TECH BRIEF

NETWORK SYSTEMS

GENERAL DATA PROTECTION REGULATION

BUILDING A SOLID FOUNDATION FOR GDPR COMPLIANCE

BeyondTrust

Table of Contents

Executive Summary:

The General Data Protection Regulation (GDPR) is one of the most important movements in the area of data protection in recent years. It was passed into European Union (EU) law on 28th April 2016 and will become enforceable on 25th May 2018. In summary, the GDPR defines controls around how organisations store and process the personal data of EU citizens, irrespective of where the organisation is based, owned, or operating. Anyone storing or processing the personal data of an EU citizen must comply with the GDPR or face significant fines in the event of an audit or data breach. Those fines can be up to 4% of the organisations global turnover or €20m, whichever is greater. With this level of impact, it is vital that all organisations understand their obligations under the GDPR and take appropriate measures to ensure they are compliant demonstrating that the proper controls are in place to protect information.

GDPR was designed to simplify the current requirements and not introduce a massive new burden on organizations. In fact, GDPR consolidates the 28 distinct implementations of the previous Data Protection Directive (95/46/EC) into one regulation for consistency, standardized version control, and reporting.

BeyondTrust offers a number of solutions that can help organisations achieve GDPR compliance by developing a strong, yet simple, cybersecurity foundation based on security best practices for Privileged Access Management (PAM). BeyondTrust's PAM solutions address privacy and user obscurity through our unique offerings, including:

- PowerBroker Password Safe (a privileged password management solution) that can help control who has access to operating sys tems, applications, databases, infrastructure and cloud resources, and provide attestation reporting on complete session activity.

- PowerBroker for Unix & Linux (server privilege management solution) which can manage privileged access to commands and appli cations eliminating the need for root access and Sudo.

- PowerBroker for Windows (server and endpoint privilege management solution) which can pseudonymise data collected around user and administrative activity ensuring data cannot be linked to individuals within a single data store.

Definitions

Three key definitions are those for a controller, a processor and what constitutes personal data as these are the primary focus for the GDPR.

Controller – Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor – Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal Data – Any information related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Legal Person – Considered to be any non-human entity which is treated as a person in law, i.e. a company or organisation that is incorporated by law.

In comparison to the definition of Personally Identifiable Information (PII), the definition of personal data includes far more traits. As an example, the definition of an online identifier includes usernames, RFID tag IDs and even IP addresses. This places the burden of identification, protection, and reporting at a much more granular level than just for PII required by other countries and regulatory frameworks.

Pseudonymisation - The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

GDPR Data Privacy Requirements

The GDPR provides guidance relating to the protection of natural persons with regard to the processing of personal data and requirements relating to the free movement of personal data including Personally Identifiable Information (PII).
It protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal information. It also allows for unrestricted movement of personal data within the EU and the requirement that the collection of this data to be deleted or removed upon request of the user protecting their digital identity.

Note: A natural person is a human being defined by GDPR

Regulation Scope

The regulation defines scope in two ways:

- Material Scope - How data is processed
- Territorial Scope - Where data is processed

In material terms, GDPR applies to the processing of personal data wholly or partly by automated (electronically) means and to processing other than by automated means, i.e. as part of a paper or manual filing system. Processing related to the prevention, investigation, detection or prosecution of criminal offences, execution of penalties and safeguarding public security is excluded from the GDPR. This is an important differentiation since law enforcement and their investigations are not participatory entities and may have exclusions when collecting personal data from organizations normally governed by GDPR.

In territorial terms, GDPR applies to the processing of personal data for data subjects who are in the European Union. In particular, when related to the offering of goods and services (irrespective of whether payment is required) and monitoring of their personal behavior. The regulation also applies to the processing of data by a controller wherever Member State law applies through public international law. If unsure, it's safest to assume that GDPR applies.

Responsibility

When your organisation is required to comply with GDPR, there are several key areas to consider:

Consent of the data subject – any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Beyond the pure collection and processing of personal data, the GDPR also lays out specific requirements around the consent of the data subject for both the collection and processing of their data. This consent requires affirmative action by the data subject to show consent to each form of processing the collected data will undergo; consent can no longer be given in a blanket manner, i.e. covering multiple processes. Consent can also be withdrawn at any time by the data subject. For more detailed information see Article 7 of the GDPR.

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The regulation provides a much stronger response to personal data breaches than previous directives and regional legislations. It requires that the controller notify the supervisory authority of any personal data breach not later than 72 hours after having become aware of the breach. If the notification cannot be given within 72 hours, the controller will be required to provide the reasons for the delay. If the controller is able to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of the natural persons whose data has been breached, the need for notification within the timeframe is removed but notification must still be made.

The GDPR also defines clear accountability for the controller over the management of personal data. The controller must ensure that data is processed lawfully, fairly, and in a transparent manner; that data is only collected for specified, explicit, and legitimate purposes and adequate, relevant, and limited to only what's necessary for the consented processing.

The controller is also responsible for ensuring the personal data is accurate and, where necessary, kept up to date. The data should also be kept for no longer than is necessary for the purposes for which the personal data are processed. Finally, the data must be processed in a manner that ensures appropriate security of the personal data, e.g. not allowing it to be subject to a personal data breach.

As a controller, you have responsibility for and must be able to demonstrate compliance with the accountability above. As is clear from this, it's vital that you have control over who has access to personal data, when they accessed the data and what was done with the data. Also, as far as possible, ensuring that there are no opportunities for unauthorised access to the personal data.

How BeyondTrust Can Help

BeyondTrust offers a number of solutions that can help organisations implement a framework of controls to prevent unauthorised access to personal data and monitor legitimate access by specifically authorised individuals.

Focusing on the fundamentals of secure access, BeyondTrust enables organizations to build a solid foundation for a cybersecurity infrastructure. The foundation is based on Privileged Access Management that trusts and verifies all privileged activity, without impacting productivity, to all sensitive personal data managed by a controller.

The technology provides session recordings based on access and reporting of any activity interacting with the data or application for a privileged user. This ensures the controls specific to GDPR can be enforced and that inappropriate access is managed accordingly.

Enterprise Password Management

One of the ways you can control access to personal data is to direct users through a simple, yet comprehensive, privileged access management platform which allows access to explicitly defined users. Whether using shared or individual accounts, BeyondTrust's Enterprise Password Management platform makes it easy to ensure access to personal data is tightly controlled irrespective of who is accessing it, and provides full session monitoring to prove the access was appropriate.

For example, a database administrator who needs to work on a system containing personal information must first request access through the platform. This access may require approval by one or more human approvers (typically management) before being granted. Or, if the workflow does not require approval, the administrator may be autoapproved. This is dependent on how you classify the data being accessed (or potentially accessed). Actual access to the database is brokered through the platform with "four-eyes" functionality and optional session recording. A full audit trail is available consisting of logged events, recorded sessions and captured keystrokes, all accessible (to appropriate individuals) through a secure, searchable interface that can be secured by geolocation (IP based) as well.

By adopting an approach of specifically granted access, it is much easier to demonstrate that you have control over access to personal data and how that data was accessed. Session review and keystroke logging allows you to prove exactly what was done with each access, contributing to the GDPR requirements for auditing of access.

Server Privilege Management

One of the fundamental areas of concern when looking at personal data security is the use of privileged accounts. These include the Administrator account on Windows, root account on Unix and Linux, or additional accounts added with the same or similar privileges. With these accounts, it is difficult to limit what someone has access to within a server or application as their innate privileges are all encompassing. It can be difficult to demonstrate control over access to personal data when using such highly privileged accounts. Tools that attempt to restrict privileged users can falter since a privileged user can often stop or remove those controls with relatively minimal knowledge. It follows the adage that once you are an administrator, there is nothing to stop you; it is essentially game over for a threat actor.

The solution to this problem requires the implementation of a least privilege model. This reverses the paradigm of privileged access. When adopting least privilege, you start all access as a standard user. All applications and commands are issued as that same standard user. This constrains what you can do and what you can access. You have no server administrator rights; no longer do you have free reign across the entire system. This is a fundamental step in being able to demonstrate control over access to personal data. When you use least privilege, only the commands and applications that need administrative rights actually execute with the proper privileges independent of the end user. This prevents the user from disabling the tools used to protect privileged access.

By using the BeyondTrust Server Privilege Management platform, you can grant specific access to targeted resources, users, applications and commands for any user or other application. This access is managed through a fine-grained policy system allowing you to have complete control and clear visibility, through extensive event logging and session recording; all without impacting productivity. BeyondTrust Server Privilege Management includes all of the functionality of the Privileged Access Management platform and least privileged capabilities.

Endpoint Privilege Management

Securing your core systems and server infrastructure is fundamental in managing GDPR compliance. Endpoints are still the most common entry point for a personal data breach using techniques like phishing or browser based vulnerabilities. As such, it's important to ensure that security controls don't stop at the servers but continue onto the user's endpoints. Endpoint Privilege Management brings the same rigor of least privilege control to workstations, desktops (including cloud and virtual), tablets, and laptops within your enterprise. The solution is designed to have minimal to no impact on the end users experience and allows you to securely remove administrative rights from the end user and supporting organizations such a call center or help desk.

The BeyondTrust platform allows you to define simple and clear policy that controls how and when specific applications run with elevated privileges. This patented technology never elevates the end user privileges, just the application privileges, and can prompt for a justification to provide auditing of personal data access. This approach of explicit capabilities, as opposed to the implicit capabilities of direct access to a privileged account, promotes a simpler and more secure model. This security model makes it much easier to demonstrate who has access to which resources, including personal data stores, and what they did with them when access was granted. This is done via extensive logging, session recording, and attestation reporting to demonstrate these controls in action.

Unfortunately, the logging of activities on an endpoint are potentially capturing personal information about the activities of natural persons. This could be a violation of GDPR compliance itself depending on the data aggregation, reporting, and destination of the results. Even as members of staff, they have a right to privacy and protection of that data is important. To help address that, BeyondTrust's endpoint solutions include the capability to pseudonymise data separating the user identity from the collected data. In line with the GDPR requirements for pseudonymisation, the information linking the user identity and the collected data are held in entirely separate data stores preventing simple association but allowing the solution to provide effect privileged management.

This approach allows you to collect data on the use of least privilege elevations wothout impacting your compliance with the GDPR.

Conclusion

The General Data Protection Regulation (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.

BeyondTrust solutions can help you provide visibility around who has access to the systems underlying your personal data storage and processing and what's being done with that access. It also helps you enforce control during those activities by limiting access to only those previously authorised. The inclusion of a powerful behavioral analysis engine in the platforms helps you quickly identify activity that is abnormal, even within the permissions and capabilities explicitly granted to the users. Limiting users to only those actions and activities that are appropriate for their roles reduces the noise in the system allowing your other monitoring and forensic tools to operate with much greater efficiency.

Better control and more comprehensive visibility are vital in the effort to comply with GDPR. When you know that system access is under control, you can focus on the higher-level compliances with confidence.

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 can however help limit the exposure and usage of personal data to streamline you GDPR compliance initiatives.

About BeyondTrust

BeyondTrust® is a global cyber security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust‘s security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100. To learn more about BeyondTrust, please visit www.beyondtrust.com.

IP ADDRESS MANAGEMENT

PRIVILEGE MANAGEMENT

ACTIVE DIRECTORY SECURITY

N3K NETWORK SYSTEMS

Über N3K: Schnellwachsende IP-Netzwerke erfordern professionelle Lösungen für die verschiedensten Facetten des Netzwerk-Managements. N3K Network Systems hat sich auf die Gebiete IP Address Management, Privilege Management sowie auf Active Directory Management spezialisiert. So können mit hoher Kompetenz auf die individuellen Anforderungen der Kunden zugeschnittene Lösungen entwickelt werden. N3K unterstützt die Kunden über den gesamten Projektzyklus hinweg bei Bedarfsanalyse, Konzeption, Projektplanung, Implementierung und Schulung. Hinzu kommen umfangreiche Wartungs-Services inklusive weltweitem 7x24-Support und direkter Einwahl beim Kunden. Aufbauend auf dieser einfachen und effektiven Philosophie hat sich N3K als führender Anbieter in Deutschland etabliert. Mehr als 50% der DAX-Unternehmen sind N3K-Kunden. Durch Standorte in den USA und in Singapur können die Leistungen weltweit erbracht werden.

n3k Informatik GmbH · Ferdinand-Braun-Straße 3 · 74074 Heilbronn · Telefon +49 7131 59495 0 · Telefax +49 7131 59495 100 · www.n3k.de · info@n3k.de