

UK & EU **GDPR** Standard

Meet the requirements of the UK & EU GDPR standards while managing compliance with ALL your IT Security requirements...regardless of source.



History of GDPR

The standard was developed in 2008 by an international, grass-roots consortium, named the Center for Internet Security, which brought together companies, government agencies, institutions, and individuals from every part of the ecosystem (cyber analysts, vulnerability-finders, solution providers, users, consultants, policy-makers, executives, academia, auditors, etc.) who banded together to create, adopt, and support the CIS Controls.



Why is there a separate GDPR for the UK?

Brexit spawned the UK's GDPR, with the Government replacing references to things like the European Parliament and the European Council with UK institutions. For example, all references to the Surveillance Authority were replaced with the Information Commissioner's Office (ICO). The UK's GDPR very closely follows the EU's GDPR regulatory environment with some slight modification for the UK's version. Compliance Manager GRC has templates for both standards that account for the differences.



Who is Subject to GDPR?








In considering who needs to ensure that they are complying, GDPR has a worldwide remit to protect the data of its European citizens. This then means that if you interact with individuals who are based within the European Union, then it is likely that you will have some responsibilities to meet under the regulation.

With both data privacy and data protection being key themes of the GDPR if an organization collects or processes any personal data, including electronic information such as cookies, then they will need to take action to ensure the rights of the individual are protected

The GDPR Requirements

When an organization is considering the requirements for becoming compliant with EU GDPR, there are two key areas which need to be considered: There are seven key principles around which the specific requirements of the GDPR are based, covering eight specific individual rights that are granted to everyone covered by the law.

The 7 GDPR PRINCIPLES

-  Lawfulness, fairness, and transparency
-  Purpose Limitation
-  Data Minimization
-  Accuracy
-  Storage Limitation
-  Integrity and Confidentiality (Security)
-  Accountability

Both the EU and UK versions of GDPR are based on 7 key governing principals. The core idea is to limit and restrict as much as possible the amount of personal information and data about individuals that organizations collect and store.









When personal data is collected, the organization needs to clearly state why, and how the data will be used.

The principals also require organizations to ensure that the information they collect is accurate, safely stored, kept confidential and that they have a process for regularly deleting or anonymizing data that they no longer need or are actively using.

And perhaps most important, the organizations need to be able to prove that they are in compliance with GDPR (either UK, EU or often times both).

The 8 GDPR INDIVIDUAL RIGHTS

There are eight fundamental rights under GDPR.

-  Right to Access Personal Data. ...
-  Right to Rectification. ...
-  Right to Erasure. ...
-  Right to Restrict Data Processing. ...
-  Right to be Notified. ...
-  Right to Data Portability. ...
-  Right to Object. ...
-  Right to Reject Automated Individual Decision-Making.








When the GDPR was first released, the European Union were very clear within their implementation to ensure that every EU citizens should have several rights for the protection of their personal data and to ensure data privacy. From these, eight areas were established, each of which has its own specific requirements to ensure GDPR compliance.

These rights also require an organization to appoint a data protection officer (DPO) to help them implement and comply with the regulation, and with handling requests and inquiries from individuals about their rights. The European Union (and now, separately, the UK) have created a new standard for data privacy that is being widely adopted around the globe, including several states in the US.

Featured Product Highlights For Center For GDPR (UK & EU Versions)

Compliance Manager GRC allows you to use all of your current IT security tools, software and systems to meet the requirements of either version of GDPR (or both at the same time) . . . while you maintain compliance with all your other IT requirements, regardless of source. The built-in Standard Management Templates allow you to quickly determine if you can “check the boxes” for every control, identifies the gaps, and automatically prepares all of the documents you need to comply with the regulation.

Here are a few of the value-added features you get:

-  **Rapid Baseline Assessments** – Quickly identify gaps where you are not compliant with the law
-  **Technical Risk Assessments** – Full risk assessment to meet the GDPR security requirements
-  **Auditor's Checklist** – Easy access for auditors to quickly verify compliance with every requirement
-  **Plan of Action & Milestones** – Tracking and management of things you need to do to become compliant
-  **Policies & Procedures Manual** – Required documentation of everything you need to do.
-  **Automated Documentation & Storage** – Helps speed up the review vaprocess in the event of an audit or lawsuit.
-  **Bullphish Integration** – Helps with end-user training

Full-Featured to Manage the **GDPR Compliance** Along with All Your Other **IT Requirements**



Compliance Manager GRC is simple to use, and you don't have to be a compliance expert to manage the specific parameters for both the EU and UK versions of GDPR. Compliance Manager GRC automatically loads the specific requirements and controls you need to implement to comply. Best of all, you can also track everything that's in scope for your IT operation at the same time, and on the same dashboard, regardless of source.

COMPLETE: ALL-IN-ONE SOLUTION

Whether complying with the requirements of the GDPR, tracking the terms of your cyber risk insurance policy, or making sure your own IT policies and procedures are being followed, Compliance Manager GRC helps you Get IT All Done at the same time, and in the same place. No other Compliance Management software gives you this kind of flexibility.

AUTOMATED ASSESSMENTS & REPORTS

Assuring compliance with the GDPR (UK or EU versions) – as well as all your other IT requirements – is easy with Compliance Manager GRC. You get more work done with less labor, thanks to automated data collection, automated management plans, and automated document generation.

AFFORDABLE FOR ALL

Compliance Manager GRC is affordable, yet boasts the power and functionality most often found in expensive, enterprise-class governance, risk, and compliance platforms. Whether you manage compliance for your own organization, or are an MSP delivering compliance-as-a-service, there's a sensible subscription for you.



[Request a Demo today](#)

and discover the advantages of Compliance Manager GRC, the purpose-built compliance management platform for IT professionals

CMGRC EU & UK **GDPR** Data Sheet

