GDPR Playbook

by **Kim Carlos** | Jul 2, 2018 | **Blog**, **Compliance**, **Digital Defense, Inc.**, **Kim Carlos**

It's time to play hardball – Fight and win the GDPR battle with a leader, plan and rock star team.

Yes. We know GDPR is here. Can we talk about something else now?

Nope, not if you haven't done **all** your due diligence to implement best practices and comply. Ignorance has been bliss but it's not an excuse post May 25, 2018.

We've already seen GDPR come down with hard on **day 1** of its enforcement with **Google, Facebook, Instagram and WhatsApp** with fines that could carry $9.3 billion. It's easy to think if you're a "mostly" U.S. focused company or if you're small or medium in size that GDPR isn't something you need to concern yourself with. The ugly truth is that is far from the case.

If you're like the majority of companies, **GDPR compliance is definitely still a dilemma** even though the deadline has come and gone.

Why?

- It's a regulation and not a straight forward security framework to follow so there's a lot of guesswork;
- There are significant hurdles in pivoting operations towards new business practices to comply;
- Data discovery to find PII, where it is and where it isn't, is challenging within all systems but especially legacy systems; and
- You only have 72 hours to report a breach, which means there isn't much time for investigation or validation, just to name a few.

Don't assume or it makes an...

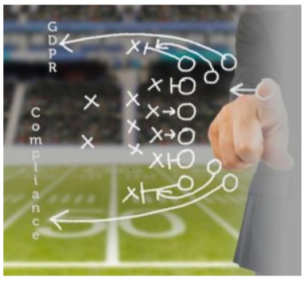
The deadline might have passed but the majority of companies aren't fully ready. Don't fool yourself into thinking that because you are compliant with other regulations like PCI DSS or HIPAA you will fall into GDPR compliance fully or easily.

You need to do an internal audit to determine your readiness to comply and build a team of winners to help you conquer. Ask yourself:

- What data security safeguards do you have in place currently and how do they align with GDPR requirements?
- What standards or regulations are you already compliant with, and where are the gaps between those and the GDPR?
- What GDPR supervising authorities should be on your radar based on your business or industry?
- Who are your key internal rock stars to help you on your way to GDPR compliance?
- How should you organize internally to audit your security practices and controls and then elect if they will be sufficient to comply?

Starting there will put you ahead of most at this stage, and having a plan in place can help reduce the chaos that can ensue from ignorance around this complex subject.

Every winning team needs the best players



You need a playbook. Top college football teams didn't become national champions by shooting from the hip. At the core, they started with a leader who built a team to win. Finding the right skillset for your team is what's key.

Creating a strong underpinning of security and compliance involves surrounding your organization with a veracious team of people:

1. **An executive, powerhouse player** –The tone from the top is key for GDPR compliance and security operations of any kind. An engaged and involved executive doesn't have to be an expert in security or even IT, but they should comprehend the goals and initiatives and have visibility into all security-related technologies, policies and processes. A good place to start would be your Chief Legal Officer, as they have a big stake in ensuring organizational adherence to GDPR.

This player can be your advocate and watch your back as the rest of your team focuses on executing and getting

Categories

Blog
Chris Graham
CTO: Information General
DDI Labs
Digital Defense, Inc.
Gordon MacKay
Headlines
Mark Bell
Mike Cotton
News
Security
Tom DeSot
Vulnerability Research Team
Zero-Day Alerts

the job done.

2. **A cybersecurity quarterback** – Someone who is willing to lead the team during both the research and implementation process. It's important that this person is included from the beginning. This person might hold the job title of CISO or ISO and is very focused on bringing departments together to avoid gaps in security and compliance due to silos within the organization.
3. **A compliance or data privacy guru** – Someone within your organization that understands GDPR and all other regulations that need to be met with any technology platform you put in place. This is actually a required position in GDPR known as the Data Privacy Officer (DPO) but they might currently hold the title of Compliance Officer or the like. This person has vast knowledge to bring to the table so be sure to stay unbiased and truly take their input under serious advisement.
4. **A security operations watchdog** –This is the person that works in-depth within your IT infrastructure to ensure no one is sneaking in through your backdoors. This is the person that is often missing internally from the small to mid-sized business due to lack of budget or scarcity of the market supply.
5. **The referee** – This member is the one who loves putting processes into place. They are your stream-liners! It's often someone with administrative duties who knows the ins and outs of your business. This person's perspective will help you identify gaps that you might not otherwise be aware of if this skill just isn't in your remit.
6. **The all-star** – It's ok to ask for directions. With your 5 internal team players being in place, it's time to consider outside help. With GDPR being complex, bringing in an expert in can really help you win the game faster. Because GDPR is so new, this person might not have many GDPR "wins" under their belt just yet, but if they do snatch them up! They likely do have compliance and security accolades and significant experience that can help your organization take their GDPR compliance plan to the next level.

Complying with any regulation is difficult but if you keep your wits about you when others are in a panic, it's probable you'll come out smelling like roses. Your team is looking for you to lead so create the plays and go for the win.

CONTACT

Digital Defense, Inc.

9000 Tesoro Drive, Suite 100
San Antonio, TX 78217

Main Line: 888-273-1412
Sales: 888-273-1412 ext. 1
Customer Support: 888-273-1412 ext. 2
support@digitaldefense.com