WHITE PAPER

hCaptcha

Are Your Security Solutions Truly Privacy Compliant?

Privacy Compliance Is Not Easy for Security Vendors, and Your Company Could Be Liable for Their Shortcomings.

hCaptcha

Are Your Security Solutions Truly Privacy Compliant?

Privacy Compliance Is Not Easy for Security Vendors, and Your Company Could Be Liable for Their Shortcomings.

Around the globe, consumers are demanding greater accountability from the companies and the services that they interact with, including how organizations use and protect their private, personal data.

To that end, many governments have spear-headed legislation to protect the Personally Identifiable Information (PII) of individuals. In 2018, the European Union's GDPR data privacy laws came into force. As one of the most far-reaching privacy laws of recent times, it impacts every organization world-wide that interacts with anyone in the EU. Other countries soon followed suit, instituting their own data privacy-oriented legislation. This is often similar in scope to EU GDPR. Examples include Brazil's LGPD, China's PIPL and Singapore's PDPA. US states have also begun to adopt similar legislation, and it is likely that US federal data privacy laws will soon be updated as well.

These laws require online services to regularly audit their operations and make changes as needed to ensure compliance with regulations relating to PII. This can be a difficult undertaking for organizations, often entailing rigorous, labor intensive evaluations.

To complicate the situation even further, organizations are constantly under attack by cybercriminals, who threaten the very privacy infrastructure they've put into place. To mitigate these assaults, companies often deploy security solutions. Unfortunately, most solutions available today rely heavily on sharing PII to do their job effectively, and were not designed to be fully compliant with global privacy laws.

This dependence on PII can be a serious impediment to organizations as they strive to fully comply with privacy laws. If the solution was not designed with privacy in mind, or if it is misconfigured, organizations can unwittingly compromise the very thing they are trying to protect – user privacy.

KEY PRIVACY REGULATIONS

Countries world-wide have already, or are currently enacting strict privacy legislation. In 2021, legal firm Morrison and Foerster identified 133 jurisdictions around the globe with privacy laws in place and over 30 of these mandates have been created or extensively revised within the last 5 years. Some of these laws, like GDPR, impact many countries.

Here are a few of the more significant privacy regulations to date:

- **EU GDPR (General Data Protection Regulation):** Sets guidelines for the collection, processing, transmission, and retention of personal information of European (EU) residents. Although the UK is no longer a member of the EU, GDPR still applies to British residents by means of the UK GDPR.
- **Schrems II - July 2020:** Stipulates that the EU-US Privacy Shield, which has been frequently used by organizations to establish a legal basis for transmitting PII from the EU to the U.S., does not meet GDPR regulations. This ruling makes it more difficult for organizations, vendors, and partners to legally transfer PII across jurisdictions. Although it targets the EU and the U.S. specifically, the law impacts countries around the world.
- **California CCPA/CCPR (Consumer Privacy Act / Consumer Privacy Rights):** The first comprehensive privacy legislation in the U.S. gives consumers more control over the personal information that businesses collect. Any entity that serves users in California is subject to this law.
- **Brazilian LGPD (General Data Protection Law):** Broadly aligns with GDPR.
- **Canada PIPEDA (Personal Information Protection and Electronic Documents Act):** Canada' privacy legislation modeled after GDPR.
- **China PIPL (Personal Information Protection Law of the People's Republic of China):** Stricter than GDPR in some respects.
- **India PDP (Personal Data Protection bill):** Embeds many of the tenets of GDPR.

YOUR BUSINESS IS LIKELY AFFECTED: PRIVACY LAWS EXTEND BEYOND GEOGRAPHIC BOUNDARIES

Most privacy laws are extraterritorial, which means that they extend beyond the geographic limits of a particular country or jurisdiction. For example, GDPR is European law but non-European businesses are still subject to it. As such, every organization that processes PII belonging to European residents must abide by GDPR, even if that organization has no physical presence in Europe.

This is also true regarding privacy regulations in many other countries. An American company that interacts with individuals in China, Europe, and Brazil, must abide by each country's specific privacy laws.

The Cost of Non-Compliance

Below are some examples of recent GDPR fines and penalties:

- Amazon is currently in the process of appealing a fine for €631 million, allegedly relating to their cookie consent process.
- WhatsApp was fined €225 million in August of 2021 for a number of cross-border data protection violations.
- Google was fined €50 million by CNIL, France's data protection agency, for loading tracking cookies without consent.

WEBSITE OWNERS LIBEL FOR THIRD-PARTY VENDOR VIOLATIONS

Many assume that a privacy violation or a data breach brought about by a third-party vendor (e.g., cloud providers, security vendors, etc.), would absolve the online property owner of liability and ensuing penalties. Unfortunately, this is not the case.

For example, GDPR places equal liability on the organization that owns the data and the third-party organizations that help process, manage, secure, or store that data. If a third-party processor is not operating in compliance with the law, your organization, by extension, is not compliant.

STEEP PENALTIES FOR NONCOMPLIANCE WITH GDPR AND OTHER REGULATIONS

Violations of GDPR and other privacy laws can lead to stiff penalties. In the case of GDPR, fines of nearly $20 million U.S. dollars, or 4% of the organization's annual revenue - whichever is greater - can be levied against non-compliant organizations. PIPL violation fines are more severe, and can total up to 5% of annual revenue.

During the first year of GDPR enforcement, which commenced on May 1, 2018, EUROPOL issued over 89,000 violation notices and more than €56 million in fines were assessed.

WHAT THE PRIVACY LAWS REQUIRE

Most privacy laws have the following requirements in common:

Lawful, fair, and transparent processing: Organizations must document a lawful reason for processing personal data, and demonstrate that end users are aware of how their information is being processed and used.

Limitations of purpose, data, and storage: Organizations can only collect personal data for a specific, lawful purpose. They must also document that purpose and ensure that personal information is deleted when it is no longer needed.

End-user (data subject) rights: Organizations must provide the means for individuals to execute the following human rights:

The right to be informed: Organizations must communicate to individuals what data is being collected, how it's being used, how long it will be kept, and whether it will be shared with any third parties. This information needs to be communicated concisely and in plain language.

Common Reasons for GDPR Fines

- Failure to obtain cookie consent
- Noncompliant consent procedures
- Failure to explain data processing practices
- Improper PII safeguards
- Sending PII outside of authorized locations
- Sharing PII with 3rd party services
- Using PII for marketing activities without consent
- Failure to comply with user's Right of Access
- Failure to comply with user's Right to Erasure
- Failure to keep PII up to date

The right of access: If an end-user requests to see the data an organization has collected relating to them, the organization must honor that request. Organizations generally have one month to comply.

The right to rectification: If an individual discovers that an organization has collected inaccurate data, that individual may request that the information be corrected. The organization must comply within one month.

The right to erasure: If an individual is no longer a customer or withdraws consent for the organization to use their personal data, the individual has the right to have their data expunged. It should also be noted that usage limitations also require organizations to delete data that is no longer needed.

The right to be notified: In the event of a personal data breach, users must be notified within 72 hours following the discovery of the breach.

Consent: GDPR law requires organizations to gain an individual's consent before collecting or processing any personal data. Consent must be given through a clear, affirmative action taken by the user. Upon request for consent, it should also be clear to the end user that they can withdraw their consent at any time.

Express consent is not needed if the data is necessary to fulfill an existing legal contract with the individual, if performing legal obligations, and in a few other situations. But for most online property owners, obtaining consent is the most appropriate, lawful means to obtain and handle PII.

International Data Transfers: When GDPR went into effect in May of 2018, a number of organizations began using the EU - US Privacy Shield framework, or Standard Contractual Clauses (SCCs) coupled with user consent as the legal basis for transferring PII from within the EU to the U.S.

However, recent GDPR rulings, such as the July 2020 Schrems II, and the Dec 2021 Austrian Data Protection Authority (DPA) rulings, make it clear that transmitting PII between the EU and the U.S., even when using the EU - US Privacy Shield, or with SCCs and user consent in place, is illegal.

Under this interpretation of the law, personal data transfers may occur from the EU, but only if a very narrow set of conditions are met. For example, to transfer PII to the U.S. from the EU, data must first be encrypted by a European organization and the encryption keys cannot be provided to the U.S. entity. Since this prevents any processing from occurring on U.S. soil,

PII Drives Many Security Solutions

Some security vendors collect a wide range of PII including:

- User IDs
- Passwords
- Camera images
- Finger and voice prints
- User time zones
- IP addresses
- Associated device fingerprints
- Working hours
- Applications used
- Websites visited
- Files downloaded or transmitted
- "Typical" amount of data sent and received
- And more

virtually all reasons to transmit PII are nullified under the law, with the possible exception of simply storing the encrypted data overseas.

Privacy by Design and by Default: To fully comply with GDPR, organizations and the third-party applications and services they employ, must practice privacy by design and by default.

- **Privacy by Design** holds that when developing any new products, processes, or services that involve personal data–privacy must be considered during the initial design stages and throughout the entire development cycle.
- **Privacy by Default** stipulates that when a system or service presents users with options related to their privacy settings, those choices must default to the most privacy-centric option. Users must opt-in through an express, intentional action to alter those default settings.

SECURITY SERVICES CAN POTENTIALLY VIOLATE PRIVACY LAWS

While security services and products are employed to protect data, including PII and other sensitive information, unless they are carefully designed and used, some security products and services can undermine privacy and make it difficult to comply with privacy laws.

Security vendors and providers are often caught in a trade-off between creating an environment that delivers tight, nearly impenetrable security–and one that fosters productivity, easy access, and individual privacy. Striking the right balance requires thoughtful design, a great deal of flexibility, and advanced technical capabilities. Not all security solutions possess these vital ingredients.

Non-security companies that provide security solutions as a byproduct or an appendage to their core business are faced with an even greater challenge when it comes to privacy compliance. This is especially true if their business depends on PII, as is the case with the marketing and advertising industry. For these organizations, the requirement to fully anonymize PII to meet privacy compliance goes against their primary business interests.

As an example, Google is primarily an advertising business, meaning their revenue is principally derived from tracking and profiling people in order to show them relevant ads. Their privacy policies are vague and flexible, allowing data to be shared across Google products and services, and their reCAPTCHA security products have been optimized for data collection in ways that are likely unnecessary for security.

IT'S NOT EASY FOR SECURITY VENDORS TO ADHERE TO PRIVACY LAWS

Security products typically collect a wide range of information related to network visitors. The more that is known about these users, the easier it is to spot anomalies and react. The information collected by security products often includes: user IDs; passwords, biometric data such as camera images, finger and voice prints; user time zones; IP addresses; associated device fingerprints; working hours; and other personal, private, or sensitive data.

In recent years, User Behavior Analytics (UBA) have been widely integrated within many security products. This trend has intensified the gathering and retention of personal data. For instance, it is now commonplace to capture, store, and analyze data like: Applications used; websites visited; files downloaded or transmitted; "normal" amounts of data sent and received; devices used, and more. Security vendors then store this sensitive information in databases–frequently in the cloud, and in disparate locations around the globe. Naturally, this practice can greatly impact privacy compliance.

Poor security solutions store sensitive information in relatively unprotected ways and retain it for years. Competent security vendors encrypt and properly gate access to the data. Better vendors fully anonymize all private information so that, even when combined with other data, PII cannot be derived. The very best vendors go beyond fully anonymizing data to offer options to provably avoid collecting PII in the first place. They may also provide options to store and process sensitive data in authorized regions, such as within the user's own country. Furthermore, these ideal vendors expunge all data on a regular basis–thus providing the only solutions that are fully compliant with today's privacy laws.

SOME SECURITY PROVIDERS HAVE A CONFLICT WITH PRIVACY

Over the years, many large enterprises have collected vast amounts of personal information, typically to support their marketing, advertising, and sales efforts. Because this data can be used to identify people, some companies created security products and services as adjuncts to their core business. Unfortunately, many of these products and services process and transmit PII to unauthorized areas–in direct violation of privacy laws.

If your organization uses security services from an organization that collects a great deal of user data without offering provable safeguards and offers products entirely unrelated to security that would benefit from that data, check thoroughly for privacy violations. Many will not comply.

Security and Related Services that Process PII

Here's a list of common security and security-related systems that gather or process user data. All of the systems enumerated below should be thoroughly evaluated for privacy compliance:

- User authentication and authorization systems
- Identity and Access Management (IAM) systems
- User Behavior Analytics systems, or any system that uses UBA
- CAPTCHA products and services
- Bot mitigation solutions
- SIEM products
- Forensic tools
- Fraud detection services
- Incident response services
- User/employee monitoring tools
- Website filtering services
- Traffic analysis systems
- Data Loss Prevention systems
- Encryption systems for data at rest and in transit
- Email and other archiving systems
- Threat intelligence services
- Document signing services
- eTransaction services
- HR systems
- Customer Relationship and Management (CRM) systems
- Marketing, advertising, and lead generation systems

PRIVACY COMPLIANCE - WHAT TO LOOK FOR

Some security solution providers may advertise GDPR compliance, even when they are only partially compliant. To help determine if your security solution providers are truly compliant with GDPR and other privacy laws, the following areas should be carefully evaluated for each product or service.

PII Data Should Not Be Transmitted Abroad

As described earlier, GDPR and other privacy regulations now make it clear that in most scenarios, PII data can't be transferred outside of the jurisdiction that established the law. European PII can't leave the EU. Brazilian PII can't leave Brazil, etc.

Each product in an organization's security stack needs to be thoroughly investigated to ensure they are not in violation. Some services appear to be wholly autonomous, but in fact use partners that may also transmit data.

PII Data Must be Anonymized

Personal data that has been fully anonymized is no longer considered PII and is not subject to GDPR or other privacy laws. Such anonymized data can be stored, transmitted, and processed without restrictions.

However, to achieve full anonymization under GDPR, re-identification of an individual, even by the company that anonymized the data, must be impossible–even when paired with other data such as IP addresses, device fingerprints, user IDs, age, etc.

This is a difficult technical challenge, which is not yet supported by many security vendors.

Third-Party Cookies - A First Rate Problem

PII is often gathered and stored on a user's device in the form of a third-party cookie. These cookies are commonly used for advertising purposes and may contain a large amount of personal, sensitive data, including the user's address, age, sex, language, past internet searches, products and pages viewed, site passwords, and more.

Often, security solution providers that advertise GDPR compliance do not fully meet the requirements.

These third-party cookies are especially dangerous from a privacy perspective because numerous sites could potentially read them. All that's needed for any website to read a third-party cookie is a small snippet of code from that third-party. Since this code is generally advertising related, that code is often available to any organization that wants it.

In addition to obtaining user consent for cookies to be placed, all organizations need to carefully evaluate how cookies are handled. For instance, the manner in which many bot mitigation services handle and transmit cookie data is not compliant with GDPR.

PII Must be Destroyed After Use

Many "big data" applications tend to archive data for years. Security applications are no exception. Privacy laws dictate that PII must be shredded when it is no longer needed. When exactly the data is no longer needed is debatable. But to be safe, products should include features that automatically destroy PII either regularly, or when certain conditions are met such as withdrawal of consent, account deletion, user request, etc.

Organizations need to ensure that their security solution providers are fully destroying unnecessary data as early as possible.

Check System and Product Log Files

Analyze all system and product logs for traces of PII. For example, SIEMs and forensic tools often require the functionality to pinpoint users. To do that, user credentials are nearly always necessary, and frequently serve as "primary keys" on which security analyses are based.

By default, most SIEMs don't capture any sensitive information, only receiving information that is explicitly sent to them. However, it's not uncommon for PII to inadvertently be sent SIEM files. Investigate the logs, and any process that sends data to SIEMs or similar products.

IN SUMMARY, CHECK THE DETAILS

With many zettabytes of information processed online worldwide, personal data is constantly at risk of being compromised. The recent proliferation of privacy laws does much to address the risks, but organizations often struggle to fully comply with the numerous mandates. While challenging for many vendors, solutions that enable organizations to strike a balance between compliance, security, and end-user experience do exist. For example, at hCaptcha we resolved data processing issues by enabling data to be processed at the network edge, local to the user, and rapidly discarded. In fact, all of hCaptcha's data is ephemeral by design.

As with many things, it's the details that matter. Unauthorized cross-border data transfers, the rampant use of cookies, the failure to fully anonymize, and the failure to delete data are common privacy-violating practices among some security solutions. You may need to fully investigate your security stack to uncover these shortcomings. Your vendors may not even be aware that they are not in full compliance.

As you scrutinize your processes, vendors, and partners, it's quite likely that your company will need to replace some of its non-complying security solutions.

Fortunately, there are privacy-first solutions, like hCaptcha, on the market that will help your organization meet the requirements and standards put into effect by governments around the world. Looking for security solution providers that place privacy as a priority, and openly advertise compliance with GDPR and other privacy legislation will significantly help.

Author: Gawel Mikolajczyk, an expert in Online Security, Privacy, and GDPR. Director of Security Operations and Data Protection Officer at hCaptcha, an Intuition Machines company.

Resources

Guide to UK General Data Protection Regulation (GDPR): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Morrison and Foerster, Privacy Around the World: https://www.mofo.com/resources/insights/210127-data-privacy-day.html

EUROPOL recorded GDPR first-year fines: https://www.asisonline.org/security-management-magazine/articles/2020/02/conducting-a-gdpr-compliant-investigation/

Clarity in Privacy: https://www.clarip.com/blog/gdpr-key-requirements/

Summary of the GDPR's 10 Key Requirements: https://www.itgovernance.eu/blog/en/summary-of-the-gdprs-10-key-requirements

EU-US Privacy Shield: https://www.privacyshield.gov/program-overview

How to Transfer Data to US and be Compliant with GDPR: https://www.privacyaffairs.com/eu-us-gdpr-data-transfer/