PARABLU

General Data Protection Regulation - eBook

PARABLU

May 2018

GDPR goes into effect

While there has been a fair amount of coverage in GDPR, it's importance and ramifications don't seem to have fully sunk in for so many businesses who either do business in the EU or have EU customers.

In case you didn't already know, the EU Commission, Parliament and Commission negotiated and finalized the text of what is called the "General Data Protection Regulation" (GDPR) in December of 2015. This was officially approved as Law in April 2016, which means GDPR goes into effect in May, 2018. And, if you're an organization that does business in the EU or even has customers from those geographies, this could significantly change the way you do business.

In this guide, we'll enumerate the key factors you should if you're an organization that does business in the EU or even has customers from those geographies,.

GDPR Compliant Organization

Protection of the data, especially customer's PIIs

+

Encrypt your data in the cloud. Have control to your encrypted keys

+

Quick response time to report a data breach

1
Why GDPR?

There are primarily two drivers for GDPR.

While EU does have an existing directive under data protection called the “Data Protection Directive” (DPD), the fact that it was drafted in 1995 during the pre-cloud, pre-social media era meant that it needed some serious updating.
Also, the DPD acted more as a template or guidance based on which individual EU nations developed their own legislation. This led to inconsistencies in laws between different EU nations making it harder for businesses to understand laws and comply.

Most importantly, since the EU believes that data protection should apply across national boundaries, GDPR seeks to regulate not only the protection of data within the EU, but extends the law to all businesses that hold data about EU citizens, even if such a business is based outside the EU. So, in cases where a business is based outside the EU, but offers goods and services to individuals in the EU or monitors their behavior, the GDPR will apply. This means that a lot more businesses than previously, especially based in the US and other parts of the world now come under the ambit of GDPR.

Lastly, because GDPR is a regulation (and not a directive), it doesn’t require each EU nation to pass any laws for it to take effect. It takes effect automatically on May 25, 2018.

28000

Data protection officers will be employed in Europe alone

PARABLU

#2
How it affects everyone

The GDPR affects several stakeholders and affects them differently. For instance:

- If you are an EU member nation, you will need to set up an Independent Supervisory Authority that can review complaints and set penalties.
- If you're a business, you will need to demonstrate compliance. Towards this end, you'll need to document their processes and may also have to appoint a Data Protection Officer
- Individuals have the most to gain. If you're an individual in the EU, you will have rights to access your data, ask for rectifications, demand portability of data (to alternate vendors), and to ask for erasure based on grounds such as unlawful processing or withdrawal of consent.

Also, transfers of data out of the EEA (European Economic Area) to the US which used to be governed by the Safe Harbor rule will now need to be compliant with a new guideline called the Privacy Shield which imposes a greater standard of protection and compliance that US companies will need to adhere to.

One of the directives that has received a lot of coverage in the media is the Mandatory Breach Notification Scheme, because of the public relations fallout it could cause an organization.

If a business suffers a data breach in the form of a loss (accidental or unlawful), alteration of data, or unlawful access to personal information), such a breach needs to be reported to a Data Protection Authority within 72 hours of your organization becoming aware of it.

Not just that, if the breach is likely to result in discrimination, fraud or identity theft, financial loss, damage to reputation, or any other economic or social disadvantages to the subjects, then the breach will need to be reported to each of the subjects (individuals) as well – even *before* the Data Protection Authority is notified.

Quite significantly, if businesses have implemented appropriate technical security measures with respect to the data affected by the breach, they may not need to notify data subjects. For instance, if prior to the breach taking place, the data had been rendered unintelligible, by means of technologies like encryption, businesses will not need to notify data subjects of the breach.

What has also grabbed attention in the GDPR is the stiffness of the penalties involved. Certain breaches can result in a fine of € 10M or 2% of a company's annual revenues – whichever is greater. More serious breaches could result in a fine that is the greater of € 20M or 4% of a company's annual revenues. In some cases, the Data Protection Authority can impose a complete ban on data processing operations by an organization.

10

or more Employees in your company? You are under compliance radar

3
What you should if you're a Business

If you're a business that is new to the EU market, then some aspects of the GDPR might seem challenging. But if you are a company that follows IT industry best practices (like PCI-DSS, SANS, ISO 27001 etc.), you probably won't find GDPR too burdensome.

While there could be several things that you should do to be compliant, one area to focus on immediately is protection of the data you're storing, especially Personally Identifiable Information about your customers.

With increased usage of cloud storage services, the risk of exposure for a business is now that much greater. Keep in mind the mandatory breach notification clause. Think about solutions that can effectively encrypt your data in the cloud. And, when you think about data – think about all data – Primary storage, Secondary storage and data you store in the cloud using SaaS based cloud storage services.

Encryption is a suggested, even if not mandated way to protect customer data. Many regulations may not be prescriptive about encryption but almost all of them consider it an acceptable and effective way to protect data. Taking that important step and including that in your data processing workflow will significantly reduce your liability in terms of reporting breaches, should they occur, and help you avoid crippling penalties.

72

Hours is what you got to report a data breach

Parablu Solution

As a business readying yourself for GDPR, encrypting your data in the cloud should arguably be your highest priority. The solutions from Parablu can integrate seamlessly into your current infrastructure like MS Active Directory, MS Azure or MS Office 365 to make this seamless for your users and your administrators.

Parablu has created a secure storage layer which can be layered on top of any cloud storage offering to store enterprise data safely and securely. Businesses implement this in the form of a Privacy gateway called BluKrypt which is designed to cipher data as it leaves an enterprise and goes into the cloud. Most importantly the keys to decipher the data are retained by the business and nobody else – thus effecting a clear separation of duties. BluKrypt not only uses encryption to obfuscate data, but applies additional techniques to considerably increase the barrier a potential attacker would have to overcome to gain access to sensitive information.

Parablu's offerings come in the form of BluVault – a secure cloud backup solution, BluSync – a secure File Sync and Collaboration solution, and BluDrive – a secure File Sharing/Transfer solution. All of them utilize the core Parablu BluKrypt technology to provide a safe container for data stored in the cloud.

Solution features:

- Total control of encryption keys
- 100% protection and visibility into compliance information
- Auditable trail across devices
- Integrates into your current infrastructure
- Scheduled backups via controlled policy
- Free flow of data with 100% encryption
- IT policy and compliance alignment

Signup for a free trial.
Be a GDPR Compliant Business, Effortlessly.

info@parablu.com

www.parablu.com

USA

1600, Duane Avenue,
Santa Clara, CA 95054
Phone: +1 (650) 762 6641

INDIA

No.62/1, NR Towers, 3rd Floor,
19th Main, 17th Cross,
HSR Layout – 4th Sector,
Bangalore – 560102
Phone: +91 80 6940 0005

ABOUT US

Parablu, an award winning provider of secure data management solutions, engineers new-age cloud data protection solutions for the digital enterprise. Our Privacy Gateway powered solutions protect enterprise data completely and provide total visibility into all data movement. Our suite of products include: BluKrypt - a Privacy Gateway that completely secures critical data on the cloud, BluVault - a powerful and secure data backup solution designed for the cloud, BluSync - a secure file sharing and collaboration solution for the agile enterprise, and BluDrive - a secure file transfer solution. These solutions easily integrate with your existing infrastructure making it a seamless solution for your enterprise data protection and management needs. Get a demo today. Visit www.parablu.com for more information