PARABLU

Regulation: Four ways your backup strategy impacts GDPR compliance

The GDPR (General Data Protection Regulation) is a new privacy regulation that came into effect in the EU back in 2018.

GDPR from a regulatory standpoint made the headlines because of the aggressive position it took (more than any previous regulation) around individual privacy and how much businesses should be held accountable for them. But as a regulation overall, it shares quite a bit of the same fundamental tenets as regulations that have come before it. In other words, if you're a business that is already compliant with other regulations like SOX or HIPAA or any other regulation that governs your line of business, chances are you won't have too much difficulty complying with GDPR.

While GDPR is a lot like other regulations, it did break new ground in some ways – especially in the way it views the rights of the individual and the penalties it assesses.

GDPR and Personal Privacy

While GDPR is a lot like other regulations, it did break new ground in some ways – especially in the way it views the rights of the individual and the penalties it assesses.

Let's see what makes GDPR different.

An aspect of GDPR, which garners a lot of attention is that the European Union has tended to place citizen rights at a higher plane than the Executive Branch's right to collect information on its citizens. One result of this is that individuals can invoke their "Right to be Forgotten" – in which case you will need to purge their data or at the least, make it inaccessible except for specific cases such as issues of public interest, legal compliance and public health.

GDPR and Geo-Locality of Data

GDPR also affects where you keep data and where you transfer it to. But unlike what most people think, GDPR doesn't dictate that EU data should not leave the EU. In fact, the GDPR has a lot to say about where data CAN move and these are detailed in **7 Articles (44 through 50) of Chapter 5** "Transfers of personal data to third countries or international organizations".

The summary is that the EU does allow movement of data to destinations outside the EU has data protection laws at least as strong as GDPR, or the entity the data is transferred to agrees to a legally binding contract around handling the transferred data – that has the same stipulations as to the GDPR.

Of course, in many cases, the simplest course of action is to have the data stay within the geography it was generated in – which is what leads to the common assumption that EU data cannot leave the EU.

GPDR and Data Loss

The way most people understand GDPR at a high level, they believe that they need to protect personal data from being "stolen" or "unlawfully disclosed". They don't think of data 'loss' or accidental 'destruction' of data as a breach.

But GDPR believes otherwise,

Article 4, (12) defines a 'personal data breach' as "…a breach of security leading to the **accidental** or unlawful **destruction, loss**, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;"

So, even an incident such as a ransomware attack, which strictly speaking isn't data theft – can have you run afoul of GDPR compliance.

Article 32, (1) – c further states, "The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including **the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.**"

Without getting into a lot of murky details – a 'controller' is the owner of the data – e.g. a business and 'processor' could be a cloud provider who stores and handles the data for the controller. But the thrust of the two excerpts above is very clear.

Being able to protect your data is a basic element of GDPR compliance. in other words, having a backup strategy is a critical underpinning to GDPR compliance.

Being able to protect your data is a basic element of GDPR compliance. in other words, having a backup strategy is a critical underpinning to GDPR compliance.

Mandatory Breach Notification

So, you're backing up your data. Is that enough?

It may not be. You need to make sure that the backed-up data itself can't be breached. The backed-up data must be stored securely enough that it cannot be lost, stolen, damaged, or altered.

And if the backed-up data is found to breached – then you have specific obligations under GDPR – like reporting the failure to the regulatory authorities in 72 hours or less.

Article 33(1) states that "In the event of a personal data breach, data controllers must notify the supervisory authority 'competent under Article 55'….Notice must be provided without undue delay and, where feasible, not later than 72 hours after having become aware of it."

This is called GDPR's mandatory breach notification clause – which is one other aspect of GDPR that has attracted a lot of attention.

You can also see here the variance in accountability that is tagged to **the Controller** vs **the Processor**. When a data processor experiences a personal data breach, it must notify the controller but otherwise has no other notification or reporting obligation under the GDPR. Note that the Controller (the owner of the data, the business) is on the hook, much more so than the Processor.

And it may not be enough that the Controller simply notifies the regulator. GDPR also says that if you think you've lost personal data, you may have to communicate that information to the impacted individuals!

Article 34(1) – "If the controller has determined that the personal data breach 'is likely to result in a high risk to the rights and freedoms of individuals,' it must also communicate information regarding the personal data breach to the affected data subjects."

You need to make sure that the backed-up data itself can't be breached. The backed-up data must be stored securely enough that it cannot be lost, stolen, damaged, or altered.

This is very important.
For companies, this is equivalent to going public with the fact that you had a breach!
But, there's an out.
Article 34(3) – The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
(1) the controller has 'implemented appropriate technical and organizational protection measures" that "render the data unintelligible to any person who is not authorized to access it, such as encryption'"

So, even if you do suffer a breach, while you will still need to report it to the regulator, you may get relief from having to go public and notify all impacted subjects – provided – you've encrypted your data!!

PARABLU

The importance of Encryption or Pseudonymization

There's a lot to unpack here. Let's take them step by step.

- You have to backup your data
- You have to keep your backed-up data safe
- If your backed-up data gets breached, irrespective of whether you trusted a cloud provider to keep it safe for you – it's still your responsibility
- In case of a breach, you need to inform an appropriate regulator within 72 hrs of the breach
- In case the breached data impacts the privacies of individuals, you will have to inform all the affected individuals – which has the same impact as going public with the breach
- But if you can prove that you adequately transformed the data using encryption or pseudonymization to ensure individual identities or their data are not at risk – you may not have to inform all the affected individuals.

While GDPR isn't prescriptive of any technology, the regulation strongly recommends pseudonymization and/or encryption of all personal data.

While GDPR isn't prescriptive of any technology, the regulation strongly recommends pseudonymization and/or encryption of all personal data. And with good reason – as you can see above.

But remember that encryption is only as strong as how safe the decryption keys are. It is important, as a business that you have sole control of the decryption keys. So, while you may keep a copy of your data in the cloud as a backup – you should ensure that the cloud vendor doesn't also have access to your data. You should make sure to encrypt that data and be the sole possessor of the decryption keys. This simple step, called separation of duties is an encryption best practice that is often overlooked by customers.

PARABLU

Four things to look for

Your backup strategy has a material impact on how compliant you are with GDPR. Remember that GDPR has teeth, perhaps even more so than previous regulations. It can hurt organizations where it matters most – Penalties can be as high as 4% of annual revenues, not to mention the negative public relations fallout.

When choosing backup software remember to look for an enterprise-class, commercial-grade solution that can do these Four important things:

- Show reports and audit logs of backup performance. You will need these in order to prove to internal and external audit teams (perhaps even an external regulator) that you have been performing backups regularly and consistently, as a matter of policy and have the evidence to prove it.
- Examine the encryption policies and mechanisms the software provides. Is the data encrypted? Is the data encrypted in transit and at rest? What encryption algorithms are utilized? How strong are the keys? Can you control the keys and change them at any time?
- Do you have a way to selectively and surgically purge data out of the backup archives? If you get a demand from a customer or a former employee who wants to exercise their "right to be forgotten", do you have the ability to surgically incise out their data out of your backup records?
- Does the software support geo-fencing or some other way to enforce data locality? Cloud hosted backups sound great – but do you know where the backup cloud is hosted and where your EU data might be ending up?

At Parablu, we provide industry leading solutions for backup, archiving, content collaboration and secure file sharing. We offer solutions that are hosted as well as on-premise. We've helped several customers accomplish regulatory compliance not only around GDPR, but regulations like SOX, HIPAA, etc.

Thoughts? info@parablu.com – we always love to hear from readers.