Automotive Company: Ensuring Customer Trust and Compliance (<https://privacypillar.com/data-privacy-for-automotive-companies/>)



Cookie Policy and Privacy Challenges and Solutions for Pharmaceutical Companies (<https://privacypillar.com/cookie-policy-and-privacy-challenges-and-solutions-for-pharmaceutical-companies/>)

privacypillar.com/data-privacy-risk-assessment/

[\(https://privacypillar.com/\)](https://privacypillar.com/)



Subscribe to our Newsletter

Your email to start

Subscribe

PrivacyPillar needs the contact information you provide to us to contact you about our products and services. You may unsubscribe from these communications at any time. For information on how to unsubscribe, as well as our privacy practices and commitment to protecting your privacy, please review our Privacy Policy.

Our Products

Consent Management Platform(<https://privacypillar.com/consent-management-platform/>)

Cookie Consent Management(<https://privacypillar.com/cookie-consent-management/>)

Consent Preference Management(<https://privacypillar.com/consent-and-preference-management/>)

Dsar Management(<https://privacypillar.com/dsar-management/>)

Social Fortuna(<https://privacypillar.com/social-sharing-buttons/>)

Solutions

Europe (GDPR)(<https://privacypillar.com/gdpr-compliance-software/>)

Colorado (CPA)(<https://privacypillar.com/colorado-privacy-law-regulations/>)

Virginia (VCDPA)(<https://privacypillar.com/virginia-privacy-law/>)

California (CPRA)(<https://privacypillar.com/cpra-compliance/>)

Canada (PIPEDA)(<https://privacypillar.com/pipeda-compliance/>)

Brazil (LGPD)(<https://privacypillar.com/lgpd-compliance/>)

Connecticut (CTDPA)(<https://privacypillar.com/connecticut-data-privacy-law/>)



Healthcare Privacy Compliance(<https://privacypillar.com/healthcare-privacy-compliance/>)

Fintech Privacy Compliance(<https://privacypillar.com/fintech-privacy-compliance/>)

Chambers of Commerce(<https://privacypillar.com/chambers-of-commerce/>)

Free Tools

Privacy Policy Generator(<https://primeconsent.com/products/privacy-policy-generator/home>)

Cookie Scanner(<https://privacypillar.com/free-cookie-scanner/>)

14 Day Free Trial(<https://calendly.com/ppsalesinfo/30min>)

Additional Resources

About(<https://privacypillar.com/about/>)

Resource Center(<https://privacypillar.com/blog/>)

Partner With Us(<https://privacypillar.com/partnership-programs/>)

Contact(<https://privacypillar.com/contact/>)

Help Center(<https://support.privacypillar.com/help-center>)

Privacy Policy(<https://privacypillar.com/privacy-policy/>)

Customer Terms of Service(<https://privacypillar.com/customer-terms-of-service/>)

Acceptable Use Policy(<https://privacypillar.com/acceptable-use-policy/>)

Do Not Sell My Personal Data (<https://privacyportal.privacypillar.com/dsar/form?orgid=5ecad716-04d7-4e2e-ac78-5275bd3982fc&propid=f1afaefc-f102-4b15-8269-c6f8b1137fce&formid=349800c6-24aa-47b5-baf5-bb10e603b91d&status=publish>)

Your Privacy

Our privacy center makes it easy to see how we collect and use your information. Disable Your popup Blocker and manage your [cookie consent preferences](#)

Privacy Matters

When we collect your personal information, we always inform you of your rights and make it easy for you to exercise them. Where possible, we also let you manage your preferences about how much information you choose to share with us, or our partners.

Legal

Any information obtained from the PrivacyPolicy website, services, platform, tools, or comments, whether oral or written, does not constitute legal or regulatory advice. If legal assistance is required, users should seek legal advice from an attorney, a lawyer, or a law firm.



©2024 by PrivacyPillar

