EU GDPR

Key activities to get you compliance-ready

EU GDPR impacts the compliance landscape way beyond the coastline of the UK. Aiming to provide protection for consumer's sensitive information, these new regulations that come into effect on the 25th May 2018 will require that all businesses which handle personal data will need to comply with the new rules put in place to ensure its protection. To prepare, your organization needs to get, well, organized - within the two year timeframe. So we've put together a brief overview of key activities that will help get your organization in shape for the big day.

Communicate impending changes to C-Suite

Ensure that your organization's key decision makers are aware that the law is changing and what these changes means for the business and how it operates. EU GDPR will impact significantly on your organization's security posture so ensuring everyone is aware of the potential impact helps get everyone on board.

 Do this as soon as you can prior to kicking off your GDPR-readiness project.

Identify the information your organization holds

You can't protect sensitive information if you don't know what you have or where it resides. Conduct a thorough audit of your business critical data to identify those assets and where on your networks they reside. Utilize data diagrams & info structure maps to help map out the data and provide quick visibility around its locations across your networks.

Between one week to 4 months, depending on the size of organization.

Review and establish access rights

Review access permissions to data across your entire estate. Identify existing permissions and revise/implement policies that ensure only those with a business need are provided with access to your data. En-sure you have a process set up for regular review and revision to ensure robust data governance and implement a system that can deliver a detailed audit trail of file permission changes that's clear and up to date.

Between a week and one month You should finalize by November 2017 to be ready by 25th May 2018.

Implement robust data monitoring capabilities

How? It's no good having the right access policies in place if you don't have visibility on their effectiveness. A monitoring solution will help to identify any existing security gaps, provide visibility around data movement and deliver detailed reporting and forensics analysis when you need it. And if your monitoring activities highlight issues, go back and remediate them and review again ad infinitum until you've got it right.

One week to a month

Create your Incident Response Plan

EU GDPR requires that you notify the right authorities of a data breach, or face the (hefty) fines if you don't or can't. Your breach notification process will be part of your Incident Response plan that comprises 4 stages - immediate action to stop or minimize the breach; post-breach investigation processes; restoration of affected data and resources and of course breach notification.

One week to a month

Form a security governance group

There should be a core group of individuals to oversee your organization's privacy activities and who understand the requirements of EU GDPR compliance. Your governance group should oversee the development of processes that measure where you're at with your privacy efforts, reporting regularly on DP status and implementing statements of compliance that will be required as part of your organisation's compliance reporting.

Implement as early on in your GDPR-readiness project

### Ensure the right staff are in place

If you're organization employees over 200 people then you might need to consider the appointment of a Data Protection Officer. However if that's not the case you'll still want to ensure that, beyond your governance group, you have a training plan for existing staff or that you're actively looking to fill the specialist roles you'll need to ensure that you have the right skillsets in place to manage your compliance requirements going forward.

Plan early on in your GDPR-readiness project to ensure resources are in place and hiring timeline is accounted for.

Don't panic!

Whilst the EU GDPR is great for customer privacy, there's no doubt that it's created big challenges for organizations who need to reconsider their approach to security in order to ensure compliance. But this is a positive move. No longer a 'nice to have', a robust, reliable security posture is critical for all organizations who must take a socially and morally responsible stance when it comes to protecting sensitive information. This translates into transparency, increased performance (both for your business and end-users) greater cost efficiencies, improved control and overall a more streamlined approach to your security. We call that a win-win situation.
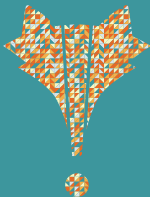
For more information about EU GDPR and how ZoneFox can
help with Compliance, get in touch - and get organized!

info@zonefox.com   www.zonefox.com/contact-us   +44 (0) 131 208 1461