14 endpoint management features

that can help you achieve & sustain

GDPR compliance

ManageEngine
IT Management, Simplified

Cyber attacks have grown immensely in recent times, leaving the data of both companies and customers vulnerable to threats. As a result, the European Union (EU) has created the General Data Protection Regulation (GDPR) to protect EU citizens' personal data from breaches and other kinds of misuse.

The GDPR's new set of regulations, which go into effect on May 25, 2018, will apply to both organizations that operate in the EU and those that gather information from EU citizens. Though this regulation is sure to provide tighter security controls for individuals' personal information, reaching GDPR compliance by the encroaching deadline will be a long and hard road for some organizations.

Achieving GDPR compliance is now a primary goal for major firms, though reaching this goal is complicated since the procedures and processes outlined in the mandate are vague. It's crucial to ensure your organization understands the personal data it holds, as not complying with the GDPR can result in a fine of four percent of your global annual turnover or €20 million, whichever is greater.

This e-book will help you understand the ins and outs of the GDPR so your organization can reach full compliance.

Who's behind the GDPR?

The EU currently has individual data protection laws that exist within each nation. The new norms and regulations in the GDPR were written after many discussions between the European Parliament, the Council of the European Union, and the European Commission.

Important GDPR terms

- **Data subject**
- **Data controller**
- **Data processor**
- **Data subprocessor**
- **Consent**
- **Data protection officer**

Data subject

A person whose personal data is collected and processed by an organization.

Data controller

The entity that defines the purposes, conditions, and methods of processing the personal data.

Data processor

The entity that has control over the personal data at the data controller's end.

Data sub-processor

When a processor shares the controllers personal data to a third party Organization, they are called as data sub-processor.

Consent

A specific, informed, and explicit agreement by the data subject to allow an organization to process their personal data.

Data protection officer

A data security and protection expert whose job is to ensure an organization sustains GDPR compliance.

Exploring and understanding the GDPR

With over 10 chapters and 99 separate articles, going through the GDPR's requirements can be overwhelming. For simplicity's sake, we can classify the GDPR broadly into two categories

- **Principles**
- **Rights**

Principles of the GDPR

The GDPR can be split into six privacy principles

- **Data minimization**
- **Purpose limitations**
- **Storage limitations**
- **Accuracy**
- **Lawfulness, fairness, and transparency**
- **Integrity and confidentiality**

Data minimization

Organizations should only collect and store personal data that is required for a specific purpose.

Purpose limitation

The purpose for which the personal data is collected should be specified to the data subject.

Storage limitation

Personal data that has been stored for a long time without any specific reason must be removed.

Accuracy

Data protection and security against data theft are the prime concerns when a company obtains personal data from users. This personal data should be kept up-to-date to ensure that it's accurate; any outdated information should be removed and/or replaced to avoid unnecessary breaches.

Lawfulness, fairness, and transparency

Organizations need to inform data subjects of the kind of processing that will be performed on their personal data and exhibit fair play while processing individuals' data.

Integrity and confidentiality

Organization should handle personal data in an appropriate manner using data protection and user privacy procedures to ensure no personal data is accidentally lost, breached, or damaged.

Individual rights of the GDPR

The GDPR mandates certain rights for individuals that organizations have to provide. Here are eight individual rights under the GDPR

- **Right to be informed**
- **Right of access**
- **Right to rectification**
- **Right to erasure**
- **Right to restrict processing**
- **Right to data portability**
- **Right to object**
- **Rights in relation to automated decision-making and profiling**

Right to be informed

Organizations are required to process information in a fair way, meaning data subjects must be informed if any breach or data loss affects their personal data. The language used during the personal data collection process should be simple and easy to understand.

Right to access

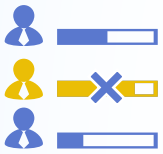
Organizations must provide data subjects with complete access to their personal data if a subject requests it. Data subjects must be able to see where their personal data is being stored and the security measures taken to protect it with complete transparency.

Right to rectification

When data subjects access their personal data, organizations must provide them with options to change or rectify their personal data without any restriction.

Right to erasure

If a data subject demands their personal data to be removed from an organization's database, the organization must comply immediately. No information about that data subject should be available anywhere within the organization once the subject has requested it be deleted.



Right to restrict processing

Even if a data subject has given an organization consent to process their personal data, they can later demand access to their personal data be restricted so the organization can only access it for certain purposes.

Right to data portability

Data subjects must be given the option to transfer their personal data from one vendor to another, a process which is known as data portability. Personal data stored in the original vendor's database must then be removed once the transfer is complete.

Right to object

The data subject has the right to demand that the organization stop processing their personal data for any reason.

Rights in relation to automated decision-making and profiling

If the data subject feels their personal data is being profiled for other marketing activities, they have the right to demand the organization stop processing their personal data.

With all these specifications to protect against the growing number of cyber attacks and data breaches reported every day, keeping your organization GDPR-compliant is possible, but it will require a bit of effort. Here at ManageEngine, we want to help you comply with the GDPR. That's why we've come up with a list of the endpoint management capabilities you need, to keep your your user's personal data safe and meet the GDPR's requirements.

How can Endpoint Central help you?

Endpoint Central is an endpoint management solution that helps you manage the data stored in all your network devices, including servers, desktops, laptops, smartphones, tablets, and more. After you become GDPR-compliant, *Endpoint Central* can help you keep your users' personal data secure and safe, so you don't have to worry about maintaining compliance. Here are 14 endpoint management features that can help your organization achieve and sustain GDPR compliance.

Protect data across computers

It has an array of desktop management features that make GDPR compliance simple

1. Update Windows, Mac, Linux, and over 250 third-party applications from one central location using UEM Central's patch management capabilities.

2. Manage USB devices in your network by restricting and providing access using our USB security management feature, which will help you restrict data transfers and secure information.

3. Gain complete visibility over applications that's running in your network using our software management capabilities.

ManageEngine
IT Management, Simplified

4. Block unwanted executables, prohibit software in your network, and stay vigilant against remote code executions using UEM Central's web-based inventory management feature.

5. Generate audit report's for the shared files and folders with selected computers using file and folder configuration reports; generate BitLocker encryption reports to monitor data security using our inventory management for BitLocker feature.

6. Manage your users, groups, files, folders, firewalls, registries, and services by limiting access, providing privileges, and redefining firewalls based on your preferences.

7. Make your users reset their passwords immediately following phishing or brute force attacks to avoid data breaches.

8. Deploy custom scripts to a select group of computers to resolve issues as soon as possible.

9. Avoid unexpected downtime using our failover server feature, which always backs up your primary server.

10. Protect against external data breaches by placing a securing server in front of your main server using our forwarding server feature.

Protect data across mobiles

When your employees go mobile, so does your personal data. *Endpoint Central's* mobile device management (MDM) feature can help you secure employees' mobile data even if they're away from your network.

1. Create corporate containers to manage employees' corporate data without disturbing their personal information.

2. Wipe corporate data completely from lost or stolen devices or find devices using the lost mode feature.

3. Blacklist anonymous or unsecured apps installed through APK downloads and restrict data sharing between apps to prevent data leaks and increase user privacy.

4. Permit users and employees to install only whitelisted apps and restrict mobile devices from accessing specific apps.

What should you do now?

We're sure you're busy equipping your organization to comply with the GDPR. But if you haven't thought about how you're going to maintain compliance after May 25, 2018 yet, then you may want to consider a tool to help you.

Uber, Maersk, and Equifax all recently faced data breaches; as their stories show, a breach can heavily damage an organization's productivity, data protection, and reputation.

This is exactly why every organization needs to employ top-level security towards their data and follow best practices to protect their users' privacy. With *Endpoint Central* on your side, all the personal data stored in your computers, servers, and mobile devices will be safe and secured.

Which ManageEngine solution is right for me?

Endpoint Management

If you need to secure the data in your servers, desktops, laptops, smartphones, and tablets, employ our unified endpoint management solution, Desktop Central.

FREE TRIAL

Mobile Device Management

If you're looking to safeguard data in mobile devices, employ our exclusive mobile device management solution, Mobile Device Manager Plus.

FREE TRIAL

Patch Management

If you're worried about breaches that happen through application and OS vulnerabilities, employ our exclusive patch management solution, Patch Manager Plus.

FREE TRIAL

SCCM Third Party Patch Management

If you've already employed Microsoft SCCM and are looking for a solution to help with automatic patch management for third-party applications, try Patch Connect Plus.

FREE TRIAL

If you're not worried about data now but you are looking for a free desktop management tool, then try our free Windows management software, Free Windows Admin Tools. If you want to manage computers even when you're on move, try our free remote system administration Android app, System Tools.

ManageEngine
IT Management, Simplified

Try our endpoint management suite

ManageEngine offers a unified endpoint management solution that helps in managing thousands of servers, desktops, and mobile devices from a central location. It automates the complete desktop and mobile device management life cycle, ranging from a simple system configuration to complex software deployment. Used by more than 6,500 customers around the globe, our endpoint management solution helps businesses cut costs on IT infrastructure, achieve operational efficiency, improve productivity, and combat network vulnerabilities.

Integration with other products

- zendesk
- servicenow
- spiceworks
- ManageEngine ServiceDesk Plus

Also available in

Windows Azure Marketplace | awsmarketplace

ManageEngine
IT Management, Simplified

About ManageEngine

ManageEngine is bringing IT together for IT teams that need to deliver real-time services and support. Worldwide, established and emerging enterprises—including more than 60 percent of the Fortune 500—rely on our real-time IT management tools to ensure tight business-IT alignment and optimal performance of their IT infrastructure, including networks, servers, applications, desktops, and more. ManageEngine is a division of Zoho Corporation with offices worldwide, including the United States, India, Singapore, Japan, and China. For more information, please visit buzz.manageengine.com/; follow the company blog at blogs.manageengine.com/, on Facebook at www.facebook.com/ManageEngine and on Twitter @ManageEngine.

About the author

Giridhara Raam is a product expert and cybersecurity analyst at ManageEngine, a division of Zoho Corp. He works with endpoint management solutions, analyzing Endpoint Central, Mobile Device Manager Plus, Patch Manager Plus and Patch Connect Plus.

He also immerses himself in cybersecurity research from an endpoint management context. His recent e-book on cybersecurity, entitled "Six best practices for escaping ransomware", helped IT pros understand cyber attacks and employ proper security measures in their network. You can listen to his cybersecurity webinar on YouTube.

ManageEngine
IT Management, Simplified


ManageEngine
IT Management, Simplified