How Cybersecurity Teams Can Support and Facilitate Compliance with the GDPR

By Grace Buckler – ISSA member, National Capital Chapter

The General Data Protection Regulation (GDPR) gives residents of the European Union control over their own personal information regarding how organizations are allowed to collect and handle their private data. This article discusses how security teams can contribute to compliance efforts right away and long-term.

Abstract
The General Data Protection Regulation (GDPR) gives residents of the European Union control over their own personal information regarding how organizations are allowed to collect and handle their private data. Consequently, for these organizations complying with GDPR means blending many business functions including privacy, security, management, human resources, legal, marketing, governance, and compliance, among others. In the long term, privacy risks will be systematically mitigated, individuals’ rights protected, and consumer loyalty and satisfaction boosted. Less money will be spent on regulatory penalties and legal actions, and the organizational culture of businesses will be healthier. How can security teams contribute to these opportunities right away and long-term? A better understanding of what GDPR requires, why GDPR matters to other business functions and the entire business operation, how GDPR impacts security strategy, and cross-functional collaboration are important. Also critical to grasp are steps security must take now to comply.

With 90+ meetings related to GDPR compliance under my belt, I’ve heard the same arguments and frustrations raised again and again:

“Aren’t we already doing that?”
“That doesn’t really tell me what to do about security!”
“Is there a list? Please just give us a list of requirements.”
“Seventy-two-hour breach notification? That’s insane.”
“What does ‘upon being aware of a breach’ mean, anyway?”

If your team has expressed similar qualms, know that these are all valid concerns.

What does your cybersecurity team really need to understand and prioritize in order to comply with the GDPR in a way that simultaneously adds value to your organization’s data management, data processing activities, and data visibility while protecting the rights and freedoms of EU residents? Let’s find out.

The GDPR in brief
The GDPR was intended to give European residents control over how their personal information is collected and handled by organizations. It replaces all previous privacy laws in the 28 EU member-states.

This actually makes it easier, in a sense, for businesses as they now only have to deal with one regulation for the entirety of the EU (as opposed to 28 different national privacy laws). The
EU’s Data Regulation Board has also been fairly expedient in its releases of GDPR guidance documents to address specific implementation concerns that organizations have expressed.

Even so, there’s been much anxiety within the cybersecurity industry as a whole, especially for those that have approached this situation without much collaboration with other teams in their organizations.

Basically, departments have had to come to grips with GDPR-related privacy principles in Article 5, outlined in table 1: GDPR privacy principles.

So how can you optimize your company’s approach to dealing with these security and privacy concerns?

**Broader long-term strategies to implement**

**Don’t let implementing GDPR requirements spark company in-fighting or morale loss.**

The GDPR allows you to implement its requirements your way, so don’t push so hard to comply that you lose the soul of your organization—its character, its ideals, and the energy and the support of your people. Also, don’t lose your human touch, vision, or security staff. Leverage people, knowledge, processes, and tools to start as no two security environments are the same regarding GDPR implementation and compliance.

Rather than saying, “It’s all about the EU and GDPR,” try saying, “Guys, it’s a new a day, and this is how business is now done according to our company. We must address new requirements to comply.”

As a manager, help to communicate obligations and expectations tactfully, starting with your team, and align the needs of other functions with overarching business strategies and goals.

<table>
<thead>
<tr>
<th>Privacy Principles Relating to Processing of Personal Data</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawfulness, Fairness, and Transparency</td>
<td>Processing personal data “lawfully, fairly, and in a transparent manner in relation to the data subject”</td>
</tr>
<tr>
<td>Purpose Limitation</td>
<td>Data collection “for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes”</td>
</tr>
<tr>
<td>Data Minimization</td>
<td>Processing personal data in a manner that is “adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed”</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Keeping personal data up to date and taking reasonable steps to “ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”</td>
</tr>
<tr>
<td>Storage Limitation</td>
<td>Keeping personal data in a form that allows identification of individuals “for no longer than is necessary”</td>
</tr>
<tr>
<td>Integrity and Confidentiality</td>
<td>Processing personal data in a way that “ensures appropriate security of the personal data,” including protection against unauthorized or unlawful modification or disclosure and against “accidental loss”</td>
</tr>
<tr>
<td>Accountability</td>
<td>Taking responsibility for data protection and being “able to demonstrate compliance with lawfulness, fairness, and transparency”</td>
</tr>
</tbody>
</table>

Table 1 – GDPR Chapter II, Principles [5]
for harmonizing privacy, security, legal, marketing, management, governance, compliance, and numerous other business functions. One of the worst that can happen is failing to demonstrate implementation of security measures or failing to show that you have a road map or plan for compliance with the regulation. According to PwC Pulse Survey, “Information security enhancement is a top GDPR initiative.” About 77 percent of US multi-national organizations “plan to spend $1 million or more on GDPR,” and over 50 percent of these organizations have made GDPR data protection requirements their top priority [1]. The lack of regulatory understanding, highlighted earlier, and the lack of budget are valid concerns but can be addressed quickly when representation from all functions contribute to making the business case for data privacy.

Implement GDPR requirements in a way that strengthens your company’s culture.

Corporate culture brings value to your organization and shouldn’t be threatened by inefficiencies or a lack of security. Because just one incident of data mishandling is a big mistake, you’ll likely incur financial losses and damage your company’s culture.

In this digital age, cybersecurity holds the key to your company’s value, reputation, and culture. Cybersecurity can add serious value to your enterprise’s entire business strategy—or hurt it if you let customers down.

It’s therefore important to understand your business obligations and meet them with solutions, processes, and procedures that will outlast GDPR compliance and ultimately reinforce a positive culture within the security team and in your organization.

Appreciate why this matters.

Protecting personal data is about protecting the rights and freedoms of individuals whose personal or private data is in your organization’s custody. Special attention should be given to such information, especially when that data involves employment records, customer contact information, tracking and behavioral preferences, health information, children’s personal data, and more.

Privacy is a different realm than protecting ordinary business confidential information. It requires special care because privacy is a human rights concern in the EU. Information covered by the GDPR includes any information that identifies a person.

Inadequate security measures or mishandling of personal information can cause damage to people in multiple ways, including harm to their reputation, embarrassment, financial loss, and loss of life, among others.

Collaborate with other teams as well as your organization’s service providers or vendors, third parties, and partners to effectively assess risks.

Privacy impact assessments (PIA) should be your concern and a cause for dialogue with your company’s privacy-focused team. If that conversation hasn’t happened yet, by all means, start with identifying the systems, data flows, storage, and processes to be assessed for privacy.

Join forces with the privacy team to obtain access to any tools that help automate the PIA and accept any meetings necessary to confirm your implementation of appropriate security control measures. Complete insight into the risk posture of the enterprise won’t be possible until your security team’s risk assessment is aligned with the privacy impact assessment.

The biggest impact of a data breach on individuals can be found in the conclusions drawn from a PIA in terms of how the liberties and freedoms of individual victims have been impacted.

The GDPR has made it clear that ignorance of regulatory requirements is not an excuse. Risks are shared. You are engaging with others to keep discovering your responsibilities to help them and your enterprise as a whole. Being a member of a GDPR-compliant organization means you’ve accepted sharing risks and obligations.

These risks are not limited to external threats such as hackers [7]. Risks associated with mishandling data may include not properly setting expectations and boundaries for the organization’s website activities, service providers, and/or third parties’ or partners’ websites, software, apps, and more.

Is vendor risk assessment included in your security risk assessment? Do you know what security assessments or audits your providers have undergone, and are these up to standards that align with your legal, privacy, and business obligations with GDPR?
Who Dares To See
The Anti-Drone
Air Defence System
Challenge
We Propose!
Listen closely to other teams’ and other companies’ concerns and struggles.

What are other teams in your company doing about GDPR to accomplish their business objectives and goals?

Be ready to answer questions that your marketing, privacy, legal, or customer care teams have, and feel free to ask questions of them. You may leave with some much-needed clarity; every team’s challenge is intertwined, and these discussions hold the key to taking actionable steps [2].

Stay aware of the mistakes and vulnerabilities of other companies as this is a simple and cost-effective way to improve privacy in your systems without bearing the costs of a big mistake.

Step up and own what you need to own.

The phrase “privacy policy” got a bad name in April, and “we’ve changed our privacy policy” is now a joke. Nonetheless, don’t let that prevent you from updating your own privacy policy.

The activities of your organization’s website and social media users are in your domain, so when the privacy team drafts sections such as “what information we collect about you,” “information we collect indirectly from you,” cookies, encryption, etc., review to ensure the website privacy policy reflects the current state of security in your company’s data collection and handling activities [3].

Likewise, review your company’s security standards, policies, and procedures documents. These mechanisms are meant to be reviewed and updated. Identify what needs to aligned with new privacy requirements, and update them.

Five things you should handle right away to support cybersecurity–privacy strategy

1. Add awareness and training opportunities to your calendar.

You can’t protect what you don’t know. The International Association of Privacy Professionals (IAPP) offers a wealth of published resources, webinars, discussions, and classes suitable for IT security professionals and technologists [10]. This shouldn’t take the place of properly engaging with a multi-functional team, however. The more you learn at your leisure, the more insight you can bring to the larger team. GDPR provides EU residents the privacy rights in table 2: Rights of the data subject.

Consider these rights carefully. Exercising these rights as well as protecting them requires automated processes, solutions, and digital protection, so cybersecurity plays a major role [6].

2. Incorporate privacy-by-design and security-by-design.

Assess upcoming initiatives, new projects, processes, and technology solutions for cybersecurity and privacy inclusion from the start. The United Kingdom’s Information Commissioner’s Office (ICO) defines “privacy-by-design and default” as implementing “appropriate technical and organizational measures to execute the data protection principles and safeguard individual rights” [4] Privacy and security should be the default control and inherent in any area where personal data is processed.

3. Encrypt and pseudonymize personal data.

Have you developed an in-scope data-flow mapping relevant to the personal data covered by the GDPR? How about encrypt-

The ISSA Journal on the Go!

Have you explored the versions for phones and tablets?

Go to the Journal home page and choose “ePub” or “Mobi.”

To use "ePubs"
- ePubs are scalable to any size device: iPad/tablet provide an excellent user experience
- You’ll need an ePub reader such as iBooks for iOS devices

To use "Mobi"
- Mobi is a format only Kindle devices can read

NOTE: choose ePub for Android & iOS; Mobi for Kindles

Take them with you and read anywhere, anytime…
The right to see personal data held by the organization

The right to restrict the processing of personal data

The right to directly transmit data to another organization

The right to object to the processing of personal data

The right to not be subject to solely automated decision-making including profiling

Table 2 – GDPR Chapter III: Rights of the Data Subject [5]

If the individual is already identifiable or identified by your enterprise through transactional activity or other relationship, any additional identifying information collected that’s linked to that individual is personal data. What does your enterprise consider personal data? Assess this against the GDPR’s definition. You have to inventory personal data in your environment, classify the data, and map its flow. Using an automated data discovery and data mapping tool can provide you an accurate determination of the personal data that you process or hold about EU residents [1].

It’s inevitable that an unauthorized party might at some point have access to private data that should be protected, so it’s crucial that personal data your organization might accidentally disclose or lose is encrypted or pseudonymized. For your organization, this might mean just narrowly escaping being fined a percentage of your annual global revenue.

4. Engage privacy and legal teams to revise your cybersecurity incident response plan.

Update your cybersecurity plan now to address what a privacy incident constitutes. What criteria will help declare such incidents? Include privacy and legal contacts in addition to the cybersecurity strategy team, among others. What improvements could be made to access controls to ensure privacy and security safeguards? Are you looking into two-factor authentication solutions? Are multi-layered network security measures considered in light of privacy and GDPR concerns? Are employees teleworking and using personal devices for business? Are all remote-access privacy rules and concerns addressed?

What about your organization’s endpoint security for laptops, workstations, and other devices? CPO Magazine highlights optimizing next-gen end-point protection and emphasizes greater use of endpoint protection platforms (EPP) [1]. Enhanced controls and tools could support data flow visibility, more instantaneous detections, and prevention of abnormalities.

5. Incorporate a personal data breach response plan.

The security team owns the breach response plan, but privacy and legal teams are key stakeholders and should be consulted on all matters relating to personal data breaches.

Great implementation of privacy obligations requires presence. Your team’s presence and participation in the requirements interpretation process is critical. This often presents learning opportunities for the business as a whole since privacy is an obligation of the entire organization. To sustain GDPR compliance success, intentional collaboration is vital and will always be a major element in achieving a suitable strategy, resources, and support.

Conclusion

According to the 2018 Pulse Survey, more than half of US global corporations indicate GDPR is their top data protection priority [9]. GDPR was enforced on May 25, 2018, and...
there’s no grace period [10]. This means regulators have begun imposing penalties and fines on businesses that do not meet compliance requirements. Security teams need to move faster than the GDPR regulators to make data protection a priority. If your organization also processes personal information of California residents, the new California Consumer Privacy Act (CCPA) provides an added set of privacy requirements that you’ll need to consider and implement prior to January 1, 2020. While this law has very similar privacy rights to the GDPR, there are a few differences. And some US state privacy laws have undergone amendments since GDPR enforcement. For example, South Carolina requires a 72-hour data breach notification.

Consider this trend an incentive to implement and monitor your organization’s GDPR compliance even more expeditiously as it will lay the groundwork for operationalizing California and other state privacy requirements. Collaboration and consultation with the privacy and legal teams are key to a successful strategy, sufficient implementation, compliance, and a healthy organizational culture.

References


About the Author

Grace Buckler, CIPP/E, CIPP/US, CIPP/G, CISA, CISSP, CRISC, PMP, is the founder and president of The Privacy Advocate, a Washington DC–based global privacy consulting firm. She delivers strategic privacy awareness, privacy governance, and privacy risk management consulting among other services to private-sector and public-sector organizations. She may be reached at info@theprivacyadvocate.com.