CYBERARK

Get Your Enterprise Ready for GDPR

A Privileged Account Security Checklist for Securing Personal Data

"GARTNER PREDICTS THAT BY THE END OF 2018, MORE THAN **50%** OF COMPANIES AFFECTED BY THE GDPR WILL NOT BE IN FULL COMPLIANCE WITH ITS REQUIREMENTS.[1]

The General Data Protection Regulation (GDPR) includes four fundamentals related to Privileged Account Management for securing and protecting personal data:

1. **Protecting access**
2. **Responding rapidly to a breach**
3. **Assessing risk to personal data**
4. **Demonstrating compliance**

Operational control over who has access to personal data is at the heart of complying with the GDPR, and this requires a strong Privileged Account Management strategy.

This practical checklist will help you evaluate not only your ability to avoid financial penalties and liability associated with GDPR, but implement a stronger enterprise security posture moving forward better protecting all your valuable corporate data, your customer relationships, and your brand and business partnerships.

In protecting access to personal data, do you:	**Need to do better**	**We're good**
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?	☐	☐
Segregate accounts used to manage domain controllers, servers and workstations?	☐	☐
Remove plain-text application credentials, such as embedded passwords and locally stored SSH keys?	☐	☐
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?	☐	☐
Force all privileged sessions through a secure jump server?	☐	☐
Isolate administrative access to personal data from Internet-connected workstations?	☐	☐
Restrict application accounts to "least privilege", e.g. not allow applications to have domain administrator privileges?	☐	☐

Prior to and in responding to a breach, can you:	**Need to do better**	**We're good**
Detect the misuse of credentials leading to a breach of personal data early in the attack lifecycle?	☐	☐
Perform live monitoring and recording of user activity during privileged sessions?	☐	☐
Detect credential theft—for example, by monitoring administrative activities associated with a password vault?	☐	☐
Isolate privileged sessions, especially those originating from outside the network and from unmanaged devices, e.g. third parties?	☐	☐
Account for who accessed what personal data on which systems when, including third party accounts who process personal data for you?	☐	☐
Identify all locations of malware that may have been used to facilitate the breach?	☐	☐

1 Gartner Press Release, "Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation", May 3, 2017. http://www.gartner.com/newsroom/id/3701117

In assessing risk to your personal data, do you regularly:	Need to do better	We're good
Exercise regular discovery processes to identify privileged accounts and credentials, including passwords and SSH keys?	☐	☐
Map trust relationships between accounts and systems that have access to personal data?	☐	☐
Limit the proliferation of administrative accounts by minimizing the use of personal privileged accounts?	☐	☐
Conduct "ethical hacking" attacks to determine areas of privileged access vulnerability?	☐	☐
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?	☐	☐
Evaluate the processes for securely adding new users and assets to the system and de-provisioning obsolete ones?	☐	☐

To demonstrate GDPR compliance, can you:	Need to do better	We're good
Provide audit logs of who and what (e.g. applications) accessed personal data, including third party access to personal data?	☐	☐
Enforce access controls to ensure that only the right users are able to access – or request access to – authorized credentials?	☐	☐
Monitor access to privileged accounts and require users to "check-out" shared account credentials to establish individual accountability?	☐	☐
Quickly and easily generate reports that verify you have privileged account controls in place?	☐	☐
Automatically and regularly scan the network to identify accounts needing better protection, and show the reduction in vulnerable accounts.	☐	☐
Provide tamper-proof audit logs and session recordings to demonstrate audit integrity?	☐	☐
Assess environmental risks and distinguish between normal and abnormal behavior?	☐	☐
Define high-risk activity and alert the necessary incident response teams?	☐	☐
Conduct impact assessments to measure the effectiveness of security controls you have in place?	☐	☐

CyberArk Privileged Account Security provides end-to-end proactive protection, continuous monitoring and threat detection for privileged accounts that have access to the systems containing personal data, whether by the controllers who collect it or their partners who process it. The CyberArk solution is proven to scale in complex environments, and can easily encompass new users, applications and systems using a distributed architecture inside the network. Taking a proactive approach to privileged access and GDPR compliance limits your risks of fines and liability, as well as provides strategic business benefits from a stronger security posture.

To learn how to address improvements in areas identified in the checklist, contact your sales representative or visit us at **www.cyberark.com/GDPR** and see how CyberArk can help your organization.