GDPR – How to Implement

As the GDPR deadline for enforced compliance looms, we are inundated by articles about how it impacts us, what we should worry about and how to be compliant. Here is an example:

https://www.linkedin.com/pulse/what-does-gdpr-really-mean-hr-teams-bernard-marr/

While this is a well written article and it has a specific HR focus, it is VERY high level. I've searched other articles and documents and came to an epiphany. No one has really sat down to fully analyze what is GDPR trying to accomplish at the Security Control level nor cross-mapped it to other frameworks, standards and regulations for compliance. So, we at Eigenspace did that. Here is what we think.

GDPR is about getting an organization to change its Cybersecurity Awareness of privacy information. The GDPR outlines the need for an organization to show its determination to comply by dedicating an officer of the company for data (and privacy) and establishing organizational policy to ensure data protections of privacy information. In addition, it focuses on how a company identifies privacy data, where is that data stored, transmitted or processed. Additionally, it also requires people to understand their processes using this type of data. It requires the ability for an organization to allow any consumer to "opt out" of using their data. To do that, all organizations must clearly explain to each consumer HOW you collect, store, transmit and use in what processes their personal information. A final tenant is of course breach notification. That is the high-level basics of the law. But, HOW do you implement (and in 99% of the cases, retroactively) to this standard?

Let's start with the comparison of GDPR to other known standards. We see that GDPR isn't well aligned to NIST standards. We do see that GDPR is aligned more closely aligned with ISO 27001. It is not exact but much closer. On the surface, this makes sense. ISO 27001 is very prolific in European organizations. But, where is the focus within the stack? Is it focused on Management, Operational or Technical Security Controls? Does it have Resiliency built in? From my perspective, GDPR is Managerial and process-oriented Security Controls. There isn't a technical focus. It does require an enormous amount of Cybersecurity Awareness regarding privacy. It does require an enormous amount of Cybersecurity Awareness of your architecture and systems. And, mot importantly, it does require an exacting knowledge of your data (what types, where is it stored, processed and transmitted, who has access, and can consumers opt in or opt out).

From an implementation perspective, where do you start? Let's assume for a moment an organization knows its data. (That means they have a data dictionary and tracked repositories and a quality Configuration Management Database [CMDB]). Where does that data come into the organization's environment? That is the boundary of control. So, that becomes the GDPR Trust Boundary for our organization. Now the organization is responsible for ALL GDPR data inside that

GDPR – How to Implement

Organizational GDPR Trust Boundary. That means they should understand how to traverse that boundary securely. Then the organization needs to make architectural decisions. Where is the GDPR data going to be stored? Do you want to try to create a GDPR protected environment throughout your entire IT, ICS, SCADA, IoT, CPS and cloud environments? Or are you going to isolate and containerize a specific area of your infrastructure to be the authorized container/location for GDPR data and bring that to the appropriate standards? HOWEVER, that becomes problematic if you have applications that crosses GDPR and non-GDPR datasets. The application needs to handle both. The application needs to handle the concept of consumer opting out of storing their personal data. Since GDPR requires protecting the data during storage, transport and processing, we also need to look at the transport layer that carries GDPR to ensure compliance. The revelations of these challenges don't even begin to discuss process or application challenges in handling this type of data. There is nothing from the engineering design approach that focuses on resiliency to protect the privacy of GDPR data either.

So, what are these points to dig into?

- **Where is the GDPR Trust Boundary?**
  - **External to Internal**
  - **Internal to Internal**
- **What transport protocol to protect GDPR?**
- **GDPR Architecture decisions**
- **GDPR Application mapping**
- **GDPR Datastore mapping**
- **GDPR Engineering design**
- **Resiliency throughout Architecture/Engineering/Process**

Obviously, there is even more in the details and, of course, down to the Security Control level. And, if we were designing a system from scratch it would be entirely easier than retrofitting existing environments to this standard.

This is where Eigenspace uses the Cybersecurity Order of Operations Methodology (COoOM) to understand all the standards and frameworks an organization is either regulated, required or choose to honor in their organization. The COoOM, provides a way for an organization to understand each of their Security Controls and their responsibilities to laws, regulations, standards and frameworks. For instance, an organization may need to be compliant with OMB, NIST CSF, ISO 27001, PCI-DSS and GDPR. How do you do that? COoOM can provide a singular and comprehensive

GDPR – How to Implement

list of Security Controls that has been deconflicted and aligned for all these (and more if required) regulations/frameworks.

My final thoughts on GDPR is organizations should take a deep breath and address it like most other audited functions. For those who have participated in cyclic audits like Sarbanes-Oxley (SOX) or ISO audits know it all begins with SCOPE. You define scope so that audits know where their boundaries are. Think the same way. Where is GDPR and where can you contain it, so it can be managed to this new standard. To me, that is the secret to becoming GDPR compliant.

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us