Arbeitsrichtlinie Individuelle Datenverarbeitung

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Individuelle Datenverarbeitung
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	01.12.2020
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
20.0	01.12.2020	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.0.	Daniel Fürdauer
21.0	09.11.2021	Redaktionelle Änderungen in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.0 in den Kapiteln 3.4 und 3.5.	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. EINLEITUNG

Individuelle Datenverarbeitung (IDV) ist die Erstellung, Weiterentwicklung und der Betrieb von Anwendungen durch die Endbenutzer an ihrem Arbeitsplatz – ohne jegliche Beteiligung der IT-Abteilung – um Problemstellungen aus ihren Aufgabenbereichen zu lösen.
Es kann sich z. B. um Berechnungen oder Arbeitsablaufautomatisierungen in Excel- oder Access-Anwendungen, fremdbezogene oder selbst erstellte Software, Statistik-Anwendungen, Tarifierungshilfsmittel oder Web-Services handeln.
Grundsätzlich sind Systeme zu bevorzugen, die durch die IT-Abteilung betrieben werden und damit unter Nutzung des Software-Entwicklungsprozesses eingeführt wurden. Der Einsatz von IDV kann jedoch sinnvoll sein, wenn beispielsweise kurze Entwicklungszeiten, schnelle Anpassungen bei geänderten oder neuen Anforderungen notwendig sind, die Abbildung wechselnder, komplexer Logiken mit Expertenwissen erforderlich ist oder die Erstellung, die Beschaffung und / oder der Betrieb durch die IT-Abteilung unverhältnismäßig aufwändig wäre. Auch beim Einsatz von IDV sind die Grundsätze der Informationssicherheit zu beachten, um Risiken zu minimieren und Schäden zu vermeiden. Wie mit IDV umzugehen ist, ist in den nachfolgenden Kapiteln beschrieben.

2. ADRESSATEN

Die Risikoverantwortlichen der Fachbereiche sind für den Betrieb der von ihnen betriebenen IDV, für deren Inventarisierung sowie zur Umsetzung aller weiteren nach dieser Richtlinie geforderten Maßnahmen verantwortlich.
Die Verantwortung für die IDV trägt der Risikoverantwortliche des nutzenden Fachbereichs (in der Regel Abteilungsleiter). Er hat regelmäßig zu prüfen, ob die Notwendigkeit für den Betrieb einer IDV weiterhin besteht, ob ausreichend qualifiziertes Personal zum Betrieb der IDV vorhanden ist und ob durch eine veränderte Situation Anpassungen erforderlich sind.

3. IDV-STEUERUNG

Die Steuerung der IDV ist in vier Schritte gegliedert:

1. Vorfilter zur Identifikation von relevanter IDV.
2. Klassifizierung zur Feststellung des IDV-Schutzbedarfes.
3. Registrierung der wesentlichen / kritischen IDV.
4. Maßnahmen zur Risikoreduktion.

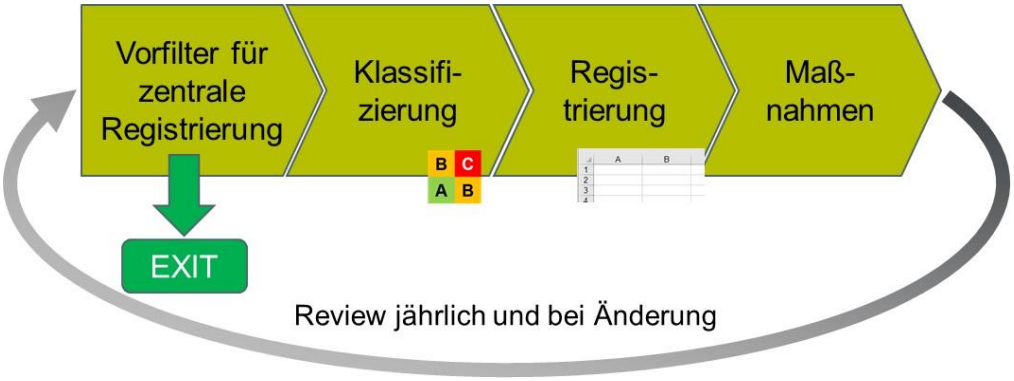

Abbildung 1: IDV Steuerung

Mindestens jährlich und bei Veränderungen muss zur Aktualisierung dieser Prozess wiederholt werden.
Die Klassifizierung der IDV durch die Risikoverantwortlichen, sowie die ordnungsgemäße Inventarisierung unterliegt der unabhängigen Überwachung durch die Stabstelle Datenschutz und Informationssicherheit.

3.1. Vorfilter

Mit dem Vorfilter wird der Zweck verfolgt, relevante IDV, d. h. insbesondere solche, die aus Risikogesichtspunkten weiterer Betrachtung bedarf, zu identifizieren.
Eine Anwendung muss nicht zentral registriert werden (= Vorfilter), wenn mindestens **eine** der folgenden Bedingungen zutrifft:

1. Die IDV wird nicht dauerhaft / regelmäßig eingesetzt wird oder
2. sie ist eine einfache Anwendung mit einfacher Funktionalität oder
3. sie stellt nur eine reine Protokoll- / Transferdateien dar oder
4. sie ist nur eine Datensammlung ohne eigene Funktionalität aus unterschiedlichen Quellen und ohne Veränderung der Daten.

Die Nutzung ist auch dann „regelmäßig“, wenn die Anwendung jährlich eingesetzt wird. Die Nutzung ist „dauerhaft“, wenn kein Enddatum (wie zum Beispiel in Projekten) bekannt ist.
Die Eigenschaft „einfach“ wird im Kontext der Kompetenz der Gruppe der Entwickler und Nutzer der Anwendung gesehen.
Die Einordnung obliegt dem Risikoverantwortlichen.

3.2. Klassifizierung der IDV

Die auf diese Weise identifizierten IDV-Anwendungen werden mittels zweier Kriterien klassifiziert:

- Kritikalität des unterstützten Geschäftsprozesses und
- Bedeutung der IDV für diesen Geschäftsprozess.

Diese können jeweils die Ausprägung „hoch“ oder „niedrig“ haben.

Aus der jeweiligen Kombination dieser Ausprägungen wird die Klasse, d.h. der Schutzbedarf der IDV, anhand der nachstehenden Tabelle ermittelt. Diese Klasse steht für den Schutzbedarf der IDV.
Die Klasse der IDV ergibt sich aus der folgenden Zuordnung:

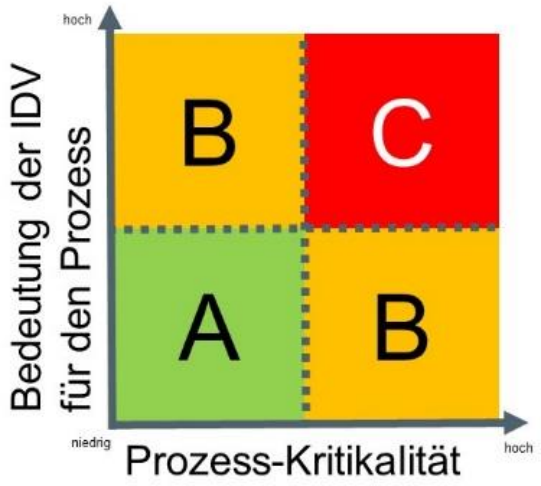

Abbildung 2: IDV-Klassen

BEDEUTUNG FÜR DEN PROZESS	PROZESSKRITIKALITÄT	KLASSE DER IDV
niedrig	niedrig	A
niedrig	hoch	B
hoch	niedrig	B
hoch	hoch	C

IDV-Anwendungen der Klasse A müssen nicht in dem zentralen Register registriert werden, da sie über die Klassifizierung als nicht kritisch oder wesentlich identifiziert wurden.
Für diese Anwendungen gelten auch die allgemeinen Sicherheitsvorgaben der VAV.

3.2.1. Kritikalität des unterstützten Prozesses

Wenn die IDV Anwendung einen der folgenden Prozesse unterstützt, wird die Kritikalität des von der IDV unterstützten Prozesses als „hoch“ eingeschätzt:

- Prozess mit gesetzlichem oder regulatorischem Zweck (wie Rechnungslegung, Steuern, Risikomanagement etc.)
- Schadens- und Auszahlungsprozesse
- Prozesse von Schlüsselfunktionen[1]

[1] Versicherungsmathematische Funktion, Risikomanagement, Interne Revision und Compliance Funktion.

- Kundenprozesse (u. a. Vertrieb).

Die Kritikalität ist ebenfalls „hoch“, wenn die IDV in Prozessen eingesetzt wird, die eine hohe Entscheidungsrelevanz haben:

- Der Geschäftsprozess ist Grundlage für wesentliche Organberichterstattungen (z. B. Aufsichtsrat) oder Vorstandsentscheidungen.
- Der Prozess ist rechnungslegungsrelevant und liefert damit substanzielle Informationen an externe Prüfer (z. B. Wirtschaftsprüfer) oder Aufsichtsbehörden (z. B. FMA).

Sofern der Risikoverantwortliche den unterstützten Prozess davon abweichend dennoch als bedeutend einschätzt, muss er die Prozesskritikalität ebenfalls auf „hoch“ setzen.
Andernfalls ist die Prozesskritikalität „niedrig“.

3.2.2. Bedeutung für den unterstützten Prozess

Die Bedeutung der IDV-Anwendung für den unterstützten Prozess ist „hoch“, wenn ein hohes Bedürfnis an der

- Integrität der Daten (Korrektheit)
- der Verfügbarkeit der Ergebnisse oder
- der Vertraulichkeit der Daten

besteht.
Andernfalls ist die Bedeutung der IDV-Anwendung für den Prozess „niedrig“, es sei denn, der Risikoverantwortliche schätzt die Bedeutung aus anderen Gründen als „hoch“ ein.

3.3. Registrierung der IDV

IDV Anwendungen der Klasse A (Prozesskritikalität **und** Bedeutung für den Prozess sind beide „niedrig“ eingeschätzt) müssen **nicht** zentral registriert werden.
IDV-Anwendungen der Klasse „B“ und „C“ müssen wegen des durch sie verursachten Risikos registriert werden.
Neben den Stammdaten (Name der IDV, Name des Risikoverantwortlichen, Ansprechpartner etc.) ist die vorgenommene Klassifizierung der IDV (siehe Kapitel 3.2) zu dokumentieren sowie eine Dokumentation der für die IDV ergriffenen technisch-organisatorischen Maßnahmen.
Die Registrierung erfolgt in einem zentralen Register.

3.4. Technische und organisatorische Maßnahmen

Der Risikoverantwortlich muss seine IDV-Anwendungen risikogerecht schützen, um Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der IDV angemessen sicherzustellen.
Grundsätzlich sind dieselben Datenschutz- und Informationssicherheitsanforderungen anzustreben, wie für die zentral zur Verfügung gestellten Anwendungssysteme.
Die zu treffenden Maßnahmen sind von der Risikowirkung der IDV abhängig und unterscheiden sich bei IDV der Klasse „B“ und „C“ durch ihre Intensität.
Im Anhang sind weitere Hinweise dazu aufgeführt.
Folgende Anforderungen gelten für alle IDV-Klassen:

- Kein Kopfmonopol: sowohl auf Entwickler- und auf Benutzerseite muss es Vertreter geben, die die Anwendung nach angemessen kurzer Zeit selbst weiterentwickeln bzw. benutzen können.

Bei Fremdentwicklungen ist entweder ein Know-How-Transfer sicherzustellen oder ein entsprechender Servicevertrag abzuschließen (siehe auch Vorgaben zu Dienstleistern)

- Jede IDV, die innerhalb der Systeme der VAV betrieben wird, profitiert von der allgemeinen Informationssicherheit der VAV. Am Beispiel der Abteilungsverzeichnisse ist dieses:
    - etablierter Zugriffsschutz (Vertraulichkeit)
    - Backup und Möglichkeit der einfachen Versionierung (Verfügbarkeit)
- Für jede IDV ist zu prüfen, ob sie durch die IT-Abteilung betrieben werden kann.

Folgende Anforderungen an die IDV Klassen „B“ und „C“ sind von Risikoverantwortlichen zu erfüllen und zu dokumentieren.

MAßNAHME	BESCHREIBUNG
Zentrale Registrierung	• IDV wird im zentralen IDV-Register erfasst
Dokumentation	• Benutzer- und Anwendungsdokumentation abhängig von Kompetenzniveau der Entwickler und Benutzer.
Test	• Definierte Testfälle • Testdokumentation und Testnachweis (unter Beachtung des Vier-Augen-Prinzips – Tester ungleich Entwickler)
Zugriffsschutz	• Einschränkung des Zugriffs auf berechtigte Personen (z. B. über Laufwerksberechtigung) • Differenzierte Zugriffsrechte (lesend, verändernd, löschend)
Integrität	• Validierungen / Plausibilisierungen (technisch oder organisatorisch) • Differenzierte Zugriffsrechte (lesend, verändernd, löschend)
Versionierung	• Versionskennzeichnung • Dokumentation des Delta zur Vorversion
Verfügbarkeit	• Sicherstellung der Verfügbarkeit von qualifiziertem Personal (Vermeidung von Kopfmonopolen) • Regelmäßige Datensicherung der IDV (unter Nutzung der existierenden VAV Verfahren)

Tabelle 1: Anforderungen an IDV-Klassen „B“ und „C“

Weitere Hinweise zur Ausgestaltung der technisch-organisatorischen Maßnahmen sind im Anhang dargestellt.

3.5. Aktualisierung

Einmal pro Jahr muss der Prozess zur IDV-Steuerung und Inventarisierung erneut durchgeführt und formlos dokumentiert werden.

Hinweise zu den technischen und organisatorischen Maßnahmen

Dokumentation

Für jede IDV ist eine angemessene Dokumentation zu erstellen.
Im Falle von z. B. Excel-IDV kann die Dokumentation gegebenenfalls in der jeweiligen Excel-Datei erfolgen. Auch ist eine Dokumentation im Sourcecode zum Beispiel bei SAS denkbar.
Die Dokumentation muss einen technischen und fachlichen Teil umfassen.
Der technische Teil muss die Funktionsweise und insbesondere technische Besonderheiten enthalten. Er muss einen kundigen Dritten in die Lage versetzen die Anwendung weiterentwickeln zu können.
Der fachliche Teil muss einen fachkundigen Benutzer in die Lage versetzen, die Anwendungen fehlerlos bedienen zu können.

Test

Jede Anwendung muss technisch und fachlich getestet werden.
Der Test muss durch andere Personen als die Entwickler durchgeführt werden. Der technische Test und der fachliche Test können allerdings durch die gleiche Person durchgeführt werden.
Der Test, sein Umfang und das Ergebnis sind zu dokumentieren.

Zugriffsschutz

Es ist festzulegen und zu dokumentieren, durch wen und wie auf die IDV zugegriffen werden darf und wie die Zugriffsberechtigungen vergeben, gesteuert und jährlich rezertifiziert werden.
Sofern möglich, sollte der Zugriffsschutz bestehende Verfahren nutzen, wie zum Beispiel auf den Abteilungs-, Gruppen-, oder anderen Laufwerken.
Gegebenenfalls können IDV Anwendungen per Passwort, Zell- und Blattschutz geschützt werden.

Integrität

Für die Sicherstellung der Integrität der IDV-Anwendungen sollte auf Eingabe-/Ausgabekontrollen wie Plausibilitäts- bzw. Summenkontrollen, Feldsperren; Mussfelder, Prüfziffern/-summen oder ähnliches zurückgegriffen werden.
Gegebenenfalls ist es denkbar, diese auch organisatorisch sicherzustellen.
Auch die technische Trennung von Eingabe, Berechnung und Ausgabe (im Falle von Excel z. B. auf unterschiedlichen Tabellenblättern) kann die Integrität erhöhen.
Es kann förderlich sein, für Entwicklungs-, Test- und produktive Versionen unterschiedliche Ablageorte zu wählen.
Insbesondere bei IDV Anwendungen der Klasse „C“ ist zu prüfen, welche Frequenz für zusätzliche Tests erforderlich sind, um (versehentliche) Veränderungen der IDV entdecken zu können.

Versionierung

Es muss dokumentiert werden, welche Veränderungen in einer IDV durchgeführt wurden. Die Version der IDV muss vermerkt sein und es muss transparent sein, welche Ergebnisse mit welcher Version erstellt wurden.

Verfügbarkeit

Durch Datensicherungen ist die Verfügbarkeit der IDV sicherzustellen.
Die (Abteilungs-) Laufwerke der VAV werden gesichert und bieten eine grundlegende Datensicherung.