Stand: Juni 2019

Inhalt:

Im dPerso Informationssicherheits-Revisions-Konzept (IS-Revision dPerso) werden Regelungen für die praktische Umsetzung festgelegt.

5010 – dPerso
Informationssicherheits-
Revisions-Konzept

der Versorgungsausgleichskasse der Kommunalverbände in Schleswig-Holstein

|  |  |  |  |
| --- | --- | --- | --- |
| 1 |  | Versionshistorie............................................................................ | 3 |
|  |  |  |  |
| 2 |  | Grundsätzliche Ziele der Informationssicherheits-Revision-dPerso.......................................................................................... | 3 |
|  |  |  |  |
| 3 |  | Aufgaben der Revision................................................................. | 4 |
|  | 3.1 | Vorbereitung der Revision............................................................ | 4 |
|  | 3.1.1 | Prüfer IS-Revision........................................................................ | 4 |
|  | 3.1.2 | Rahmenbedingungen................................................................... | 4 |
|  | 3.2 | Erstellung eines Prüfplans............................................................ | 5 |
|  | 3.3 | Dokumentenprüfung..................................................................... | 5 |
|  | 3.4 | Vor Ort Prüfung............................................................................ | 5 |
|  | 3.5 | Auswertung der Vor-Ort Prüfung.................................................. | 6 |
|  | 3.6 | Erstellung Revisionsbericht.......................................................... | 6 |
|  |  |  |  |
| 4 |  | Fortschreibung des IS-Revisions-Konzept................................... | 6 |
|  |  |  |  |

***In Abstimmung mit der Gleichstellungsbeauftragten ist auf die weibliche Form der Bezeichnungen verzichtet worden, um eine bessere Lesbarkeit zu erreichen.***

|  |  |
| --- | --- |
| **1** | **Versionshistorie**  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Datum | Geänderte Kapitel | Bemerkungen | AbnahmeDatum/Kürzel |
| 1.0 | 29.04.16 | alle | Erstbearbeitung | 29/04/16 AS |
| 1.1 | 01.06.16 | 3.1, 3.4 | Präzisierung Protokolle | 02/06/16 AS |
| 1.2 | 07.06.16 | 3.1, 3.2 | Erweiterung auf Maßnahmenprüfung | 07/06/16 AS |
| 2.0 | 24.06.19 | alle | Aktualisierung (dPerso etc.) | 25/06/19 AS |

|  |  |
| --- | --- |
| **2** | **Grundsätzliche Ziele der Informationssicherheits-Revision dPerso**  |

Viele Geschäftsprozesse in der VAK werden elektronisch unterstützt und große Mengen von Informationen sind digital gespeichert, werden digital verarbeitet und in IT-Netzen übermittelt. Damit sind die VAK und ihre Mitglieder von einem einwandfreien Funktionieren der eingesetzten Informationstechnik und deren Anwendung abhängig. Deshalb ist Informationssicherheit ein Muss.

Den steigenden Bedrohungen für die Verfügbarkeit, die Vertraulichkeit und die Integrität von Daten, IT-Systemen und Prozessen wirkt ein angemessenes Informationssicherheitsmanagement entgegen.

Bestandteil des Informationssicherheitsmanagement ist die Informationssicherheitsrevision.

Ziel einer IS-Revision ist es, das aktuelle Sicherheitsniveau innerhalb der VAK durch eine unabhängige Instanz festzustellen und Hinweise zu bestehenden Sicherheitslücken und -mängeln zu geben.

Da dPerso eine Auftragsdatenverarbeitung ist und über Dataport zur Verfügung gestellt wird, ist eine Prüfung bei Dataport auch Inhalt dieser Prüfung.

Ein allgemeines IS-Revisionskonzept ist noch zu erstellen.

Die Prüfintervalle sind bislang noch nicht festgelegt, eine Prüfung alle 3 Jahre erscheint angemessen.

|  |  |
| --- | --- |
| **3** | **Aufgaben der Revision** |

|  |  |
| --- | --- |
| **3.1** | **Vorbereitung der Revision** |

**3.1.1 Prüfer IS-Revision**

In der VAK gibt es derzeit keinen IT-Sicherheitsbeauftragten, daher ist ein geeigneter Prüfer zu finden.

Als Revisor kann nicht der Fachverantwortliche berufen werden, da dieser sich selbst kontrollieren würde. Als Prüfer kommen daher nur Personen die

* in einer unabhängigen Stellung in der Organisation der VAK (zur Vermeidung von Interessenkonflikten) sind,
* ein unmittelbares Vorspracherecht bei dem Geschäftsführer haben sowie
* über ausreichende Kenntnisse der Informationssicherheit, insbesondere der Vorgehensweise nach IT-Grundschutz verfügen.

Damit entfällt auch die IT-Abteilung als Prüfer.

Mit der IS-Revision ist bis auf weiteres die Datenschutzbeauftragte betraut worden.

**3.1.2 Rahmenbedingungen**

Zu Beginn jeder Revision werden die Rahmenbedingungen (Zeit, beteiligte Personen) mit den Verfahrensverantwortlichen abgesprochen und erforderliche Dokumente bzw. Zugriffsmöglichkeiten angefordert.

Erforderliche Dokumente sind:

* Rollen-Rechte dPerso VAK
* Rollen-Rechte dPerso Dataport
* Admin Rechte dPerso Dataport
* Auszüge Datenschutz-Protokoll
* Auszüge Rollen-Berechtigungsliste-Protokoll
* Auszüge User-Berechtigungsliste-Protokoll
* Auszüge maskenbezogene Protokollierung
* Auszüge administrative lesende Zugriffe

Zu den Protokollen maskenbezogene Protokollierung sowie administrative lesende Zugriffe gibt es über die Rolle Protokollprüfung in dPerso einen vollständigen Zugriff.

Eine Einsichtnahme in die anderen Protokolle kann mit Terminvereinbarung in der fachlichen Leitstelle von Dataport erfolgen.

Auch die Überprüfung der getroffenen organisatorischen und technischen Maßnahmen zur Datenvermeidung, Datensparsamkeit und Datensicherheit (siehe auch CD dPerso) gehört in den Prüfplan.

|  |  |
| --- | --- |
| **3.2** | **Erstellung eines Prüfplans** |

Auf Grundlage der Dokumente wird ein Prüfplan erstellt. Verschiedene Geschäftsvorfälle im dPerso Basispaket (z.B. Neuanlage Abrechnungsfall, Änderung Eingruppierung, Import von geänderten Lohnsteuerdaten) sollen exemplarisch untersucht werden. Anbei ein Muster Prüfplan Geschäftsvorfälle.

Ebenso müssen die getroffenen organisatorischen und technischen Maßnahmen zur Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Intervenierbarkeit und Nicht-Verkettbarkeit überprüft werden. Anbei ein Muster Prüfplan Maßnahmen.

|  |  |
| --- | --- |
| **3.3** | **Dokumentenprüfung** |

Anhand des Prüfplans werden die vorliegenden Dokumente und Maßnahmen einer inhaltlichen und praktischen Prüfung unterzogen und dokumentiert. Gegebenenfalls werden weitere Dokumente nachgefordert.

|  |  |
| --- | --- |
| **3.4** | **Vor Ort Prüfung** |

Die Vor-Ort-Prüfung erfolgt sowohl in der VAK als auch bei Dataport. Sie beginnt mit einem Eröffnungsgespräch mit den Hauptbeteiligten. Dann folgt die Prüfung nach den aufgeführten Prüfmethoden sowie eine vorläufige Auswertung. Beendet wird die Vor-Ort-Prüfung mit einem Abschlussgespräch.

Prüfmethoden sind:

* mündliche Befragung,
* Inaugenscheinnahme von Systemen, Orten, Räumlichkeiten und Gegenständen,
* Beobachtungen,
* Aktenanalyse (auch elektronische Akten),
* technische Prüfung (z.B. Zutrittskontrollen),
* Datenanalyse und
* schriftliche Befragung.

Die Wahl der Prüfmethoden soll nach dem Grundsatz der Verhältnismäßigkeit erfolgen.

Bei der Feststellung von Abweichungen wird bedarfsorientiert der Sachverhalt näher untersucht. Die Prüfung schließt erst mit der Klärung des Sachverhalts ab.

Durch den begrenzten Zugriff auf die unter 3.1.2 genannten Protokolle sind mindestens 5 verschiedene Geschäftsvorfälle gemäß dem Prüfplan Geschäftsvorfälle Revision zu betrachten.

|  |  |
| --- | --- |
| **3.5** | **Auswertung der Vor-Ort Prüfung** |

Alle Informationen, die während der Vor-Ort-Prüfung erhoben wurden, werden weiter konsolidiert, ausgewertet und protokolliert. Anbei ein Muster.

|  |  |
| --- | --- |
| **3.6** | **Erstellung Revisionsbericht** |

Die Ergebnisse werden am Ende der Prüfung in einem Bericht zusammengefasst. Dieser wird den Verfahrensverantwortlichen bei der VAK und bei Dataport bekannt gegeben. Bei Bedarf wird den Verfahrensverantwortlichen der Bericht erläutert.

Bei Verfahrensmängeln ist der Mangel zu erläutern, eine Frist für die Behebung zu setzen und zu kontrollieren, ob der Mangel behoben wurde.

|  |  |
| --- | --- |
| **4.** | **Fortschreibung des IS-Revisions-Konzept** |

Die Fortschreibung des IS-Revisions-Konzept sollte spätestens 2020 erfolgen.