Arbeitsrichtlinie Informationsklassifizierung

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Informationsklassifizierung
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	10.10.2019
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
19.0	10.10.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.2.	Daniel Fürdauer
20.0	04.12.2020	Redaktionelle Änderungen und Änderungen in Anlehnung an die Arbeitsrichtlinien der VHV bis zur Version 20.2	Daniel Fürdauer
21.0	08.11.2021	Redaktionelle Änderungen in Kapitel 1 und 3 in Anlehnung an die Arbeitsrichtlinien der VHV bis zur Version 21.1	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

TABELLENVERZEICHNIS

1. ZIELSETZUNG

Damit sichergestellt ist, dass Informationen über ein angemessenes Schutzniveau verfügen, sind diese anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung zu klassifizieren. Informationen bezeichnen alle Daten und Dokumente, die nicht durch die Schutzbedarfsfeststellung erfasst werden, unabhängig davon, in welcher Form sie vorliegen (elektronisch, gesprochen, auf Papier etc.).
Die Klassifikation bietet Personen im Umgang mit Informationen eine prägnante Angabe zu deren Handhabung und den notwendigen Schutzanforderungen.

2. KLASSIFIZIERUNG VON INFORMATIONEN

2.1. Grundsätzliche Regelungen

Die Klassifizierung von Informationen ist vom Dokumentenverantwortlichen bzw. Informationseigentümer vorzunehmen.
Die Bezeichnung „persönlich“ ist keine Klassifizierung, sondern ein postalischer Hinweis, dass die Informationen nur für den Empfänger persönlich bestimmt sind.
Bei der Zusammenfassung unterschiedlich klassifizierter Informationen müssen die Informationen entsprechend der höchsten Klassifikation behandelt werden (z. B.: Versand mehrerer Informationen in einer E-Mail).
Nicht-klassifizierte Informationen sind automatisch wie „Intern“ klassifizierte Informationen zu behandeln. Gleiches gilt für nicht-klassifizierte Informationen externer Herkunft.
Sofern Informationen von VAV-fremden Absendern mit einer Vertraulichkeitsstufe gekennzeichnet wurden, sind diese mit einer vergleichbaren Vertraulichkeitsstufe entsprechend dieser Richtlinie zu behandeln.

2.2. Klassifizierungsstufen

Folgende Leitfragen können zur Bestimmung der Klassifikation herangezogen werden:

- Welcher potenzielle Schaden kann bei einer unerwünschten Offenlegung oder Weitergabe der Information entstehen?
- Welcher Personenkreis darf die Information zur Kenntnis nehmen?
- Welche Art von Daten sind betroffen und unterliegen diese ggf. gesetzlichen Anforderungen?

Die Klassifikation kann entweder „offen“, „intern“, „vertraulich“ oder „streng vertraulich“ sein. Die einzelnen Stufen sind in der nachfolgenden Übersicht mit Beispielen erläutert.

Klassifikation	Schadenpotenzial	Beispiele
Offen	Kein Schaden zu erwarten, da die Informationen für die Öffentlichkeit bestimmt sind	Informationen, die der Allgemeinheit aus öffentlich verfügbaren Quellen frei zugänglich sind. Diese Quellen sind beispielsweise: • Verzeichnisse von Postleitzahlen, Bankleitzahlen • Öffentliche Telefonverzeichnisse und Handelsregister • Produktflyer • Pressemitteilungen • Veröffentlichte Geschäftsberichte • Inhalte der Internetpräsenz der VAV
Intern	Keine weitreichenden Konsequenzen, z. B. rechtlicher oder finanzieller Art zu erwarten	Informationen, die in der VAV einem größeren Mitarbeiterkreis zugänglich sein sollen. Hierzu können auch externe Mitarbeiter gehören. Beispiele sind: • Mitarbeiter-Adressbuch • Organigramme Hinweis: Die Häufung von „Intern“ klassifizierten Informationen kann zu einer Erhöhung der Klassifizierung führen
Vertraulich	Rechtliche Konsequenzen (Bußgelder, Vertragsstrafen, Schadensersatzansprüche etc.) in geringem Umfang Ansehen der VAV in geringem Maße beeinträchtigt	Informationen, die nur einem definierten Personenkreis zur Verfügung stehen dürfen, wie z. B.: • Vertrags-, Schaden- Inkasso- und Leistungsdaten • Partnerdaten • Rechnungslegungsrelevante Unterlagen • Interne Geschäftsdaten (z. B. Controlling-Daten, Kalkulationen, etc.) • Informationen, die im Rahmen einer Vertraulichkeitsvereinbarung erlangt worden sind • Gremieninformationen, soweit sie nicht zur Veröffentlichung in einem weiteren Kreis bestimmt sind oder höher klassifiziert wurden • Managementberichte, z. B. von Schlüsselfunktionen • Personalakten, Gehaltsabrechnungsdaten, Bewerbungsunterlagen • Mitarbeiterdaten außerhalb der Personalakte, wie z. B. Informationen zur Zeiterfassung • Betriebskonzepte, Netzwerkpläne und sicherheitsrelevante Dokumentationen

Klassifikation	Schadenpotenzial	Beispiele
Streng vertraulich	Erhebliche rechtliche Konsequenzen (Bußgelder, Vertragsstrafen, Schadensersatzansprüche etc.) Nachhaltiger Verlust von Ansehen und Vertrauen bei Kunden, Vertriebspartnern etc.	Informationen, die in der Regel nur einem sehr eng begrenzten Personenkreis zur Verfügung stehen, wie z. B.: • Entscheidungen des Vorstands / Geschäftsführung, Gesellschafterversammlung oder Aufsichtsrat, die bewusst für einen engen Adressatenkreis vorgesehen sind • Geschäftsgeheimnisse • Besondere Arten personenbezogener Daten gemäß der DS-GVO / DSG, insbesondere Gesundheitsdaten • Informationen über Straftaten • Daten des Betriebsarztes • Verträge von Kunden im Zeugenschutzprogramm bzw. mit nachgewiesener Schutzbedürftigkeit • Identitätsdaten der Mitarbeiter (beispielsweise Kennwörter) • Kennwörter, Notfallkennwörter, Master-Kennwörter (Dürfen nicht vollständig per E-Mail versendet werden) • Risikoberichte (z.B. ORSA-Bericht)

Tabelle 1: Klassifizierungsstufen

3. UMGANG MIT KLASSIFIZIERTEN INFORMATIONEN

Wie wird gekennzeichnet?	Offen	Intern	Vertraulich	Streng vertraulich
Kennzeichnung von Dokumenten	Siehe Arbeitsrichtlinie „Lenkung dokumentierter Informationen“			

Was mache ich bei…?		Offen	Intern	Vertraulich	Streng vertraulich
Vervielfältigung mittels Kopierer, Drucker		Keine Einschränkungen	Keine Einschränkungen	Beaufsichtigung des Vervielfältigungsvorgangs	Nur nach Freigabe durch den Dokumentenverantwortlichen bzw. dem Informationseigentümer, Beaufsichtigung des Vervielfältigungsvorgangs
Weitergabe		Keine Einschränkungen	An alle Mitarbeiter der VAV bzw. beauftragte Dienstleister, sofern betrieblich notwendig oder vertraglich vereinbart. (z.B. Vertraulichkeitsvereinbarung)	Weitergabe an vom Dokumentenverantwortlichen bzw. Informationseigentümer definierte Nutzer (namentlich oder Rollen), sofern betrieblich notwendig oder vertraglich vereinbart. Bei externen Empfängern/Dienstleistern muss z.B. eine Vertraulichkeitsvereinbarung vorliegen	Weitergabe nur an namentlich vom Dokumentenverantwortlichen bzw. Informationseigentümer definierte Nutzer. Vom Empfänger dürfen streng vertrauliche Informationen nur nach expliziter Freigabe des Dokumentenverantwortlichen bzw. Informationseigentümers weitergegeben werden. Bei externen Empfängern/Dienstleistern muss z.B. eine Vertraulichkeitsvereinbarung vorliegen
Übermittlung per Post	**Intern**	Keine Einschränkungen	Hauspostmappe	Verschlossener Briefumschlag	Verschlossener Briefumschlag, sofern möglich mit dem Zusatz „persönlich“
	Extern	Keine Einschränkungen	Verschlossener Umschlag	Verschlossener Briefumschlag	Verschlossener Briefumschlag

Was mache ich bei…?		Offen	Intern	Vertraulich	Streng vertraulich
Übermittlung per E-Mail	**Intern**	Keine Einschränkungen	Keine Einschränkungen	Keine Einschränkungen bei der Übermittlung	Keine Einschränkungen bei der Übermittlung
	Extern	Keine Einschränkungen	Keine Einschränkungen	Verschlüsselte Übermittlung	Verschlüsselte Übermittlung
Übermittlung per Fax	**Intern**	Keine Einschränkungen	Keine Einschränkungen	Keine Einschränkungen	Nur nach Vorankündigung
	Extern	Keine Einschränkungen	Keine Einschränkungen	Der Empfänger des Faxes muss im Vorwege über dessen Versand informiert werden	Eine Übertragung per Fax ist nur in Ausnahmefällen zulässig. Der Empfänger des Faxes muss im Vorwege über dessen Versand informiert werden
Verbale Weitergabe		Keine Einschränkungen	Nur erlaubt, wenn keine Unberechtigten zuhören können		Nur erlaubt, wenn keine Unberechtigten zuhören können. Nicht auf Anrufbeantworter / Mailbox hinterlassen. Identität des Gesprächspartners sicherstellen
Vernichtung von Informationen in Papierform		Keine Einschränkungen	Gemäß Arbeitsrichtlinie „Entsorgung von Datenträgern“		
Austausch/ Kollaboration über Circuit, MS Teams (VHV) und sonstige genehmigte Kollaborations-Tools	**Intern**	Keine Einschränkungen	Sprache, Video und Präsentation[1]: Keine Einschränkung im Rahmen der berechtigten Teilnehmer Speichern und Hochladen[1]: Speicherung unter Berücksichtigung der Angemessenheit von Zugriffsrechten / Wahrung des „Need-to-Know“ Grundsatzes Eine dauerhafte Dateiablage für Dokumente mit Aufbewahrungs- / Löschfristen oder Auskunftspflichten ist nicht zulässig		Nicht zulässig

[1] Beispiele im Anhang A

Was mache ich bei…?		Offen	Intern	Vertraulich	Streng vertraulich
	Extern	Keine Einschränkungen	Sprache, Video und Präsentation[1]: Es ist sicherzustellen, dass die vertraglichen und rechtlichen Regelungen zur Verschwiegenheit / Vertraulichkeit mit dem Kommunikationspartner ausreichen (NDA, Datenschutz), um interne und vertrauliche Informationen zu übermitteln Speichern und Hochladen[1]: Speicherung unter Berücksichtigung der Angemessenheit von Zugriffsrechten / Wahrung des „Need-to-Know“ Grundsatzes Eine dauerhafte Dateiablage für Dokumente mit Aufbewahrungs- / Löschfristen oder Auskunftspflichten ist nicht zulässig		Nicht zulässig

Informationen in IT-Systemen	Offen	Intern	Vertraulich	Streng vertraulich
Speicherung in IT-Systemen / Anwendungen und interne Kollaborationstools (z.B. Jira, Confluence) der VAV	Keine Einschränkungen	Speicherung unter Berücksichtigung der Angemessenheit von Zugriffsrechten / Wahrung des „Need-to-Know“ Grundsatzes Die Speicherung versicherungstechnischer Informationen auf dem H-Laufwerk ist untersagt.		
Cloud- und Onlinedienste (die nicht bereits durch die VAV eingeführt wurden) **(z.B. Foren, Chats, Cloud-Speicher, PDF-Converter, WhatsApp, Dropbox, Zoom, Facebook, Twitter)**	Keine Einschränkungen	Die Nutzung von offenen oder frei verfügbaren Cloud- oder Online-Diensten bedarf ggf. der rechtlichen, aufsichtsrechtlichen, lizenztechnischen, strategischen, datenschutzrechtlichen oder sicherheitstechnischen Prüfung vor Nutzung oder Inbetriebnahme, ansonsten nicht zulässig		Informationen oder Dokumente dürfen nicht erstellt, hochgeladen oder in Chats genutzt werden
Mobile Endgeräte (z. B. Handys, Notebooks)	Keine Einschränkungen	Keine Einschränkungen	Verschlüsselte Datenträger	Verschlüsselte Datenträger
Mobile Datenträger (z. B. CD, DVD, USB-Stick)	Keine Einschränkungen	Keine Einschränkungen	Verschlüsselung erforderlich, z. B. durch „Drive Lock“ oder „Containerverschlüsselung“	Verschlüsselung erforderlich, z. B. durch „Drive Lock“ oder „Containerverschlüsselung“
Bereitstellung im Internet (Blogs, Foren)	Keine Einschränkungen	Verboten	Verboten	Verboten
Löschung von elektronischen Informationen	Löschung im Filesystem	Löschung im Filesystem	Löschung im Filesystem	Löschung im Filesystem

Entsorgung / Vernichtung von Hardware und mobilen Datenträgern (CD, DVD, USB-Sticks)	Keine Einschränkungen	Gemäß Arbeitsrichtlinie „Entsorgung von Datenträgern“

Physische Aufbewahrung und Ablage	Offen	Intern	Vertraulich	Streng vertraulich
Allgemein	Keine Einschränkungen	Zugriff durch unbefugte Dritte durch einfache Mittel verhindern	Zugriff durch unbefugte Dritte durch angemessene technische Maßnahmen verhindern	Zugriff durch unbefugte Dritte durch angemessene technische Maßnahmen verhindern
Backup-Datenträger (z.B. Bänder, Wechsel-Platten)	Aufbewahrung in einer vor Zugriff und Elementarereignissen geschützten Umgebung (z. B. feuersicheres Behältnis, Datensafe, separater Brandabschnitt)			
In eigenen oder gemieteten Gebäuden der VAV	Keine Einschränkungen	Keine Einschränkungen	Gemäß Arbeitsrichtlinie „Clean Desk“ und Arbeitsrichtlinie „Physische und umgebungsbezogene Sicherheit“	
Unterwegs und zu Hause	Keine Einschränkungen	Abgesperrter Raum, z. B. Hotelzimmer, Heimbüro	Vor Zugriff sicher aufbewahren Grundsätzlich ist der Transport und eine Aufbewahrung außerhalb von VAV Liegenschaften zu vermeiden. Beim Transport und der Aufbewahrung außerhalb von VAV Liegenschaften (z.B. Hotel, Zuhause) ist der Zugriff durch Unberechtigte auszuschließen (z.B. durch verschließbaren Schrank, Sicherheitskoffer, Safe im Hotel).	Vor Zugriff sicher aufbewahren Grundsätzlich sind der Transport und eine Aufbewahrung außerhalb von VAV Liegenschaften nur in Ausnahmefällen und nur nach expliziter Freigabe durch den Dokumentenverantwortlichen bzw. Informationseigentümer gestattet. Beim Transport und der Aufbewahrung außerhalb von VAV Liegenschaften (z.B. Hotel, Zuhause) ist der Zugriff durch Unberechtigte auszuschließen (z.B. durch verschließbaren Schrank, Sicherheitskoffer, Safe im Hotel).

Anhang A: Beispiele für Zulässigkeit in genehmigten Kollaborationstools

Tätigkeiten	Zulässigkeit in „Circuit“, „Skype“ oder „MS Teams (VHV)“?	Grundlage / Voraussetzung
Vorbereiten einer unternehmenskritischen Entscheidung	Nein	Unter der Annahme, dass es sich um streng vertrauliche Informationen handelt
Kopie von Informationen aus der Personalakte von Mitarbeitern hochladen	Nein	Aufbewahrungs- / Löschfristen, Auskunftspflichten werden nicht eingehalten
Implementierung als Teile von versicherungstechnischen Geschäftsprozessen	Nein	Aufbewahrungs- / Löschfristen, Auskunftspflichten werden nicht eingehalten
Schnelle / einfache Kommunikation mit Versicherungsnehmern	Nein	Widerspricht der Betriebsvereinbarung, Aufbewahrungs- / Löschfristen, Auskunftspflichten werden nicht eingehalten
Kommunikation mit Maklern, die keinen regulatorischen Pflichten unterliegt	Ja	Wenn die rechtlichen Grundlagen mit dem Makler geschaffen wurden (Vertrag und Verschwiegenheitserklärung), keine Aufbewahrungs- oder Nachweispflichten für die Kommunikation bestehen und es sich nicht um streng vertrauliche Informationen handelt
Kollaboratives Erstellen von LA-Unterlagen	Ja	Ergebnis muss außerhalb von Teams (VHV) aufbewahrt werden
Kollaboratives Erarbeiten von Ergebnissen (Projekt / Linie)	Ja	Ergebnis muss evtl. außerhalb von Teams (VHV) aufbewahrt werden
Abteilungs- / Ressortkonferenzen (Homeoffice, versch. Standorte)	Ja	Nicht für streng vertrauliche Informationen
Online-Workshops mit externer Moderation	Ja	Wenn alle rechtlichen Grundlagen mit dem Dienstleister geschaffen wurden (z. B. NDA) und nicht für streng vertrauliche Informationen

Übermittlung von großen Dateien an einen externen Dienstleister	Ja	Wenn alle rechtlichen Grundlagen mit dem Dienstleister geschaffen wurden (z. B. Vertrag mit Verschwiegenheitserklärung) und nicht für streng vertrauliche Informationen
Angebotsvorbereitungen mit externen Dienstleistern oder Lösungsanbietern	Ja	Wenn alle rechtlichen Grundlagen mit dem Dienstleister geschaffen wurden (z. B. NDA) und nicht für streng vertrauliche Informationen
Produktpräsentationen von externen Dienstleistern oder Lösungsanbietern	Ja	Wenn von Seiten VAV nur „offen“ klassifizierte Informationen beigetragen werden