Compliance GDPR & GDPR-UK Manager

The General Data Protection Regulation (GDPR) is a law that took effect in 2018 that applies to any organization that processes or retains data on any citizen of the countries that form the European Union. While UK citizens were covered under GDPR when implemented, as a result of Brexit, on Jan. 1, 2021, the UK rolled out its own version of the law.

Both versions of GDPR (EU and UK) are the toughest privacy and security laws in the world. Each law includes hundreds of pages of IT requirements for organizations around the world. And the reach of the laws extend to every organizations in the world, regardless of location, if they target or collect data related to people in the EU or UK.

What is the UK-GDPR?

Following BREXIT, the United Kingdom implemented its own version of GDPR, which took effect on Jan. 1, 2021. While the UK version is largely based on its EU counterpart with many common requirements, the UK-GDPR changes key areas of the law concerning national security, intelligence services and immigration. Any website, company or organization that processes personal data from individuals inside the UK is required to comply with the UK-GDPR – even if the website or company isn't itself located within the UK.UK GDPR ISO 27001 Auditor Checklist

The ISO 27001 Auditor Checklist gives you a high-level overview of how well the organization complies with ISO 27001-2013. The checklist details specific compliance items, their status, and helpful references. Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

UK GDPR Evidence of Compliance

Compiles compliance information from both automated scans, augmented data, and questionnaires. Gathers evidence into one document to back up the Auditor Checklists with real data.

UK GDPR Data Protection Impact Assessment

The Data Protection Impact Assessment (DPIA) is the foundation for the entire GDPR compliance and IT security program. The DPIA identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of Personal Data at rest and/or during its transmission.

UK GDPR Risk Treatment Plan

Based on the findings in the GDPR Compliance Assessment, the organization must create a Risk Treatment Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, GDPR Manager provides a risk scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are issues solved. The Risk Treatment plan defines the strategies and tactics the organization will use to address its risks.

UK GDPR ISO 27001 Policies and Procedures

Guidance suggests that compliance with ISO 27001 can be used as a means to demonstrate technical compliance with the information security aspects of GDPR. The tool provides an “out of the box” version of policies and procedures for ISO 27001 for use by your organisation. These work in tandem with our GDPR P&P.

UK GDPR Policies and Procedures

One of the first requirements is to have a set of policies and procedures used to implement Personal Data security and compliance with GDPR. Some organisations don’t have a set of data protection policies – or at least one that conforms to GDPR provisions. The tool provides an “out of the box” version of policies and procedures for GDPR for use by those organisations.

UK GDPR Auditor Checklist

The UK GDPR Auditor Checklist gives you a high-level overview of how well the organization complies with the GDPR provisions. The checklist details specific compliance items, their status, and helpful references. Use the checklist to quickly identify potential issues to be remediated in order to achieve compliance.

Supporting Documents

UK GDPR Full Detail Excel Report

The Full Detail Excel Export includes every detail uncovered during the UK GDPR assessment’s network and computer endpoint scanning process. Details are presented in line-item fashion in an editable Excel workbook document. The report is organised by titled worksheets to help you locate the specific findings of interest, and problem areas are conveniently highlighted in red, making it easy to spot individual problems to be rectified

UK GDPR Compensating Control Worksheet

The report is used present the details associated with security exceptions and how Compensating Controls will be or have been implemented to enable compliance. Here you can document any false positives. You can also indicate if you have taken measures to reduce or avoid any issues identified in the assessment that might not otherwise appear in your assessment documentation. The benefit of this feature is that it adds back in the human element into the assessment and allows for explanation of special circumstances and specific environment requirements.

UK GDPR External Vulnerability Scan Detail by Issue

Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

UK GDPR Personal Data Validation Worksheet

During the Personal Data (PD) scan performed by GDPR Manager, suspected PD may be detected in files stored on network and stand-alone computers. The Personal Data Validation Worksheet report presents a record of which computer files were verified by a participant in the GDPR assessment process as containing actual instances of PD.

UK GDPR Personal Data Scan System Selection Worksheet

Understanding where you have Personal Data (PD) is an important component of GPDR compliance. The Personal Data Scan System Selection Worksheet allows you to specify which systems are scanned for PD during the assessment process. A comprehensive scan should be performed annually to help identify and document all potential locations for personal data as defined by GDPR.

UK GDPR Site Walkthrough Checklist

Assess the physical security and the workplace environment as it relates to information security. The worksheet will guide you through your assessment of the physical security. It is best done on-site as it requires identifying risk that may currently exist in the client's environment outside the computer network itself.

UK GDPR ISO 27001 Compliance Questionnaire

Guidance suggests that compliance with ISO 27001 can be used as a means to demonstrate technical compliance with information security aspects of GDPR. This questionnaire will collect information required to demonstrate ISO 27001 compliance that cannot be discovered through automated scans.

UK GDPR Compliance Questionnaire

The GDPR Compliance Questionnaire will collect information about the network and environment that cannot be discovered through automated scans. This includes information about the Data Protection Officer, principles relating to processing of personal data, privacy policies, and third-party information processors.

UK GDPR Asset Inventory Worksheet

The Asset Inventory Worksheet is used to augment the asset data that was collected during the internal network scan. Details include the asset owner, acceptable use, environment, backup agent status, as well as device and sensitive information classification. The Sensitive Information Classification is used to determine the risk to the organization in the event of a security incident where the asset's information is compromised.

UK GDPR User Access Review Worksheet

The User Access Worksheet is used to augment the user data that was collected during the internal network scan. Complete the worksheet to provide the additional information requested.

UK GDPR External Port Use Worksheet

This worksheet allows you to document business justifications for all of the allowed external ports, the protocol configured to use a specific port, and the documentation of any insecure configurations implemented and in use for a given protocol.

GDPR Risk Update Assessment Reports

UK GDPR External Vulnerability Scan Detail by Issue

Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

UK GDPR Risk Treatment Plan Update

Based on the findings in the GDPR Risk Update Assessment, the organization must create a GDPR Risk Treatment Plan with tasks required to minimize, avoid, or respond to identified risk to IT security and GDPR regulatory compliance.

The Risk Treatment Plan Update report contains a list of tasks that can be executed to mitigate identified IT Security risks and GDPR compliance lapses.

UK GDPR Network Change Summary Report

Every time you use GDPR Manager to run a GDPR Risk Update assessment on a given network, the GDPR Manager generates the Network Change Summary report.

This report compares the results the last Full GDPR Assessment with the Risk Update Assessment's network scan, local computer scan(s), and external vulnerability scan results performed during the Risk Update Assessment process.

This report details changes in the network's User Accounts, Local Computer Accounts, Active Directory (A/D) Computers, Non-A/D Computers, Non-A/D Devices, External Vulnerabilities, along with a Windows computer Patch Summary.

UK GDPR Data Protection Impact Assessment Update

The Data Protection Impact Assessment Update report lists IT Security risks identified during a Risk Update Assessment that impact the state of network security and GDPR compliance. The Data Project Impact Assessment Update identifies what protections are in place and where there is a need for more.

The Data Protection Impact Assessment Update report presents results in a list of items that must be remediated to ensure the security and confidentiality of Personal Data at rest and/or during its transmission.