BeyondTrust

GENERAL DATA PROTECTION REGULATION (GDPR)

Building a Solid Foundation for GDPR Compliance

The information landscape has changed significantly since the European Union (EU) introduced its Data Protection Directive in 1995 aimed at protecting the privacy of EU citizens. The amount, sources, and types of data that are collected and used by organisations today has exponentially grown, together with the value organisations can gain from this data.

With the growth of the 'always on' culture, driven by the ever-expanding capabilities of mobile devices and the increase in the digital transformation of services, a wide range of identifiable and behavioural data is now collected and processed by organisations every time we interact online. In addition, organisations such as Facebook and Google gather huge amounts of data every day.

At the same time, how and where organisations store and process this data has moved from inside the traditional IT perimeter and server rooms into hybrid and cloud environments in data centres across the globe. How organisations process this data has also changed now that data privacy is threatened. Respondents of BeyondTrust's 2018 Secure Access Threat Report found that 62% of employees send files to personal email accounts, 63% download data onto an external memory stick or drive and 56% have employees that log on to company networks over unsecured WiFi (e.g. from a coffee shop).

This proliferation in how and where data is gathered, processed, and stored, plus its ever-increasing value, led the EU Commission to update its regulations in 2018 to better protect the privacy of its citizens and to standardise data protection laws across the EU.

The EU General Data Protection Regulation (GDPR) has been designed to better protect how personally identifiable information (PII) of EU citizens is collected, processed, and stored.

Who is required to comply with GDPR?

It applies not only to all organisations based in the EU, but also to any company that processes the data of EU citizens. Within an organisation, the GDPR applies to both the data controller and all data processers. In addition, organisations must also understand the physical location of where the data they collect and store reside especially if they utilise SaaS solutions and hybrid and cloud environments.

Backed by significant penalties of up to €20m or 4% of an organisation's global turnover for those who fail to comply, organisations must understand what they need to do to be compliant.

How can you comply with the GDPR?

Organisations need to understand the requirements of the GDPR and how these will impact processes, policies, training, technology and security around the data they gather and process. Compliance and IT teams must be proactive to ensure they will be compliant and should consider the following steps:

1 IDENTIFY WHAT DATA YOU HOLD

Organisations need to obtain a full picture of all relevant data they hold to implement any necessary changes to ensure that they are compliant. However, with the complex hybrid IT environments today and proliferation of data across the organisation (e.g. on personal devices), this task may present a significant challenge. Organisations must be able to answer:

- Where does the data ***reside***? The physical location of all relevant data, whether online or offline – don't forget your filing cabinets! – must be established.
- Who has ***access*** to the data? Organisations must limit the access to personal data to only employees who specifically require it for their job role.
- How is data is ***processed and transmitted***? Within an organisation, data could be traveling in and out of network to third-party vendors, and stored on a variety of servers.

2 REVIEW EMPLOYEE TRAINING

Each employee must now be able to identify if their organisation is in violation of the GDPR and report this to the necessary authority. This could be a data breach from an external attacker for malicious purposes, or an employee that has been granted an improper level of access to personal data.

3 CONSIDER YOUR SUPPLY CHAIN

Who else has access to your data in addition to your employees? This can include cloud providers, marketing agencies, and SaaS CRM, HR, and procurement applications. You must ensure that they have the necessary policies and security measures in place so you are compliant if they store or process your data.

4 CONTROL AND MONITOR ALL ACCESS TO YOUR DATA

Organisations need to ensure that by default personal data is not made accessible to those who do not need it, as well as manage what people who have authorized access can and can't do with the data. Give privileged users just the access they need to enforce "least privilege," and create an audit trail by logging all session activity.

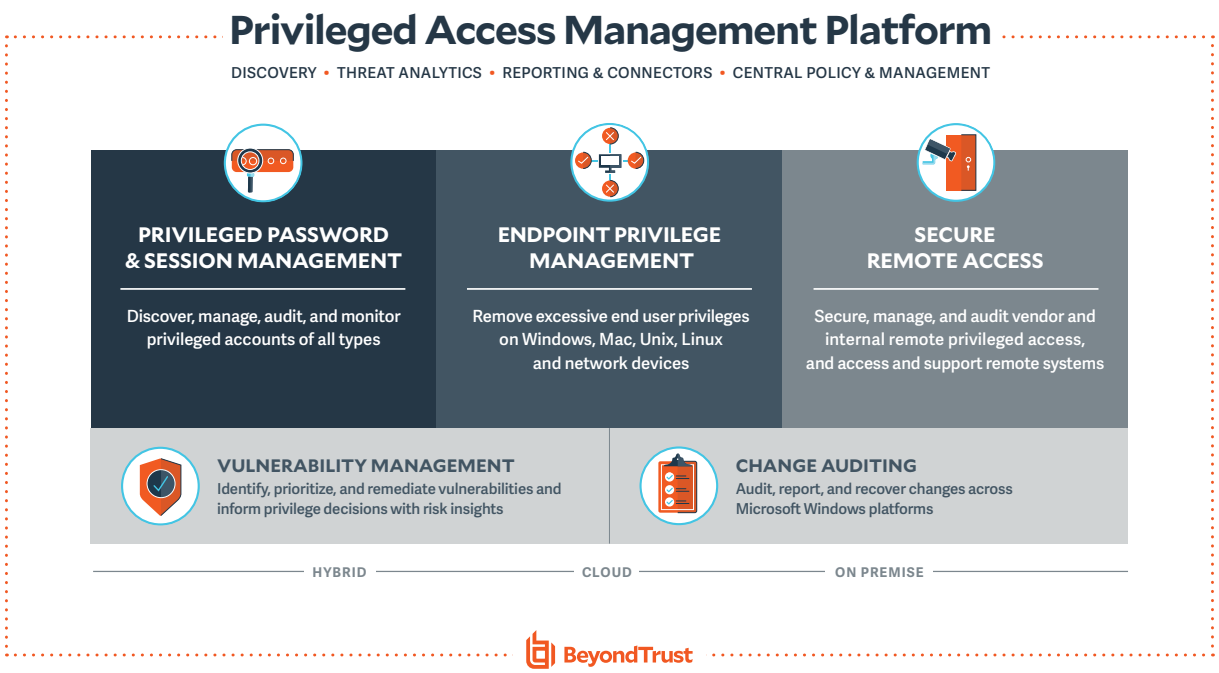
How BeyondTrust can help your organization meet GDPR requirements

BeyondTrust's Privileged Access Management (PAM) solutions enable businesses to control, monitor and manage access to critical systems and data, while ensuring that people remain productive and are not impeded in their day to day job tasks. BeyondTrust solutions allow users to access systems quickly and securely, while defending against threats related to stolen credentials, misused privileges, and unwanted remote access.

- **Enforce policy of least privilege:** Only give access to data to those who need it, when they need it, with granular levels of access controls that eliminate "all or nothing" access
- **Manage privilege 'sprawl':** Identify and secure all your privileged accounts centrally across your organisation including dormant credentials, eliminate insecure practices of employees sharing or writing down passwords, and integrate your security policies
- **Create an audit trail:** Every session and all session activity is fully recorded, creating accountability of which specific people accessed a system and what actions were taken to provide effective attribution
- **Remove all point to point pathways:** BeyondTrust's secure architecture breaks any point to point access paths into your systems with no descending connections, eliminating the need for VPNs
- **Encrypt communication:** BeyondTrust ensures all privileged access session data in transit or at rest are encrypted using TLS 1.2
- **Secure and protect all privileged accounts:** Privileged credentials are stored, rotated, and managed within a secure enterprise password vault, and privileged users are granted access based on their job roles and requirements creating a reliable privilege on-demand workflow
- **Eliminate manual password management and access controls:** Implement secure 'one-click' access to systems for privileged insiders and third parties with automated credential injection
- **Enforce data security policies to meet GDPR compliance:** Integrate your identity providers and security policies with BeyondTrust solutions

BeyondTrust GDPR Solutions

The BeyondTrust Privileged Access Management Platform enables organizations to achieve GDPR compliance by defending against threats related to stolen credentials, misused privileges, and unwanted remote access.



Meeting GDPR Compliance

BeyondTrust can help you meet a variety of GDPR standards and significantly reduce security risks related privileged accounts, users, and access.

ARTICLE SUMMARY	CONTROL OBJECTIVE
ARTICLE 5 – Principles relating to processing of personal data: Organisations must implement appropriate technical and organisational measures that ensure and demonstrate that they comply and includes staff training and creating and improving security features on an ongoing basis.	BeyondTrust PAM solutions enable organizations to securely access remote devices, systems, and users. With features such as secure two factor authentication, granular permissions settings and approval processes, automatic recordings, encryption, and a choice of deployment options, BeyondTrust helps organizations to meet security standards. BeyondTrust offers highly granular control over user access and privileges, and all traffic runs through standard ports. Controllers have the ability to set granular session permissions and configure parameters such as access time constraints and network areas of access. Access can be approved on an ad hoc basis. Sessions automatically terminate after the specified time is up. Controllers have the ability to set up Jump Clients (BeyondTrust proxy) for frequently accessed systems and use existing protocols, including RDP, Vpro, SSH Telnet, SUDO, and others. All access can be automatically recorded for auditing, enabling the organization to demonstrate compliance.

ARTICLE SUMMARY	CONTROL OBJECTIVE
ARTICLE 7 – Conditions for consent: Individuals must provide explicit consent as to the purpose of the data an organisation is collecting from them. They can withdraw this consent at any time.	In a remote support scenario, the controller has the ability to customize information fields required to start a session during set up. A customer agreement prompt guarantees explicit consent before a session starts, and at any time the data subject is able to modify or withdraw their consent.
ARTICLE 15- Right of access by the data subject: The data subject has the right to know whether their personal data is being processed, and where. They can request this from the controller at any time.	Recorded BeyondTrust data can be retrieved as needed. Controllers can populate and retrieve information for a request based on a specific data subject.
ARTICLE 17 – The right to be forgotten: The GDPR significantly increases the right of individuals. They can request access to any data covered by GDPR that an organisation holds on them and have the right to be forgotten so organisations must have processes in place to remove this data.	Anyone using BeyondTrust, whether from the technician or support rep perspective, or as a customer has the right to be forgotten. The controller can search for a specific user using the indexed search field and either remove or anonymize the user. Customizable retention policies allow an organization to choose how long and what data they need to retain in order to meet compliance.
ARTICLE 18- Right to restriction of processing: Individuals have the right to restrict processing of their personal data. The data subject must give consent before any data is processed.	BeyondTrust enables controllers to ensure consent for processing is obtained. A customer agreement prompt guarantees consent before a session starts, and at any time the data subject is able to change their consent. The action of consent or denial is automatically recorded in BeyondTrust.
ARTICLE 20- Right to data portability: Individuals have the right to receive the personal data concerning him or her that a company holds in a structured, commonly used and machine-readable format. They have the right to share that data with another organization.	BeyondTrust enables the controller to provide a report on the session details pertaining to data subject, exported in XML format.

ARTICLE SUMMARY	CONTROL OBJECTIVE
ARTICLE 25 – Data protection by design and by default: This article states that the data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Such measures shall ensure that by default personal data are not made accessible to those who do not need to.	BeyondTrust enables secure two factor authentication via RADIUS, Smart Cards, or natively, which allows users to authenticate using a device of their choice such as their mobile phone or laptop. BeyondTrust can be integrated with identity management solutions such as LDAP(s), Active Directory, or SailPoint to enable granular control over group policies. BeyondTrust offers highly granular control over user access and privileges, and all traffic runs through standard ports. Admins have the ability to set granular session permissions and configure parameters such as access time constraints and areas of access. Access can be approved as necessary. Sessions automatically terminate after the specified time is up. BeyondTrust's data at rest encryption allows organizations to use their existing key management solution to encrypt their BeyondTrust configuration, text-based session audit history, and session recordings, further ensuring that personal data is only being used when necessary.
ARTICLE 32 – Security of processing: Organisations need to implement appropriate technical and organisational measures to ensure the security of data being processed including who can access the data, encryption etc.	Administrators can create vendor and user profiles with specific permissions to actively manage vendors and privileged users. When integrated with an enterprise directory, it is that directory that enforces established procedures for creating, changing, and safeguarding passwords. Reporting on demand enables the controller to generate a report on who has access to the data and systems. All data is encrypted using TLS 1.2. BeyondTrust provides a range of cipher suites that may be appropriately restricted by authorized system administrators. All remote system communications are initiated outbound from the client toward the BeyondTrust instance using TCP/IP port 443 and using the public key certificate resident in the client software running on the remote device. There is no underlying access to the operating system. Data at rest encryption allows organizations to use their existing key management solution to encrypt their BeyondTrust configuration, text-based session audit history, and session recordings, further ensuring that personal data is only being used when necessary. Any security patches and bug-fix software are made available regularly.
ARTICLE 33 – Notification of a personal data breach to the supervisory authority: Organisations must notify the relevant regulatory body within 72 hours of a data breach and describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.	Session activity is automatically recorded and logged and there are built in capabilities allowing users to generate comprehensive reports for analysis. BeyondTrust can also integrate with SIEM tools for advanced analysis of audit logs. Alerts can be set for misuse or suspicious activity. Preventative measures can mitigate breach risk. Sessions can be authorized on an ad hoc basis, and workflows can be configured via integrated change management tools. Access can be restricted on a granular basis. Immediate credential rotation upon session completion ensures a minimal availability of useful credentials.

This framework is generated based on BeyondTrust software released in 2018 or later. Older versions of the software may not meet all of the compliance requirements as stated.

Conclusion

The General Data Protection Regulation (GDPR) is one of the most important movements in the area of data protection in recent years. GDPR is a complex and wide-ranging law that has far reaching consequences. Complying with this regulation will require a significant amount of work for most organisations. Building a solid cyber security foundation - that is both powerful and simple - provides a vital base on which to assemble the processes, procedures and products necessary for full GDPR compliance. The BeyondTrust PAM Platform can be quickly deployed to help your organization achieve GPDR compliance with a fast time to value and lower total cost of ownership.

This document does not constitute a full guide to GDPR compliance, BeyondTrust recommends that you consult with a GDPR legal specialist in order to manage your compliance with the new regulation.

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing privilege-related breaches. Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. We are trusted by 20,000 customers.

beyondtrust.com

V2019_04_ENG