The CISO'S Guide to GDPR: Q&A with Thomas Fischer

2018–03–27

hackerone

"I am by trade now a CISO. So I have to care about risk and compliance all the time, which is really exciting. I sold a little bit of my soul to do that... In my role of CISO, I have to care what GDPR is, and I went a little grayer in the process. So, I'm cautiously optimistic that Thomas can help us navigate the waters because honestly, for every person I talk to I get different answers to my questions..."

BRUCE POTTER
CISO, EXPEL

Maybe you can relate to Bruce. The above quote, in fact, is how Bruce introduced Thomas Fischer at the ShmooCon conference in Washington DC for his talk titled, Don't Ignore GDPR, It Matters Now.

Bruce looks to Thomas (as do others), as an expert in GDPR and so we recently caught up with Thomas for his help in answering some questions for us on this hot topic.

1 GDPR is going to take effect soon, but so many things are still unknown. What are you hearing from CISOs and others? What's top of mind for them with respect to GDPR?

There are three main concerns that have emerged from the discussions with CISOs that I have had regarding the GDPR. I wish it were otherwise, but the one thing that's top of mind for the CISO is the maximum potential fine for non-compliance with the regulation. For me, much of the panic around the new fines has been driven by vendor marketing emphasising the 'FUD' (fear, uncertainty & doubt) factor. I would much rather CISOs focus their attention on the things they can control and can implement to comply. This includes ensuring proper accountability is in place, personal data is correctly and securely used and stored and putting in place a means to demonstrate this.

Second, I believe that there's still a deep lack of understanding, or perhaps confusion, as to exactly what needs to be done to comply with the GDPR. Many CISOs are struggling to confirm exactly what is affected by the GDPR, understand the GDPR's definition of personal data and how to determine what personal data they hold. This confusion probably stems from the need to both protect a data subject's personal data whilst also meeting the original intent of the GDPR, which is to give data subjects more power over their personal data.

Thirdly, I have heard several stories about the colossal scope of work the GDPR represents. Fundamentally, CISOs are beginning to see that the GDPR will require nothing short of a paradigm shift in how companies treat personal data – from something that they owned, to something that has been loaned to them.

2 Are the companies you speak with or hear from generally on track to be compliant by May 25, or are they taking a "wait and see" approach?

Most companies are taking a proactive approach to the GDPR, ranging from simple compliance activities through to a full-scale GDPR implementation project to roll out changes across their organisation. The organisations that I have spoken with that are taking a "wait and see" approach are doing so primarily because they believe that the DPA (Data Protection Authority) will not be able to enforce the corrective actions and fines with any credibility. That said, the stance is a rare one and I've since seen some of these "wait and see" organisations reverse their position.

Regarding preparedness, what has surprised me the most is the belief still held by many companies – and often those based outside the EU – that they still have years to comply. Of course in reality, the EU adopted the regulation in April 2016, it came into force May 2016 and the two-year post-adoption grace period ends in May 2018 meaning that the GDPR will be enforceable.

3 Can smaller or lesser known companies skate by under the radar or should every company of every size be taking GDPR compliance seriously?

No, the GDPR will affect every company, of every size. This goes back to the foundation of the GDPR, which is to give greater rights to the data subject to control their personal information. A data subject will be able to exercise their rights, regardless of the size of the company that has collected their personal data.

At some point in time, even the smallest companies will form business partnerships or interactions that will require them to demonstrate that they comply with the regulation. The GDPR takes into account that companies will work with partners or suppliers and defines the shared responsibility between a data controller and a data processor.

As an example, I recently advised a business services company based in Switzerland. It is a relatively small operation with less than ten staff. Its customers are already asking about how the company will comply with the GDPR and what it is doing to protect personal data. This is a good example of why all companies need to take data protection seriously and be proactive about the GDPR.

4 Some have said that the authorities will look to make an early example of a high-profile company who violates GDPR. Do you think that's likely, based on past activity?

I have had discussions about how some large organisations that are known to be lacking in proper controls around and misuse of personal data are indeed preparing to be hit by a flood of data subject requests and DPA notifications. That said, it is more complicated than simply issuing a fine to a company. Guidelines have been set out by the Article 29 Working Party (WP29) on how supervisory authorities should carry out enforcement. Ultimately, it starts with an investigation if the DPA is notified of an infringement. The investigation needs to determine several things including the seriousness and impact that it had on a data subject as well as understanding if actions have already been taken to mitigate the incident. Based on this evaluation, the authority will decide what corrective measures need to be addressed and if a fine is necessary.

5 Others point to the fact that governments are ramping up enforcement capabilities (with the UK alone hiring 200 new enforcement staff). Do you think fines will be rampant once GDPR takes effect?

While the GDPR defines some rather hefty fines, the purpose of the regulation is not to just issue as many fines as possible. It's about setting a framework for DPAs and companies to be able to address data subject requests and complaints, investigate any violations or breaches and then recommend corrective measures.

Personally, I think the fines are a double-edged sword. If DPAs start issuing lots of fines, I believe the purpose of the regulation will be lost in a quagmire of endless court cases. However, being able to fine companies does give the DPA both the authority and a means to finance its mission. There is also strong guidance around issuing administrative fines that states that they need to be consistent and fair across all EU member states.

6 You recently commented that GDPR flips the mindset on data from companies owning the data to people owning their data. Is that the future mindset that companies need to start considering now, or is it all still up for debate?

Yes, this is something that I explain quite often. Many articles, discussions, and executives miss the fact that the main purposes of the GDPR is to give EU citizens more control over their personal data and how it is processed. The principal is that, as an EU citizen and thus data subject, I am providing you, the company, with my personal information for a specific use. You are now entrusted by me to safeguard my personal information and use it properly and according to the agreed upon use. However, I still own the data and I am still in control. I can, at any point, come back and for example revoke your right to use it. This is not up for debate. The data subject rights are, for me, a clear validation of the transfer of ownership back into the hands of the data subject.

7 What is the Article 29 Working Party and why should companies be aware of it?

The Article 29 Working Party, WP29 for short, works on behalf of the EU Commission to interpret and define data protection activities. It is an authoritative board composed of data protection authority representatives from the EU member states, as well as from the EDPS (European Data Protection Supervisor) and EU commission. One of WP29's main missions is to help interpret the GDPR and provide guidance on how it should be implemented.

Companies should be aware of WP29 because the information it publishes can help them better define and understand their responsibilities under the GDPR. WP29 provides guidance on what personal data is, how to carry out a data protection impact assessment, the breach notification process and more.

8 DLA Piper recently published guidelines on consent, for example. Will companies be expected to follow every suggestion that comes out of the Article 29 Working Party? Or are they just suggestions?

The DLA Piper blog references two separate documents from WP29. The first is WP29's draft 'Guidelines on Consent' and the second is WP29's 'Opinion on the definition of consent'. It's important to distinguish between the two, because Guidelines will have more of an impact on companies than opinion papers. This is because Guidelines are published to help DPAs and organisations understand the GDPR rules and, importantly, provide frameworks and recommended actions to comply with the regulation. The 'Guidelines on Consent' referenced in the DLA Piper blog is a detailed analysis of what consent, in the case of the GDPR, is. Companies should use the guideline document to ensure their approach to consent or lawful

processing is in line with what the DPA will be looking at. To summarise, while Guideline documents from WP29 may seem like suggestions, it's in companies' best interest to take note of them, because they will provide clear advice about meeting the GDPR itself.

9 Amazon seems to be very proactive on GDPR compliance and disclosure, and in ensuring AWS is compliant before GDPR takes effect. Why is their "Data Processing Agreement" so important to their customers?

Amazon's Data Processing Agreement is important to both AWS as data processor and also customers that are either data controllers or data processors themselves. Article 17 and 28 actually require that the data controller (i.e. the company collecting the personal data) has legal agreements in place with the data processor (in this case, AWS) that ensure that personal data is secured and processed in a consistent manner and that all parties in the processing chain only use the data as it was consented to be used.

By providing its own Data Processing Agreement and asking customers to accept the new terms of service for the GDPR, Amazon is helping customers by providing the frameworks and agreements that will be mandatory under the GDPR.

10 Salesforce, too! What should companies be asking their data/computing/cloud vendors about GDPR?

The GDPR defines the relationship between companies and their suppliers, partners and vendors very clearly as it recognises this is a huge part of modern business. Companies collecting personal data need to ensure that any service they are using complies with the GDPR. This means ensuring that personal data is secured and processed according to the reasons for which it was collected. Importantly, companies need to ensure that their service providers or vendors can demonstrate how personal data is secured and that they have a framework in place to report any violations or investigation requests from the DPA.

11 Does GDPR treat data differently if it's managed by a company vs. a company's vendor?

The responsibility for protecting personal data is equal across all organisations, meaning that all parties processing personal data must process it securely and comply with the data subject rights and processing controls. For example, data processing needs to be done according to the consent given by the data subject. If the data subject wants to update their personal data or request to be forgotten, this request must be completed consistently throughout the entire processing chain.

12 It seems to be getting more confusing as we get closer to May. What's your overarching advice for most companies today?

I believe that much of the confusion surrounding the GDPR has come about because companies are, for one reason or another, too focused on just one or two aspects of the regulation like consent and the fines. In fact, they should consider moving away from handling this as compliance activity to focus attention on ensuring they can demonstrate accountability for all data subject rights and personal data processing activities.

Companies should see this more as a transformation project and build an implementation plan that is organisation-wide. They should focus activities by implementing work streams that cover aspects such as design, gap analysis, data inventories, retention and expiration, handling breaches and complaints, review consent management, ensure data subject rights are achievable, data protection impact assessments, awareness, 3rd party management, and finally, adopt data protection by design into the build, maintenance and operation process.

I always start GDPR discussions with the big picture questions: Do you know what personal data is being collected and processed? Do you know where the personal data is stored? Can you demonstrate what has happened to personal data? Does your breach notification assessment correctly detect and identify personal data misuse, destruction, alteration or exfiltration? Being able to answer these questions will put companies on the right path to reducing the confusion.

About Thomas

With over 25+ years experience, Thomas Fischer (@FVT) has a unique view on security in the enterprise with experience in multi domains from risk management, secure development to incident response and forensics.

Thomas has held roles varying like incident responder to security architect for fortune 500 company to industry vendors and consulting organizations. Thomas currently plays a lead role in advising customers while investigating malicious activity and analyzing threats for Digital Guardian. Thomas is also an active participant in the infosec community not only as a member but also as director of Security BSides London and ISSA UK chapter board member.

Enjoyed reading this post? Please share it on Twitter.

You can read more GDPR content pieces by checking out the GDPR content tag on our blog.