druva

5-Step Guide For GDPR Compliance

A Guide For Constructing Your Planning Timeline

This document provides a framework for all companies that have customers in Europe, as they have to prepare their own systems to meet the new needs of GDPR data protection regulations before 2018.

5-Step Guide For GDPR Compliance

At its core, the GDPR is about the rules companies must follow to ensure they are protecting Personally Identifiable Information (PII) in good faith. If a business breaches that faith, then they have to pay stiff fines and penalties. This is especially worrisome in an environment that is becoming increasingly mobile and cloud-based. Why? Because the data companies are tasked to protect is becoming both harder to track and at greater risk of being compromised, because it's no longer behind the firewall.

Use this **5-point plan** to prepare your own systems to meet the new needs of these data protection regulations before 2018.

What you need to do to get ready for GDPR:

1. Audit your current approach to managing data, to establish your current position and processes around data protection

You should carry out an audit of all customer data sets that are held across the business. Setting up new processes or augmenting the existing approach will only be possible if all instances of PII are known about.

- This audit will help companies understand current business processes that create or use customer data over time
- Include areas where customer data might not be adequately protected or managed at present, for example on individual employee IT assets. This audit will also help ensure that any changes to processes are put in place to meet future needs

2. Prepare the lead contact within the business when it comes to data protection compliance

Just as the EU will have a lead Data Protection Authority in place to manage GDPR, so businesses will need to appoint a lead for data protection and security internally as well. This role will be within IT, but will involve collaboration with both other groups within IT as well as other business teams / units.

This person should have the backing of the senior management team, and the person

who will provide evidence that rules are being followed.

- This person can lead an effort to review backup, disaster recovery and archiving processes. Rather than running multiple tools for different tasks across the company's data, consider a converged solution that enables a single view over the data, minimizing replication.
- In future, you will have to track data creation and automatically apply appropriate rules for personally identifiable information and customer data sets. Druva InSync can help to automate this process whether data is created within Cloud applications, on individual user devices or saved centrally.

3. Publish initial guidance to the business

Companies will have to make sure their internal teams are aware of their responsibilities in the same way. Revisit your existing business continuity policies and update them so they comply with GDPR. However, this policy document should also be shared with the rest of the business too. This awareness can help acceptance of any new processes as well as supporting any investment in new technologies.

- The Data Protection Board will share information for businesses on meeting the requirements of the GDPRs "right to be forgotten" rule. This will include where it is appropriate to delete data when customers ask for it, and where data can be legitimately kept after customers migrate away or no longer use a service.
- Align your own data archiving processes to make this task easier. Companies in regulated industries may have to hold customer data for years, even when the customer may no longer be purchasing goods or services. In the event of a data deletion request, there may be overlap between data for archival and that used for customer records.

4. Consolidate to make protection easier

For many companies, data will exist across their operations and within various IT assets. Today, around 40 per cent of company data never reaches the central IT platforms. To meet the needs of GDPR, it's worth looking at how to manage all the

data that involves customer information and where this can be reduced.

- Protect data on mobile devices and in remote offices in the same way as information that is held centrally. Druva inSync can scan files and data for potential PII and other sensitive data risks. This approach ensures that the organization knows where all its data is and can ensure proper security measures are taken to protect it.
- Encryption of data held on mobile devices is essential to protect customer data. This prevents issues if devices are lost or stolen leading to a compliance problem. If a device is lost or stolen, then the information on it should be wiped based on a command issued remotely too.
- Alongside encryption of data on the devices themselves, companies also have to encrypt data centrally too. For companies looking at storing data in the Cloud, control over that central data should be considered too. Look for encryption that ensures only the company can unlock the files involved.
- Apply policy management across files matters too – this centralisation of management can help ensure that all steps for compliance are followed automatically.

5. Plan for regular communication

GDPR compliance will be an ongoing requirement from 2018 onwards. To meet the needs of GDPR, communication between the IT team responsible for data protection and security, and other business functions such as compliance, legal and audit will be required.

Alongside this, you should think about communicating regularly with employees across the business to remind them around their roles and responsibilities for customer data.

- Define a communications strategy around data and how it should be protected. This should be given to employees as they start, as well as provided to refresh people on their responsibilities too.
- Alongside this, put together a communications strategy in the event of any data breach or data loss. As well as informing the local Data Protection Authority of the breach, the company will have to tell its customers and the wider public as well.

Using Druva inSync to protect and manage customer data

Druva InSync can track the creation of new files on laptops or mobile devices and automatically ensure that files containing customer data and PII are protected in accordance with company rules. This offers companies:

- Centralized visibility as to what is on devices and cloud services to assess and mitigate their data risks.
- Tools to help track and identify the potential for data leaks by alerting organizations of potential data risks on devices and cloud services.
- The ability to remotely wipe data on mobile devices to minimize exposure risks if a device is lost or stolen
- Help companies know what is on a device that was lost or stolen to assess level of exposure.
- Enforce encryption on devices (not all) to protect the files stored on them in the event the device isn't already encrypted

From a cloud perspective, Druva inSync can securely store the data we collect in the EU region to aid with recovery and deeper data assessment.

Follow these guidelines to get ahead of regulatory requirements when doing business with European customers, as well as cutting your data protection and disaster recovery costs.

To learn more about how Druva can help, visit www.druva.com/proactivecompliance

Druva is the leader in converged data protection, bringing data-center class availability and governance to the mobile and distributed enterprise. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

Q117-CON-10582

Druva, Inc.
1 888-248-4976
sales@druva.com
www.druva.com