Mag. Novotny: Passdaten DSGVO-konform speichern und verarbeiten.

Urteile wegen unberechtigter Verarbeitung von Passdaten! Wie die Echtheit feststellen?

Fakt ist, dass Sie in der **täglichen Praxis immer wieder Ausweiskopien erhalten**. Möglicherweise, weil sich jemand bei Ihnen mit Lebenslauf, Bild und Ausweis für eine Stelle bewirbt. Oder weil Sie aufgrund des **FM-GWG** (Finanzmarkt-Geldwäsche-Gesetz) und den diversen **Geldwäsche-Gesetzen** „bei Begründung einer Geschäftsbeziehung" dazu verpflichtet sind, die Identität des Kunden festzustellen („know your customer"). Dies hat durch einen **amtlichen Lichtbildausweis zu erfolgen,** worunter in Österreich Reisepässe, Führerscheine und Personalausweise fallen.
Auch werden Ihre Dokumentationspflichten in Zeiten von **IDD bzw. MiFID-2** immer umfangreicher. **Dabei kann man vieles falsch machen, wie 3 Urteile zeigen,** die wir für Sie recherchiert haben, um bei Ihnen Problembewusstsein zu wecken. Und wir geben **praxisnahe Tipps** zu folgenden Fragen:

- **Wann** muss ich einen Ausweis **einholen?** Was sagt dazu die **FMA?**
- Worin liegt das **Gefahren-Potential?** Was kann passieren, wenn Passdaten **in die falschen Hände fallen?**
- Wie das **Risiko reduzieren?** Wie **speichere ich ihn sicher** ab? Wie sende ich ihn weiter?
- Wie lange darf oder muss ich ihn **speichern?**
- Wie stellen Sie fest, ob ein vorgelegter ausländischer **Pass echt** ist?
- **Ausgewählte Urteile** im Zusammenhang mit Pass-Daten. **Was daraus lernen?**

Ad) Wann muss ich einen Ausweis verlangen?

Aufgrund des **FM-GWG** (Finanzmarkt-Geldwäsche-Gesetz) und den diversen **Geldwäsche-Gesetzen** sind Sie „bei Begründung einer Geschäftsbeziehung" dazu verpflichtet, die Identität des Kunden festzustellen („know your customer"). Dies hat laut **Leitfaden der FMA** (den Sie hier herunterladen können…) durch einen **amtlichen Lichtbildausweis zu erfolgen,** worunter in Österreich Reisepässe, Führerscheine und Personalausweise fallen.
Konkret wird in § 6 des FM-GWG definiert, dass es zu Ihren Sorgfaltspflichten gehört, die Identität des Kunden anhand eines amtlichen Lichtbildausweises zu überprüfen.

Ad) Worin liegt das besondere Gefahren-Potential bei Pässen?

Sie als Unternehmen, das solche Ausweiskopien **von Kunden sammelt**, müssen sich bewusst sein, dass es sich hier um **besonders wertvolle personenbezogene Daten** handelt, deren Sicherheit Sie – und Ihrer Mitarbeiter - aufgrund der DSGVO sicherstellen müssen. **Wird Ihr Unternehmen „gehackt" und es werden auch solche Daten gestohlen,** dann ist das Missbrauchs-Potential um ein Vielfaches höher, als wenn „nur" die Infos über einen abgeschlossenen Versicherungsvertrag für das KFZ des Kunden gestohlen würden.

Leider macht sich kaum jemand von uns Gedanken, **was ein Betrüger mit dieser Pass-Kopie und den dort darauf befindlichen Daten** (Name, Geburtsdatum, Foto) alles anstellen kann. Etwa damit auf diesem Namen ein **Konto einzurichten und dann für Geldwäsche zu nutzen**. Oder im Internet einzukaufen, Kredite aufzunehmen, usw. Die Betroffenen erfahren davon meist erst Monate später und müssen dann in mühsamen Gerichtsverfahren nachweisen, dass sie die in ihrem Namen getätigten Geschäfte nicht selbst abgewickelt haben und dafür nicht verantwortlich sind.
Daher sollten **wir selbst vorsichtiger werden** bzw. sollten wir **unsere Kunden auf diese Gefahr aufmerksam machen.**

Denn fast alle von uns haben wohl schon gedankenlos unseren **Ausweis eingescannt und per Mail versendet (der wohl unsicherste Übertragungsweg, den es gibt)**, um etwa damit ein Konto oder Sparbuch neu zu eröffnen, einen Leihwagen oder Wohnung zu mieten oder etwa einen Handy-Vertrag abzuschließen, etc.

Daher: Kriminelle nutzen immer häufiger gestohlene Ausweiskopien, um durch diesen Identitätsdiebstahl Straftaten in fremdem Namen zu begehen. Gehen wir also besonders vorsichtig damit um.

ad) Wie das Risiko reduzieren? Wie speichere ich ihn sicher ab? Wie sende ich ihn weiter? Dazu rät Watchlist Internet:

a) Kritisch hinterfragen, ob der Geschäftspartner zu Recht einen Ausweis verlangt (man gibt zu leichtfertig eine Passkopie her)

b) Ausweis „verändern", um Missbrauchsrisiko zu minimieren

Ad a) Kritisch hinterfragen:

JA, einer seriösen Bank, Versicherung, etc. wird man auch künftig eine Ausweiskopie zusenden bzw. für die Online-Identifikation verwenden können. Doch hier ist auf eine **gesicherte Übertragung** zu achten (also Online-Portal mit entsprechenden Sicherheiten, verschlüsselte E-Mail-Übertragung, ein PDF daraus machen und mit einem Passwort versperren und dieses auf einem anderen Wege (etwa SMS) übermitteln, etc.).

Und auch Ihre Kunden immer wieder auf dieses Gefahren-Potential aufmerksam machen. Wenn etwa ein angebliches **Marktforschungsinstitut anbietet,** 100 Euro pro abgeschlossener Umfrage auszuzahlen, man aber dafür eine Ausweiskopie hochladen muss, dann müssen hier alle Alarmglocken läuten. Sofort stoppen. Denn wozu braucht ein Markforschungsinstitut meinen Pass?

Also immer nachdenken und besonders skeptisch werden, wenn jemand einen Ausweis von Ihnen oder Ihren Kunden haben möchte.

Ad b) Ausweis „verändern", um Missbrauchsrisiko zu minimieren

„Watchlist Internet", eine der führenden Informationsplattformen zum Thema Internet-Betrug empfiehlt die eingescannte Ausweiskopie mit dem Hinweis **„KOPIE"** und dem Zusatz „nur für Kontoeröffnung bei Bank XY verwendbar" zu versehen. Wir hören zwar, dass **einige Banken / Versicherer so überarbeitete Kopien nicht akzeptieren würden.** Aber wir betonen hier nochmals, Watchlist Internet ist nicht irgendein Verein, sondern ein Projekt des Internet Ombudsmannes, das in enger Zusammenarbeit mit dem Bundeskriminalamt erfolgt und u.a. vom Bundeskanzleramt, Bundesministerium für Soziales, Gesundheit und Konsumentenschutz (BMASGK), der Bundesarbeitskammer (BAK) und Wirtschaftskammern ermöglicht wird und zur erhöhten Sicherheit im Internet beitragen soll. **Also sollten auch „konservative" Banken / Versicherer derart kompetente Ratschläge annehmen und in die Praxis umsetzen (lassen), weil sie ansonsten im Betrugsfall eine Mitschuld angelastet bekommen könnten.**

Denn wie oben angeführt: Die DSGVO verlangt, dass man die Sicherheit der personenbezogenen Daten sicherstellen muss. Und hier ist die **Sorgfaltspflicht wohl gröblich verletzt, wenn zwar der Versicherungsvermittler einen „mit Kopie" versehenen Pass einreichen will, die Versicherung diesen „geschützten Pass" aber ablehnt.** Das wird man wohl keinem Richter erklären können….

Unwillige Banken /Versicherer könnte man auf eine **ausführliche Handlungsanleitung** des **Landesbeauftragten für Datenschutz in Nordrhein-Westfalen verweisen.** Dort werden z.B. sehr übersichtlich die Gründe aufgelistet, wann welches Unternehmen Ausweiskopien für welche Zwecke verwenden darf und wie man damit umgehen sollte.
Hinweis: Die Landesbeauftragten der deutschen Bundesländer haben eine **ähnliche Funktion wie die Datenschutzbehörde in Österreich** und deren Tätigkeit ist daher sehr wohl beachtenswert, weil die DSGVO eine europäische Verordnung ist, die aber durch Urteile in den Nationalstaaten stetig präzisiert wird.

Und zum Falle der „Markierung als Kopie" oder sogar dem Schwärzen **rät der Datenschutzbeauftragte folgendes:**
„Schwärzung von Angaben"
„Grundsätzlich sind nur der Vor- und Nachname, die Anschrift und gegebenenfalls auch die Gültigkeitsdauer zur Identifizierung erforderlich. Die übrigen Daten dürfen und sollen von Ihnen geschwärzt werden (zum Beispiel die Zugangs- und Seriennummer, die Staatsangehörigkeit, die Größe, die Augenfarbe, das Lichtbild und die maschinenlesbare Zone).
Die Angabe des Geburtsdatums und gegebenenfalls -ortes kann nur erforderlich sein, wenn trotz der vorgenannten Angaben eine Personenverwechslung möglich ist und das Unternehmen in seinem bisherigen Datenbestand überhaupt das Geburtsdatum oder den -ort als Referenzdatum gespeichert hat".
Nachzulesen hier: https://www.ldi.nrw.de/datenschutz/wirtschaft/personalausweis-und-datenschutz

Ad) Wie lange darf / muss man Ausweiskopien speichern?

Laut DSGVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie es für den Zweck der Verarbeitung erforderlich ist. D.h. grundsätzlich für die Dauer der Geschäftsbeziehung. Darüber hinaus nur, wenn gesetzliche Aufbewahrungspflichten dies erfordern (etwa Steuerdaten zumindest **7 Jahre**, usw.).

Weiters wird in § 21 des FM-GWG definiert, dass Sie Kopien von Dokumenten und Informationen, die Sie erhalten haben „für die Dauer von **10 Jahren** nach Beendigung der Geschäftsbeziehung mit dem Kunden" aufzubewahren haben.

Versicherungen in Österreich sind verpflichtet, Dokumente ihrer Kunden für unterschiedliche Zeiträume aufzubewahren, abhängig von den spezifischen gesetzlichen Anforderungen und der Art der Dokumente. Gemäß den unternehmensrechtlichen Aufbewahrungspflichten müssen Versicherungen Daten zu Personen, Drittpersonen (z.B. Mitversicherten), Leistungsfällen und Versicherungsverhältnissen über die Beendigung des Versicherungsverhältnisses hinaus oder nach Abschluss eines Leistungsfalls aufbewahren. Diese Daten werden so lange aufbewahrt, wie die Geltendmachung von Rechtsansprüchen aus dem Versicherungsverhältnis möglich ist (OGH 23.11.2022, 7 Ob 112/22d).

Gemäß § 12 des Versicherungsvertragsgesetzes (VersVG) **verjähren Ansprüche** aus dem Versicherungsvertrag **in 3 Jahren.** Wenn der Anspruch einem Dritten zusteht, beginnt die Verjährung, sobald diesem sein Recht auf die Leistung des Versicherers bekannt wird, und **verjährt spätestens nach 10 Jahren** (§ 12 VersVG). Auch hier wäre es denkbar, dass eine Ausweiskopie im Streitfalle notwendig sein kann. Die Datenschutzbehörde sieht dies allerdings sehr restriktiv.

Versicherungsmakler sind berechtigt, personenbezogene Daten, die notwendig sind, um nachweisen zu können, dass keine Beratungsfehler begangen wurden, entsprechend den schadenersatzrechtlichen Verjährungsfristen des § 1489 ABGB **bis zu 30 Jahre** aufzubewahren. Dies gilt jedoch nicht pauschal für alle Daten, sondern es muss ein individuelles Löschkonzept erstellt werden, das die Speicherdauer im Einzelfall festlegt (Keltner in Koban (Hrsg), Rechte und Pflichten des Versicherungsmaklers3 (2023) Teil G: Datenschutz für Versicherungsmakler). Aber auch hier ist die Datenschutzbehörde sehr restriktiv.

Im 2. Teil des Beitrags – im nächsten BAV-Newsletter – erfahren Sie, wie Sie die unterschiedlichsten Ausweise aus diversen Ländern auf Ihre **Echtheit prüfen können.**

Und erfahren mehr über die **3 Urteile,** die einen Zusammenhang mit dem Umgang von Ausweisen haben, die wir für Sie recherchiert haben, um zu zeigen, was im Zusammenhang mit Ausweisen erlaubt ist und was keineswegs gemacht werden darf.

Quellen: DER STANDARD, NTV, Webseite der Datenschutzbehörde dsb.at, meineberater.at, RIS.at, Webseite des Landesbeauftragten für Datenschutz und Informationssicherheit in NRW

Beste Grüße von RA Mag. Stephan Novotny und Mag. Günter Wagner, B2B-Projekte

Sollten Sie noch keinen Anwalt haben: **Mag. Stephan Novotny,** ein **auf Versicherungs- und Datenschutzrecht spezialisierter Fachanwalt** steht gerne zur Verfügung.
Für Zurich-Newsletter-Leser sogar zum **Spezialpreis.**

RA Mag. Stephan Novotny
1010 Wien, Landesgerichtsstraße 16/12
kanzlei@ra-novotny.at
https://www.ra-novotny.at