Datenschutz: Rechtliche Grundlagen und Datenschutzkonzept für das PVS

Version: 24.07.2020 Bearbeiter: Klopfer

Rechtliche Grundlagen

Das Europäische Parlament hat am 14. April 2016 einen neuen Datenschutz-Rechtsrahmen verabschiedet:

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

Der sächsische Datenschutzbeauftragte informiert auf https://www.saechsdsb.de/umsetzung:

Gemäß Art. 46 Nr. 2 a) aa) des Gesetzes zur Anpassung landesrechtlicher Vorschriften an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG gilt das Sächsische Datenschutzgesetz weiterhin für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen des Freistaates Sachsen, Gemeinden und Landkreise sowie sonstige der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts, soweit diese innerhalb des Anwendungsbereichs nach Artikel 2 Absatz 1 und 2 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung** sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016,S. 89) tätig werden, (öffentliche Stellen).

Der sächsische Datenschutzbeauftragte stellt unter https://www.saechsdsb.de/saechsdsg-alt/formulare folgende für das PVS relevante Formulare bereit:

- Mitteilung und Beschreibung der Verfahren nach § 10 SächsDSG
- Mitteilung zur Vorabkontrolle gemäß § 10 Abs. 4 SächsDSG

Datenschutzkonzept zum Personalverwaltungssystem (PVS)

Gegenstand

Bei der Personalverwaltung werden Datenbestände erfasst und verwaltet, die besndere Anforderungen an zu realisierende Schutzmechanismen stellen. Für eine IT-Anwendung kommt es darauf an, eine hinreichende benutzerspezifische Differenzierung der Zugriffsberechtigungen zu ermöglichen und alle Zugriffe vollständig zu protokollieren.
Gegenstand des vorliegenden Konzeptes ist es daher, die Einhaltung des Datenschutzes beim Arbeiten mit PVS umfassend zu gewährleisten.

Zielstellung

Bei den Sicherheitsüberlegungen ist § 9 Abs. 2 des SächsDSG zu Grunde gelegt worden. Daraus ergeben sich die Ziele des vorliegenden Konzeptes. Es sind daher Maßnahmen zu treffen, die geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren (Zugangskontrolle),
2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, dass das PVS mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden kann (Benutzerkontrolle),
5. zu gewährleisten, dass die zur Benutzung des PVS Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, dass nachträglich geprüft und festgestellt werden kann, welche Daten zu welcher Zeit von welcher Person eingegeben worden sind (Eingabekontrolle),
7. die innere Organisation derart zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle) und
8. eine hinreichende Datensicherung zu gewährleisten.

Realisierung der Ziele

1. Zugangskontrolle

Das PVS besteht aus mehreren technischen Systemkomponenten:

1. einer Menge von Programmdateien (Frontend), die ausschließlich auf einem Dateiserver des Netzwerkes (LAN) zur Verfügung stehen,
2. einer anwendungsunabhängigen Datenbank-Maschine (Backend) auf einem Datenbankserver im LAN und
3. einer anwendungsspezifischen Datenbank, die von der Datenbank-Maschine verwaltet wird.

Der Zugriff auf das PVS setzt genau definierte Berechtigungen für alle Komponenten dieses Systems voraus.

LAN-Administrator
Der LAN-Administrator ist für die anwendungsunabhängigen administrativen Aufgaben im LAN verantwortlich. Er richtet die LAN-Benutzer mit den erforderlichen Zugriffsberechtigungen ein. Ferner wird eine Benutzergruppe mit den erforderlichen Zugriffsberechtigungen festgelegt. Dadurch wird nur den Mitgliedern dieser Gruppe der Zugriff auf die Programmdateien des PVS und auf die anwendungsunabhängige Datenbank ermöglicht.

LAN-Benutzer
Jeder LAN- Benutzer erhält einen Benutzernamen und ein Passwort.
Für das Passwort gilt Folgendes:
- es gilt jeweils nur eine bestimmte Zeitdauer (? Tage),
- nur der Benutzer selbst kann sein Passwort ändern,
- ein Passwort muss aus mindestens ? Zeichen bestehen,
- ein neues Passwort darf nicht identisch mit einem der letzten ? Vorgänger sein und
- nach maximal ? Anmeldeversuchen wird der Benutzername gesperrt.

PVS-Datenbankadministrator
Der PVS-Datenbankadministrator ist für die administrativen Aufgaben am Datenbankserver und an der PVS-Datenbank verantwortlich.

PVS-Fachadministratoren
Die PVS-Fachadministratoren sind für die jeweiligen anwendungsabhängigen administrativen Aufgaben im PVS verantwortlich. Sie richten die PVS-Benutzer mit den erforderlichen Zugriffsberechtigungen ein; hierzu stehen ihnen innerhalb des PVS entsprechende Funktionen zur Verfügung. Damit wird der differenzierte Zugriff auf die Inhalte der PVS-Datenbank ermöglicht. Darüber hinaus sind die PVS-Administratoren für die Konfiguration der Anwendungsfunktionen verantwortlich.

PVS-Benutzer
Jeder PVS-Benutzer erhält einen Benutzernamen und wird beim Programmstart gezwungen, sich ein Passwort zuzuweisen. Das PVS besitzt eine eigene Benutzerkennung, welche unabhängig von der LAN-Benutzerkennung ist, auch ist eine strikte Trennung der Passwortverwaltung zwischen LAN und der PVS-Anwendung gegeben.
Für das Passwort gilt Folgendes:
- nur der PVS-Benutzer selbst kann sein Passwort ändern,
- ein Passwort muss aus mindestens ? alphanumerisch gemischten Zeichen bestehen,
- ein neues Passwort darf nicht identisch mit einem der letzten ? Vorgänger sein und
- nach maximal ? Anmeldeversuchen wird der Benutzername gesperrt.

Auf jeder Arbeitsstation und somit auch auf denen mit PVS-Zugang, ist ein Bildschirmschoner mit Passwortschutz installiert, der auch bei kurzfristiger Abwesenheit des Benutzers unbefugten Zugang verhindert. Ferner besteht die Möglichkeit, die Arbeitsstation bei Verlassen des Arbeitsplatzes zu sperren.

Datenschutzbeauftragter PVS
Der Datenschutzbeauftragte PVS erhält mit Hilfe einer speziellen Programmfunktion des PVS Zugang zum Logbuch (siehe unten). Diese Rolle bleibt einer Person vorbehalten und ist nicht mit anderen Rollen verknüpft.

2. Datenträgerkontrolle

Der LAN-Administrator garantiert, dass nur der Datenbankadministrator, die PVS-Administratoren und die PVS-Benutzer auf die Datenträger des PVS zugreifen können.

Die Zugriffsmöglichkeiten sind soweit eingeschränkt, dass kein PVS-Benutzer die Programmfunktionen des PVS verändern kann. Auf den Festplatten der Arbeitsstationen sind keine PVS-Komponenten gespeichert. Alle PVS-Komponenten befinden sich auf dem vom LAN-Administrator verwalteten File-Server sowie auf dem vom PVS-Datenbankadministrator verwalteten Datenbank-Server.

3. Speicherkontrolle

Nur entsprechend autorisierte PVS-Benutzer sind in der Lage, Daten in die PVS-Datenbank einzugeben, einzusehen oder zu löschen. Alle Zugriffe der PVS-Anwendungen auf PVS-Daten (Abfragen, Änderungen, Löschungen) werden im PVS-Logbuch protokolliert. Neben den PVS-Benutzern hat der PVS-

Datenbankadministrator grundsätzlich Zugriff auf die PVS-Daten. Er ist mit den datenschutzrechtlichen Bestimmungen vertraut und wendet sie an.

4. Benutzerkontrolle

Ein Zugang zum PVS über Einrichtungen der Daten-Fernübertragung ist nicht möglich, da die Server des PVS keine entsprechenden Dienste anbieten. Alle Anmeldungen an das PVS, auch erfolglose, werden im Logbuch protokolliert. Die maximale Anzahl der Anmeldeversuche ist beschränkt (siehe oben).

5. Zugriffskontrolle

Durch die Eingabe des PVS-Benutzernamens und Passwortes identifiziert sich der PVS-Benutzer. Das Passwort kann ausschließlich vom Benutzer selbst geändert werden (siehe oben).

Es existieren verschiedene Benutzergruppen, welche die Arbeitsteilung und Zuständigkeiten im Anwendungsbereich widerspiegeln. In Abhängigkeit von der Gruppenzugehörigkeit des Benutzers werden Zugriffsrechte auf die benötigten Ressourcen eingeräumt.

Durch die Einordnung eines PVS-Benutzers in eine Benutzergruppe können die Zugriffsmöglichkeiten auf ausgewählte Funktionen und Anwendungen beschränkt werden.
Im Anhang befindet sich eine Übersicht der Benutzerrollen und zugeordneten Ressourcen.

> Hinweis: Diese Auflistung kann innerhalb der PVS-Anwendung mit dem Menübefehl *Berichte* | *Rollen und Ressourcen* erstellt werden.

Die PVS-Fachadministratoren verwalten die Zugriffsrechte der PVS-Benutzer. Änderungen von Zugriffsrechten werden wie alle Datenänderungen im PVS-Logbuch protokolliert. Die PVS-Fachadministratoren haben keinen Zugriff auf die Funktionen und Inhalte des PVS-Logbuches.

6. Eingabekontrolle

Das PVS verfügt über ein integriertes Logbuch, in dem folgende Aktivitäten protokolliert werden:

a) erfolgreiche und erfolglose Anmeldungen und Abmeldungen beim PVS,
b) die Einrichtung von Benutzern und die Verwaltung von deren Zugriffsrechten,
c) die Eingabe, Änderung und das Löschen aller Daten und
d) die Abfrage von Daten innerhalb von Suchfunktionen, Berichten und Abfragen.

Die PVS-Fachadministratoren und die PVS-Benutzer haben keinen Zugang zum PVS-Logbuch. Für die Verwaltung des Logbuches existiert eine spezielle PVS-Funktion, die nur der Datenschutzbeauftragte PVS aufrufen kann. Logbuch-Einträge werden nach einem Jahr Speicherung automatisch gelöscht.
Mit diesem Verfahren können Manipulationen durch PVS-Benutzer weitestgehend ausgeschlossen sowie anhand der Protokolleintragungen aufgeklärt werden. Der Datenschutzbeauftragte PVS führt in regelmäßigen Abständen (mindestens halbjährlich) stichprobenartig Auswertungen im Logbuch des PVS durch. Diese Auswertungen sind durch ihn zu dokumentieren.

7. Organisationskontrolle

Die Server, auf denen Personendaten gespeichert werden, sind getrennt von den Arbeitsstationen in einem separaten Raum aufgestellt.

Folgende Maßnahmen zur räumlichen Sicherheit der Server wurden getroffen:

a) Zugang zu diesem Raum haben nur dazu befugte Personen (LAN-Administrator) und
b) fensterloser Raum.

Jeder Raum, in dem sich PVS-Arbeitsstationen befinden, wird beim Verlassen verschlossen. Wenn eine gestartete PVS-Arbeitsstation eine bestimmte Zeit lang nicht genutzt wird, wird ein Bildschirmschoner aktiv, der nur durch ein Passwort deaktiviert werden kann.

8. Datensicherung

Die Sicherung der PVS-Datenbank wird täglich außerhalb der regulären Arbeitszeit zusammen mit der Datensicherung des gesamten lokalen Netzes durchgeführt. Die Datensicherungen werden in einem feuerfesten Stahlschrank deponiert.