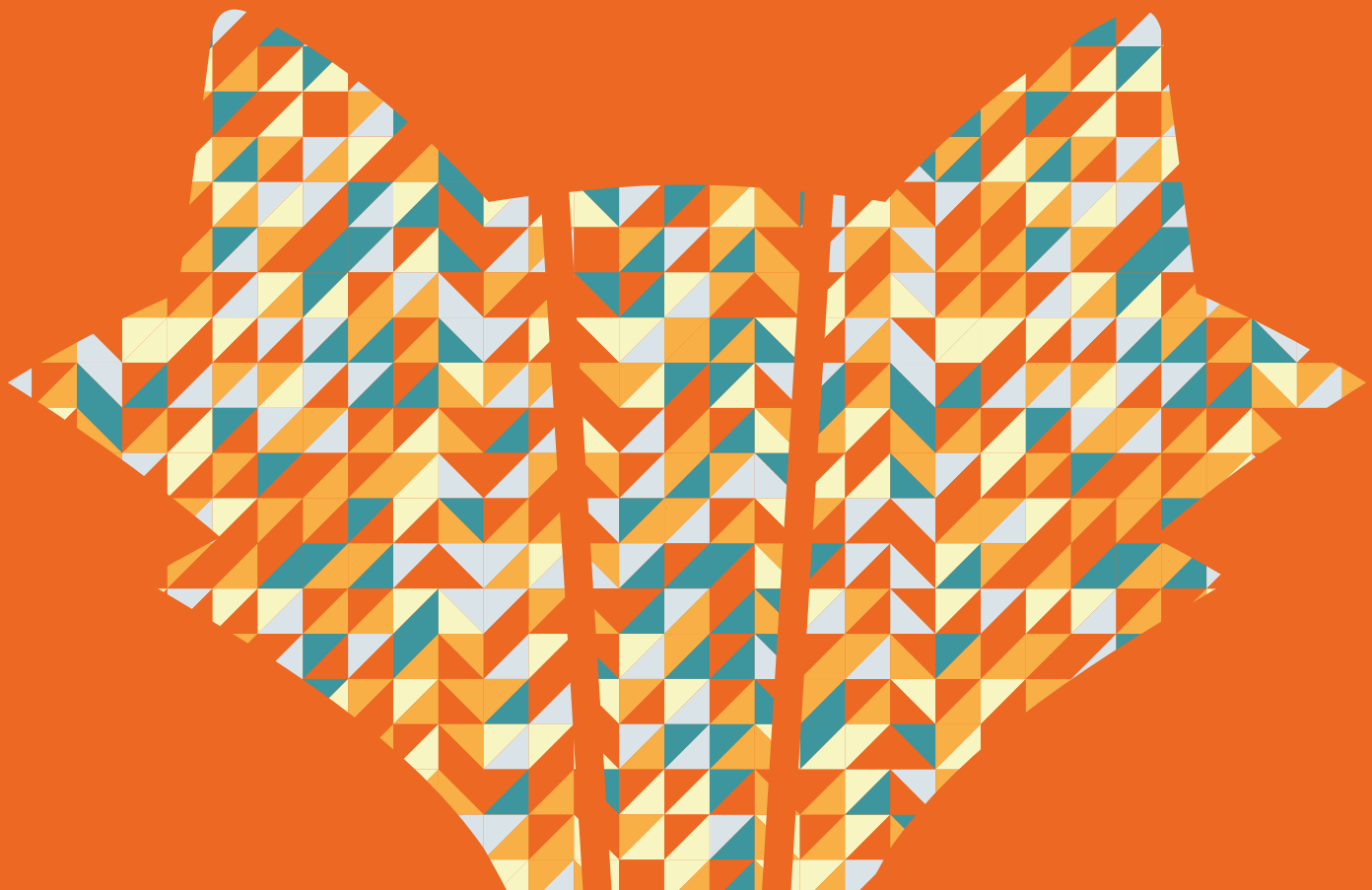
ZoneFox

Whitepaper

Everything you wanted to know about EU GDPR - but were afraid to ask



ZoneFox

Introduction

Information can be considered the new global currency, and it has become more apparent over the years that the protection of user info is paramount for any organisation.

The European Union is striving toward greater protection of its citizens' data by creating and implementing the GDPR. The General Data Protection Regulation of the EU is a new regulation designed to enhance data protection for EU citizens by helping regulate data protection measures within the EU, as well as data accessed by EU citizens within non-EU organisations.

While a highly ambitious objective, the GDPR may very well revolutionize organisational data protection as we know it. So come May, 2018, will your company be ready to embrace the change brought forth by the GDPR?

What does GDPR bring to the table?

In order to enhance data protection for EU citizens, the GDPR implements the following high-level controls:

- Expanded territorial scope
- Single set of rules for EU member states
- organisational responsibility and accountability
- Explicit consent requirements
- Subject access requests
- Right to erasure for user data
- Data breach notification requirements
- Appointment of a Data Protection Officer

Expanded territorial scope

The GDPR will apply to both organisations (data controller/processor) and data subjects (users) based in the EU, as well as non-EU organisations that process or control EU citizens' personal data. Personal data is defined with a rather large scope, including a user's name, social media posts, banking information, and IP address. The GDPR does not, however, cover personal data processed for investigations by law enforcement or national security agencies.

Single set of rules - or a "one stop shop"

Each EU member state will be appointing a Supervisory Authority; the regulator of all things GDPR. The SA will attend to complaints and investigations based on the GDPR, and sanction any offences. For organisations doing business in multiple EU states, the SA will reside at their main location. Each member SA will need to cooperate and coordinate with other SAs in joint operations. The European Data Protection Board will have oversight of the SAs throughout the EU, ensuring that the member SAs get along, and providing ultimate decisions should an organisation disagree with a ruling by their member SA.

Organisational responsibility and accountability

Organisations will be required to ensure that they are adhering to the GDPR. It is each organisation's responsibility to audit their practice to ensure that they are incorporating privacy by design and data protection by default. This noble goal is intended to ensure that organisations are not set to "disclose by default".

Organisations must also keep true to the original purpose(s) for which they have collected user data. If the new purpose is compatible with the original purposes, however, the GDPR will abide. On top of these responsibilities, organisations exporting data to third countries must also ensure that the country in question can ensure adequate privacy and protection measures. Countries that do not comply with the GDPR can face penalties up to 4% of annual global turnover or 20 million Euros, whichever is higher.

Explicit consent required!

In order to process personal data, organisations will be required to garner consent from data subjects. Proof of consent will be required, as well as proof that the user was well informed and gave their consent of their own free will. The consent will need to be expressed by the acceptance of a clear statement, or the presence of an affirmative action. For minors, the default age of 16 years can be reduced to as low as 13 years old.

Subject access requests

Curious users of an organisation's information services will be able to create subject access requests to find out just how much of their personal data is being stored and used by an organisation.

Data controllers will need to respond to SARs within one month of receipt, without undue delay, although this period can be extended by two months in the case of overly complex or an excessive number of requests. If a SAR is "manifestly unfounded or excessive", the data controller may charge a small fee to cover admin costs or refuse to respond to the request.

Right to be forgotten (or erasure)

Data subjects have the right to be forgotten and have their data erased from the data controller's infrastructure if they withdraw their consent, if they object to the data being stored - based on legitimate grounds, of course, if their data is no longer necessary to the purpose for which it was collected, or if the organisation's data processing methods do not comply with the GDPR.

It should be noted that a data controller must also alert any third-parties with which they have shared the user's data, as due diligence must be observed in ensuring that any copies of or links to the user's data are removed as well.

Breach notification requirements

Always a touchy subject, data breach notification is no less important with the GDPR. Data controllers must notify their SA of a personal data breach within 72 hours after detection, where feasible. If the breach does not end up risking the rights and freedoms of the individual, there is more wiggle room.

If the data processor is separate from the data controller, the former must inform the latter on the double. Data subjects must also be informed ASAP of any breaches of their personal data. Again, if risk is mitigated by obfuscating or encrypting data in an effort to make it unreadable by a third party, a public announcement can be made in lieu of direct notification to each user.

Appoint a Data Protection Officer

If an organisation's core business focuses on the gathering and regular, systematic monitoring of personal data, they will need to appoint a DPO. The DPO should be an expert in data protection practices and legislation to be most effective. EU member states can add requirements as they see fit, as well.

The DPO will also have oversight of data protection impact assessments. DPIAs are a necessity if there are inherent risks to the rights and freedoms of data subjects. The assessment and mitigation of any risks to customer data leading to any potential compromise of the rights and freedoms of these data subjects, as well as an approval from the SA must take place before a data processor can commence any data processing activities.

How can I prepare for May 2018?

The GDPR is paving the way for government regulated data protection, and now is a great time to start getting on board. The implementation of this new regulation provides a great new opportunity to enhance your information security practice from technical, governance, and legal perspectives. Here are some tips to help you achieve compliance come May, 2018.

Proactivity is key

As in most information security initiatives, being proactive will greatly enhance your chances of success. Here are a few tasks you can do up front to get your ducks in a row:

- Audit any and all of your organisation's activities that involve the collection, processing, and storage of user data.
- What measures do you currently have in place to protect your data? Perform vulnerability assessments and penetration tests to determine if unauthorized access and downloading of your data is a possibility. This is also a great chance to test your data encryption standards.
- Understand any relationships with third party organisations. With whom do you share your user data, if any? How do third parties collect data from your organisation?
- Have your compliance officer and legal team go over your end user agreements to ensure that all of your data subjects are willfully agreeing to let you store and process their personal data.
- Lay out how you are using your end user data, and ensure that it is in line with what you tell your clientele. Engage a third-party to review your processes and agreements if possible, to get an outsider's opinion.
- Understand risks to your current data storage solution and create a risk registry if you currently do not have one. This is a great time to implement this practice if you do not already.

Get your Board on board

You'll need to outline your strategy to your board of directors. Here is some data to bring to those meetings to get the resources you may require:

- Any discrepancies between your end user agreements and GDPR requirements - as well as roadmaps and resource requirements to reconcile the two.
- Create metrics based on vulnerability assessments and penetration tests to outline any deficiencies in your data defenses. Don't forget to provide solutions to help fix any holes!
- Provide current and future-state data loss protection strategy that will help ensure compliance with the GDPR.
- Highlight any deviations from the GDPR, and lay out a strategy including technical, legal, and compliance measures that will ensure compliance - including measurements and timelines - leading up to May, 2018.
- GIve the board members insight into the inherent risks by showing off a risk registry pertaining specifically to GDPR controls and risk mitigations.

GDPR risk mitigations and information threat countermeasures

In order to obtain compliance to the GDPR, you will require some strong risk mitigations. Since user data is one of the most valuable and tradable artifacts on the Internet, having solid technical countermeasures and risk mitigations in place is key. Here are a few pointers in keeping your user data secure:

- Classify your data - this is the key to solid data loss prevention.
- Monitor your environment to ensure that your data stays put and prevent any user data from leaving your network.
- Encrypt your databases! This should go without saying, but recent events have shown us that some large organisations are still not encrypting. Make sure that you use strong encryption algorithms as well; if the bad guys get your data, at least they won't be able to read it.

Conclusion

While the implementation of the GDPR may seem kinda scary, this regulation presents a huge opportunity for CIOs and CISOs across the EU, and potentially across the globe, future state. Ensuring that your organisation is prepared for the GDPR implementation by planning well in advance will definitely pay off in the long run, and compliance to the GDPR may be the push your board requires to help get some of your key security and compliance initiatives funded! Whil 2018 will bring lots of change to many organizations, with the right planning your organisation can become an industry leader in data and information security.

ZoneFox

About ZoneFox

ZoneFox is a highly innovative Endpoint Monitoring & Threat Detection solution that delivers 360 visibility around endpoint activities, data flow and application behaviour. Protect your IP, maximize your existing security and stay compliant. To find out how, visiit www.zonefox.com.

ZoneFox