A PRIVILEGED ACCOUNT SECURITY APPROACH TO GDPR READINESS
There is no personal information security – hence very difficult to achieve GDPR compliance – without securing the privileged pathways to the systems containing personal data.

The General Data Protection Regulation (GDPR), which goes into force May 25, 2018, is designed to better protect the personal information of EU citizens and residents. This Advisory is the first in a series of guides that will help you prepare for GDPR and avoid being found in non-compliance.

The series will show you how to take practical steps to aid your organization in meeting GDPR requirements for protecting personal data:

- Protect access
- Respond rapidly
- Assess your risk
- Demonstrate compliance
CHAPTER ONE

PROTECTING THE PATHWAYS TO PERSONAL INFORMATION
A lot of attention is placed on the financial penalties resulting from non-compliance with GDPR. But there are strategic business benefits to stronger protection of personal data beyond the near-term avoidance of fiscal pain.

- Strengthen customer relationships and brand.
- Keep your partnerships strong and running smoothly.
- Achieve a better overall security posture for other valuable corporate data.
- Carry security forward by design and default into new processes and applications.
- Protect your investment in control systems already in place.

A strong Privileged Account Security strategy is critical to securely leverage personal data so you can advance in an increasingly dynamic, competitive business environment.

“Firms not only passively consume data from online platforms. They are also actively expanding their user databases and analysing qualitatively the trends on the demand side. This can lead them to increase their market shares by designing new products and services that better suit consumer preferences.”

Source: LSE Business Review - The economic value of personal data for online platforms, firms and consumers, January 19th, 2016
WHAT DOES GDPR REQUIRE IN PROTECTING ACCESS?

Fundamental to meeting GDPR Article 25 is controlling who, or what, have privileged access to your personal data. As stated in the Article, part of meeting Article 25 is putting in place “Technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.”

Integrating a Privileged Account Security solution that enforces least privilege access helps to demonstrate that you are addressing Article 25’s requirement to protect personal data by design and default.

Least privilege limits user access to the minimal level of data that allows normal business functions and significantly strengthens your operational control over access to personal data.

Least Privilege Checkpoints:

☑ Do you manage accounts by the “least privilege principle,” e.g., use admin accounts for administrative tasks only? Delegate only those permissions needed for a user to do his/her job?

☑ Do you restrict application accounts to “least privilege”, e.g. not allow applications to have domain administrator privileges?

GDPR Article 25 requires protection of personal data by design and by default.

Privilege and Accountability

Privileged “users” include employees and third-parties – even certain applications or processes – that have access to personal data. You are now responsible for all of these under GDPR.
WHY WON’T MY SOLUTIONS PROTECT ACCESS TO PERSONAL DATA?

Today’s advanced attacks frequently breach existing perimeter defenses – and malicious insiders continue to compromise personal data. Here’s where the design of real privileged access protection comes into play.

Proactive data protection strategies must move inside the organization, assuming the attacker is already there, protecting from the inside out. The key is to tightly control your pathways to privileged access so unauthorized users are blocked on the spot, whether they are malicious or mistaken.

GDPR Article 32(2) says you must protect against the accidental or unlawful destruction, loss, alteration or access to personal data.
Cybercriminals infiltrated some 1.4 billion data records last year—a whopping 86% increase over the previous year.

Proactive Protection Checkpoints:

- Do you currently use a password vault which automatically enforces strong password policies?
- Enforce multi-factor authentication for users to access credentials in the vault?
- Automatically select and rotate unique passwords for all admin accounts?

Putting every credential in a secure digital vault and enforcing individual accountability for each action taken using that credential at any particular time is a proactive step toward helping organizations comply with Article 32(2).
A COMPREHENSIVE PRIVILEGED ACCOUNT SECURITY STRATEGY IS KEY TO COMPLIANCE

Privileged accounts are everywhere – in every piece of hardware and software. They exist across the entire IT stack including in databases, applications, endpoints and the network.

Strong Privileged Account Security requires more than management of individual users’ passwords. You need to comprehensively isolate, control, and monitor privileged access across systems, databases, and VMs as well.

System Access Checkpoints:

Do you:

☑ Currently segregate accounts used to manage domain controllers, servers and workstations?
☑ Remove plain-text application credentials, such as embedded passwords and locally stored SSH keys
☑ Force all privileged sessions through a secure jump server?
☑ Isolate administrative access to personal data from Internet-connected workstations?

When you secure privileged accounts on both user and system access levels, you remove the ability of external attackers and malicious insiders leveraging compromised credentials to bypass your monitoring solutions and security controls.

Seventy-seven percent (77%) of the time, attackers used a combination of hacking, malware, and social engineering to steal credentials and then used those stolen credentials to advance their attacks.

Source: 2016 Verizon Data Breach Investigations Report (DBIR)
PREVENTING A WORST-CASE SCENARIO

The attacker (or malicious insider) has penetrated the perimeter, and starting with weakly protected credentials, elevated their privileged status and stolen a hash for an admin password to access a domain controller. The attacker executes a golden ticket attack, compromising the Kerberos protocol to steal the secret key used to encrypt Kerberos tickets. The attacker can now stealthily access anything they want – effectively owning the corporate network, including all personal data assets and the security systems joined to that domain.

Taking these proactive steps can help you prevent this scenario:

• Identify and discover all your privileged accounts within your environment
• Automatically select and rotate unique passwords for all admin accounts.
• Use a password vault which automatically enforces strong password policies.
• Enforce multi-factor authentication for users to access credentials in the vault.
• Manage accounts by the “least privilege principle.” Use admin accounts for administrative tasks only. Delegate only those permissions needed for a user to do his/her job.
• Restrict application accounts to “least privilege”, e.g. not allow applications to have domain administrator privileges.

Rapid Risk Reduction: A 30-Day Sprint to Protect Privileged Credentials

This report outlines a proven framework for an intensive sprint of approximately 30 days, to implement a set of key controls around privileged credentials. The recommendations, developed in collaboration with a panel of experienced Global 1000 CISOs, enable security teams to proactively protect their organizations
DETECTING AND RESPONDING RAPIDLY TO PERSONAL DATA BREACHES
RAPID DETECTION AND RESPONSE HAS BENEFITS BEYOND GDPR

The potential for being fined up to 4% of global turnover is sobering. But putting in place strong Privileged Account Security measures for early breach detection and rapid response does more than help you avoid fiscal pain.

A proactive Privileged Account Security posture brings strategic business benefits:

- Helps you demonstrate your commitment to customer privacy, building trust that helps attract and retain customers;
- Allows you to rapidly mitigate cyberattacks leveraging privileged access, limiting potential damage;
- Prepares you to meet other notification and compliance regulations more easily and consistently.

To rapidly and accurately report what happened in a breach—or, better yet, detect a threat before a breach occurs—you need robust operational controls. A strong Privileged Account Security strategy is critical to such control.

GDPR article 33 stipulates notification to a supervisory authority (SA) by a controller within 72 hours of discovery of a personal data breach be made.

68% of respondents cite losing customer data as one of their biggest concerns following a cyber attack.

Source: Global Advanced Threat Landscape Survey 2016, CyberArk
HOW QUICKLY CAN YOU DETECT A THREAT TO ACCESS?

Blocking unauthorized access to personal data helps you prevent reportable data breaches in the first place.

As much as possible, automatic detection and blocking access should be a proactive function built into your Privileged Account Security solution. This type of early detection is different than perimeter defenses, monitoring, and security controls which are focused on protecting your systems from attacks from the outside.

A strong Privileged Account Security strategy focuses on proactively detecting threats to personal data from the inside out. Real-time profiling and analyzing individual privileged session behavior within the network can help an organization detect breaches early, with prioritized alerts when abnormal activity is detected.
More than one third (36%) of respondents believe a cyber attack is currently on their network, or has breached their organization’s network in the past 12 months.

Proactive Detection Checkpoints:

- How early in the attack lifecycle can you detect the misuse of credentials leading to a breach of personal data?
- How do you currently detect credential theft—for example, by monitoring administrative activities associated with a password vault?
- Are you able to terminate in progress sessions to prevent high-risk activity that may result in a breach?

Implementing real-time privileged session monitoring not only helps organizations detect credential-use anomalies as they occur, it also helps give you the information you need to meet notification and reporting compliance requirements.

Source: Global Advanced Threat Landscape Survey 2016, CyberArk
WHAT DOES GDPR REQUIRE IF A BREACH DOES OCCUR?

GDPR Article 33 generally requires notification to a supervisory authority (SA) by a controller within 72 hours of discovering a breach. Beyond notification you must also describe and document:

- The nature of the personal data breach, the categories and approximate number of data subjects impacted
- Likely consequences
- Measures taken or proposed to be taken by the controller to address the personal data breach

Despite the proliferation of privileged accounts across the enterprise, and the often unrestricted, anonymous access to these accounts, you should still produce accurate, reliable reports that prove who is accessing accounts, when they are requiring privileged access and what actions they are performing with these critical accounts.
Privileged Access Accounting Checkpoints:

- Do you currently perform live monitoring and recording of user activity during privileged sessions?
- Do you currently isolate privileged sessions, especially those originating from outside the network and from unmanaged devices, e.g. third parties?

A Privileged Account Security solution should enforce privileged credential use controls such as user activity monitoring, session recording and ensuring individual accountably with privileged access to help an organization meet GDPR notification and reporting requirements.

Source: Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, June 2017

72 hours
The GDPR generally requires breached controllers to notify regulators within 72 hours of discovering a breach, and affected consumers “without” undue delay.

50%
Half of our survey respondents said they experienced a global breach that required notification of victims.

10%
Only 10 percent were able to do so within the GDPR’s 72-hour window;

38%
38 percent reported notification took two to five months to complete.
PREVENTING A WORST-CASE SCENARIO

Using a pass-the-hash technique, an attacker extracts password hashes which are stored in local computer memory for all users – including administrators. Using stolen password hashes, the attacker can move laterally to other workstations eventually landing on, a sensitive workstation where they steal confidential personal data.

As is often the case, because there is no mechanism in place to detect anomalies in administrative user behavior, such as unusual lateral movement or access to personal data, nor to monitor real-time privileged sessions, the breach occurs and the information needed to report the breach is unavailable within the 72 hour timeframe GDPR requires.

Taking these proactive steps can help you prevent this scenario:

- Detect the misuse of credentials early in the attack lifecycle to prevent a breach of personal data.
- Detect credential theft—for example, by monitoring administrative activities.
- Perform live monitoring and recording of user activity during privileged sessions.
- Isolate privileged sessions, especially those originating from outside the network and from unmanaged devices, e.g. third parties.
- Identify all locations of malware that may have been used to facilitate the breach.

Rapid Risk Reduction: A 30-Day Sprint to Protect Privileged Credentials

This report outlines a proven framework for an intensive sprint of approximately 30 days, to implement a set of key controls around privileged credentials. The recommendations, developed in collaboration with a panel of experienced Global 1000 CISOs, enable security teams to start proactively protect their organizations.
GDPR Article 32 requires “regularly testing, assessing and evaluating the effectiveness” of your personal data security. Article 35 further specifies that prior to implementing any new technologies processing personal data you must carry out a “data protection impact assessment”.

Securely managing privileged access pathways is a critical component of assessing your risks to personal data. And for the first time, the requirements in GDPR Articles 32 and 35 extend these requirements to third party processors of personal data, e.g. your supply chain, business partners, service providers.

"... a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

Source: GDPR Article 32
Knowing and managing better your privileged access risks sets you up for business benefits beyond compliance:

- Compliance done right (i.e., by design) may carry forward into new processes and applications—assessments are likely to become easier moving forward.
- Helps assure existing and potential 3rd party partners that they will enjoy continuous, secure information sharing.
- Minimizes gaps in personal data protection as you pursue the digital transformation of your business in an increasingly dynamic, competitive business environment.
- Helps you remove vulnerabilities in privileged access to other valuable information assets, e.g. IP, trade secrets, financials.

Assessing and regularly testing your Privileged Account Security strategy is essential to compliance, protecting personal data—and the health of your business.
A privileged user is any person—or application—that has the capability to change, alter or impact the operational service of a business process. This includes not only system administrators, but also certain business users, social networking managers, and increasingly third party individuals and applications. Typically, the number of privileged accounts in an organization is actually three times the number of employees.

Securing personal data requires a map of privileged access pathways—one that can be updated regularly to reflect your dynamic business environment.

**Secure Access Checkpoints:**

- Do you currently exercise regular discovery processes to identify privileged accounts and credentials, including passwords and SSH keys?
- Can you map trust relationships between accounts and systems that have access to personal data?
- Do you regularly limit the proliferation of administrative accounts by minimizing the use of personal privileged accounts?

If you don’t have a firm handle on who has access to what, you end up with weak links in security that extend well beyond the protection of personal data! Without comprehensive, up-to-date visibility into privileged accounts, network, security teams and assigned Data Protection Officers (DPO) cannot effectively assess the risk to your business.

---

Seventy-seven percent (77%) of the time, attackers used a combination of hacking, malware, and social engineering to steal credentials and then used those stolen credentials to advance their attacks.

Source: 2016 Verizon Data Breach Investigations Report (DBIR)
A MUCH MORE COMPLEX PERSONAL DATA ECOSYSTEM

Companies today rely upon a dynamic eco-system of business partners, vendors, contractors, consultants and service providers. GDPR identifies such third parties handling personal data as “processors”, and requires them to implement “appropriate technical and organizational measures to ensure a level of security appropriate to the risk” – just like those collecting personal data.

Yet it can be a real challenge assessing risk to personal data across a broader network that has many more and widely distributed points of privileged access.

Third Party Access Checkpoints:

✓ Do your access discovery processes include third party privileged accounts and credentials, including applications?
✓ Can you map trust relationships between accounts and third party systems that have access to personal data?
✓ What measures do you have in place to ensure visibility into, and control of, 3rd party access to personal data?

Successful business collaboration across this expanded network requires access to information, including personal data (both of customers and employees). GDPR compliance may require greater visibility into and accountability for partners’ (processors’) privileged access strategies.

Nearly half (49%) of organizations allow third-party vendors (supply chain, IT management firms, etc.) remote access to their internal networks.
Security operations teams know they must regularly test their ability to identify, contain and eradicate threats. Given the significance of misappropriated credentials in advanced attacks, testing your Privileged Account Security strategy can mean the difference between normal operations and becoming headline news.

Regular testing across your extended network is even more important when it comes to measuring your privileged access visibility and management. Using red team tactics to try and compromise (safely) your systems is one of the best ways to benchmark and improve on the vulnerability of your Privileged Account Security strategy.

Security Testing Checkpoints:

Do you:

☑️ Regularly conduct “ethical hacking” attacks to determine areas of privileged access vulnerability?
☑️ Have in place processes for securely adding new users and assets to the system and de-provisioning obsolete ones?
☑️ Look for signs of suspicious lateral movement or privilege escalation in real time?
☑️ Leverage behavioral analytics to detect suspicious user and account activity that could indicate a compromised privileged account?

Red teaming, on a regular basis and from the outside, provides fresh insights into the strengths and weaknesses of your privileged access pathways, and overall security. Results provide a baseline from which future security improvements can be measured during the implementation of new technology.

Source: https://techbeacon.com/6-reasons-hire-red-team-harden-your-app-sec
An enterprise connects with a wide variety of third parties to do business: suppliers, data processors, and multiple cloud services. In reality, the enterprise has very little visibility on how privileged access is managed across its business network.

For example: A data processing partner is compromised by a phishing attack. The attacker escalates privileges within the partner network to steal admin password hash and ultimately gain remote access to personal data in the enterprise’s customer database.

Taking these proactive steps can help you prevent this scenario:

• Map trust relationships between accounts and systems that have access to personal data—including third party partners.
• Conduct red team testing that includes third party privileged access pathways to determine areas of risk before being compromised.
• Exercise regular discovery processes to identify and inventory privileged accounts and credentials, including passwords and SSH keys.
• Leverage behavioral analytics to detect suspicious user and account activity that could indicate a compromised privileged account.
DEMONSTRATING GDPR COMPLIANCE TO HELP PROTECT AGAINST LIABILITY
DEMONSTRATING COMPLIANCE HELPS THE BUSINESS

GDPR Article 82 establishes unprecedented liability for data breaches, down to an individual’s right to compensation and liability from damage due to non-compliance and compromised personal data.

The ability to demonstrate GDPR compliance is critical to help limit financial exposure. But as with strong personal data protection and the ability to respond rapidly to a breach, effectively demonstrating compliance can lend itself to strategic business benefits as well. For example:

• Demonstrating responsible custodianship of your customers’ data – perhaps in response to an event – helps you recover and protect your revenue stream. Responsibility enhances customer trust and loyalty, strengthening retention, attracting new customers, and increasing their lifetime value;
• Demonstrating compliance can protect and enhance your brand, attracting new employees, better partners, and more business.
• GDPR applies to both controllers and those who process personal data. The ability to demonstrate strong personal data security between you and your partners can strengthen the way you work together.

Having an effective Privileged Account Security strategy is a powerful way to demonstrate you have operational controls in place to protect personal data.

GDPR article 82: Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
OPERATIONAL CONTROLS HELP DEMONSTRATE COMPLIANCE

GDPR Article 25 calls for personal data protection by design and default. A Privileged Account Security strategy that enforces least privilege access, both for controllers and processors of personal data, help show you are putting in place one of the key “measures which meet in particular the principles of data protection by design and data protection by default.”

An effective Privileged Account Security strategy should also enforce strong controls around session recording and ensuring individual accountable with privileged access. Such strong operational control is important in demonstrating compliance and helping protect you from both the financial and reputational risks of non-compliance with GDPR.
Operational Control Checkpoints:

- Does your security strategy include access controls to ensure that only the right users are able to access – or request access to – authorized credentials?
- Do you monitor access to privileged accounts and require users to “check-out” shared account credentials to establish individual accountability?
- Do you automatically and regularly scan the network to identify accounts needing better protection, and show the reduction in vulnerable accounts?
- Can you assess environmental risks and distinguish between normal and abnormal behavior?
- Have you defined high-risk activity so you can alert the necessary incident response teams?

21,000 accounts

A UK company was fined £100k for exposing personal sensitive info from 21,000 accounts handled by a third party. A probe by this company found an issue with their own portal through which customer information could be accessed.

Source: http://www.theregister.co.uk/2017/08/10/talktalk_fined_100k_for_exposing_personal_sensitive_info/
In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility.


SHOWING COMPLIANCE IN SPECIFIC CASES

Documenting measures taken to protect personal data becomes key to reducing the risk of penalties of liability – financial or otherwise. Having a strong Privileged Account Security strategy includes the ability to quickly locate and document specific personal data incidents:

- Who is accessing privileged accounts;
- When individuals are requiring privileged access;
- Actions they are performing with these critical accounts.

Searchable privileged access audit trail and session recordings – even administrators tampering with an audit trail on a target system – enable your team to report on who has accessed which files, and whether certain files were viewed or downloaded. A tamper-resistant audit trail and easy reporting enables you to pull the precise data needed to demonstrate you have taken responsible, defensible steps to protect personal data.

Documentation Checkpoints:

Can you:

- ✔ Currently provide audit logs of who and what (e.g. applications) accessed personal data, including third party access to personal data?
- ✔ Quickly and easily generate reports that verify you have privileged account controls in place?
- ✔ Provide tamper-proof audit logs and session recordings to demonstrate audit integrity?
- ✔ Do you regularly conduct impact assessments to measure the effectiveness of security controls you have in place?
PREVENTING A WORST-CASE SCENARIO

A company partnered with a third party service provider and allotted them a number of privileged accounts so they could access customers’ personal data through a portal. Employees at the service provider (the “processor” under GDPR) exploited these privileged accounts via a vulnerability in the company’s portal to misappropriate data.

Even though these were the employees of a third party, the company was fined by its Supervisory Authority because they could not document and prove they had appropriate technical or organizational measures in place to detect the misuse of privileged accounts. This opened the door to litigation from thousands of customers whose personal data had been breached.

“With so many third-parties granted access to an organization’s systems, perhaps it’s no surprise that more than two thirds (67 percent) have already experienced a data breach [that]...

...was definitely (35 percent) or ‘possibly’ (34 percent) linked to a third-party vendor.”

Source: https://www.helpnetsecurity.com/2017/05/10/remote-access-technology/
Taking these proactive steps can help you prevent this scenario:

- Monitor access to privileged accounts and require users to “check-out” shared account credentials to establish individual accountability.
- Assess environmental risks and distinguish between normal and abnormal behavior.
- Regularly conduct impact assessments to measure the effectiveness of security controls you have in place.
- Generate audit logs of who and what (e.g. applications) accessed personal data, including third party access to personal data.
- Provide tamper-resistant audit logs and session recordings to demonstrate audit integrity.

“External suppliers continue to be an integral part of how most organizations do business. On average, 181 vendors are granted access a company’s network in any single week, more than double the number from 2016.

In fact, 81 percent of companies have seen an increase in third-party vendors in the last two years, compared to 75 percent the previous year.”

Source: https://www.helpnetsecurity.com/2017/05/10/remote-access-technology/
LEARN MORE

To learn more about demonstrating compliance and help protecting your organization from liability, contact your sales representative or visit us at [www.cyberark.com/GDPR](http://www.cyberark.com/GDPR) and see how CyberArk can help your organization with GDPR readiness.