10 STEPS TO GDPR COMPLIANCE

GDPR is a complex, wide-ranging set of rules most organizations doing business with Europe need to follow. It goes deeper than that. California and others are adoptingrules identical to or close to GDPR.

While it seems like GDPR is a lot to tackle, with large fines if you fail, you can get started by hitting the top areas first.
Here are ten steps to take – right now!

01 EDUCATION

Your organization, and all relevant stakeholders, should be up to speed on GDPR rules – which are now over two years old. First thing to discover – do you fall under these rules? If so, all employees that touch sensitive data, and especially the IT department, should know these rules and how to follow them.

02 FIND OUT WHERE YOU STAND

Companies are in various states of GDPR compliance, ranging from none at all to complete adherence. Before embarking more deeply on your GDPR journey, find out where you stand right now. What are your policies and practices regarding data governance? Are they presented to the outside world in an open and transparent way?

If there is already data governance documentation, review this and use it as a starting point for further work. Under GDPR, this kind of documentation is mandatory. This is all part of a data protection assessment, which you can learn more about here.

03 WHAT DATA DO YOU HAVE?

Most every organization has at least some sensitive information, and chances are it needs protecting. IT should discover this information through a data audit, where it came from, where it resides, and who has access.

04 POSTING PRIVACY POLICIES

If you fall under GDPR, you must have a privacy policy showing that you comply. That same policy is checked off when people visit your web site.

05 CREATE OR FINE-TUNE CONSENT PROCEDURES

Having a GDPR privacy policy is just the beginning. You need to get actual consent from outsiders, so-called data subjects, for any data processing – and this consent has to be detailed, specific and able to be audited This consent has to be easy to give, and just as easy to take back. Finally, document all instances and records relating to consent.

06 DEALING WITH SUBJECT ACCESS REQUESTS (SAR)

Under GDPR, any person who has data about them held in your organization can file a SAR, which means you must gather that data, provide it to them, and delete it if requested under the right to be forgotten rule.

07 BUILD GDPR STAFF INCLUDE DATA PROTECTION LEADS

Just as you need to educate all those who touch or process sensitive data, your IT and executive staff has their own responsibilities. A core decision is who has overall responsibility for data governance and compliance. At the same time, you need a point person to deal with regulatory authorities, who may or may not be the same person that manages governance.

08 DATA BREACH REPORTING

Blocking data breaches and reporting those that break through your barriers are key parts of the GDPR rule set. You need to have processes to prevent, investigate, report and respond to breaches. Blocking breaches is a top priority as fines are assessed for successful incursions. Having processes related to breaches can mitigate the monetary damages if one occurs.

09 KNOW WHAT RIGHTS DATA SUBJECTS HAVE

GDPR is all about protecting data and giving the data subjects deep rights. These include the right of access, right to be informed; right to restrict processing; right to data portability; the right to object, the right to not be subject to automated decision-making including profiling; and the right to erasure (the right to be forgotten).

10 CONTINUALLY UPDATE YOUR GDPR COMPLIANCE PLAN

It is clear that shops facing GDPR compliance need a plan that includes best practices and policies. This is just the start. Regularly review the plan to insure it is current with your organization's changes or modifications made to the regulations.

WHAT COREVIEW CAN DO FOR YOU

CoreScan from CoreView is a great tool for identifying data that falls under compliance rules. With CoreScan, it only takes a few seconds to audit your company's documents for Personally Identifiable Information (PII), and a few quick clicks to meet GDPR compliance.
Here are other key benefits:

- ✓ **GDPR Compliance Is Simplified**
  CoreScan helps you find sensitive data so you can manage data risks and remain GDPR compliant.
- ✓ **File Scanning Is Lightning Fast**
  With CoreScan, you can look through thousands of documents for sensitive information in mere seconds.
- ✓ **Taking Action Is Easier**
  Whether you need to redact info or delete files, CoreScan makes it easy to locate issues and take action.
- ✓ **Prioritization Is Built-in**
  Risk scores help you prioritize a file's threat level. Score more for credit card numbers, less for email addresses.
- ✓ **Reporting Is Fine-Grained**
  Scans can focus on particular folders, file types, PII and more, so reports show exactly where action is required.
- ✓ **Scan All Your On-Premises Documents**
  This on-premises GPDR software solution offers a comprehensive review of all key documents.

Finally, thanks to CoreScan, a company like yours saved $550,000 by reducing a Subject Access Request response time from 20 days with four employees – to under five minutes with just one employee.