Mag. Günter Wagner
B2B Projekte
für Finanz- und Versicherungsbranche

Ausweiskopien: Wie damit in der Praxis umgehen?
Wie sichern Sie die personenbezogenen Daten und wie lange ist Speichern nötig / erlaubt? Was sagen relevante Urteile?

Wir fassen für Sie das **Allerwichtigste** zum Themenkreis zusammen:

> Etwa: Wann muss ich ein Pass einholen? Was sagt dazu die FMA?
> Wie stellen Sie fest, ob ein vorgelegter ausländischer Pass echt ist?
> Wie speichere ich ihn sicher ab? Wie sende ich ihn weiter?
> Wie lange darf oder muss ich ihn speichern?
Und wir haben **interessante Urteile** gefunden, die zeigen, **wie man es nicht machen darf / soll!**

Die **bisher erschienen Praxis-Beiträge von Mag. Novotny auszugsweise:**

DSGVO 22: **Ausweiskopien** in der täglichen Praxis. Hier…
DSGVO 21: Ein Gespenst namens **DORA.** Hier…
DSGVO 20: Vorsicht bei **Software**. Hier…
DSGVO 19: EuGH zu Schadenersatz nach Hacker-Angriff. Nutzen Sie TOMs, um sich freizubeweisen. Hier...
DSGVO 18: Wann ist eine **Datenpanne** zu **melden?** Hohe Strafen drohen! Hier...
DSGVO 17: **EU-USA Datenschutz-Abkommen:** Sind Google & Co nun wieder erlaubt? Hier...
DSGVO 16: USA wollen **TikTok** verbieten. Hier...
DSGVO 15: Praxisfragen zu **Kommunikationstools.** Hier...
DSGVO 14: Urteil droht **250.000 €** wegen **Google Fonts** an. Hier…

IDD 16: Alles in **GISA** eingetragen? **Konsequenzen?** Hier...
IDD 15: Seit 1.5. **Altersdiskriminierung** verboten. Oder doch nicht? Hier...
IDD 14: **Aufbewahrung Beratungs- und Verkaufsunterlagen:** Was sagen IDD / DSGVO dazu? Hier...
IDD 13: IDD **Aufsicht: Grobe Mängel aufgedeckt.** Welche Behörde kontrolliert bei Ihnen was? Hier...
IDD 12: Die neue Whistleblower-Richtlinie. Was müssen Sie tun? Hier...
IDD 11: Die **Behörde kommt.** Wie darauf **vorbereiten?** Hier...
IDD 10: Wann und wie darf man **Kunden und Interessenten noch kontaktieren?** TKG? Hier...

Praxis 4: **Erlagschein-Gebühr** schon wieder. Was sagt **OGH** dazu? Hier...
Praxis 3: Wie setzt man neue Whistleblowing-Vorgaben (Einrichtung Meldesystem, etc.) um? Hier...
Praxis 2: Aktuelle **EDV-Gefahren**, typische **Einfallstore** und Betrugsmaschen. Hier…
Praxis 1: Praxis von **Abmahnanwälten** kann teuer werden. Hier…

ALLE bisherigen IDD und DSGVO-Praxisbeiträge können Sie hier herunterladen…
Oder kostenlos mit "JA zu INFO" an g.wagner@b2b-projekte.at anfordern.

Hier folgt nun der Beitrag, den wir mit RA Mag. Stephan Novotny erarbeitet haben.

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Ausweiskopien: Wie damit in der Praxis umgehen?
Wie sichern Sie die personenbezogenen Daten und wie lange ist Speichern nötig / erlaubt?
Was ist spätestens seit Urteilen verboten?
Wir fassen für Sie das **Allerwichtigste** zum Themenkreis zusammen:

> Etwa: Wann muss ich ein Pass einholen? Was sagt dazu die FMA?
> Wie stellen Sie fest, ob ein vorgelegter ausländischer Pass echt ist?
> Wie speichere ich ihn sicher ab? Wie sende ich ihn weiter?
> Wie lange darf oder muss ich ihn speichern?

Und wir haben **interessante Urteile** gefunden, die zeigen, **wie man es nicht machen darf / soll:**
> **Topaktuell: UBER: 290 Mio. € Strafe** wegen Übermittlung von Daten in die USA
> Taxifahrer **fotografiert Führerschein** und versendet ihn über **WhatsApp**
> Urteil gegen **Bank** wegen **unberechtigter Verarbeitung der Passdaten**
Unten kommen Sie zum Beitrag, den wir mit RA Mag. Stephan Novotny erarbeitet haben:

Fakt ist, dass Sie in der **täglichen Praxis immer wieder Ausweiskopien erhalten** werden. 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) „bei Begründung einer Geschäftsbeziehung“ dazu verpflichtet sind, die Identität des Kunden festzustellen („know your customer“). Laut **Leitfaden der FMA** (den Sie hier herunterladen können: FMA-Leitfaden_FM-GWG_Sorgfaltspflichten_23.02.2022) hat dies durch einen amtlichen Lichtbildausweis zu erfolgen, worunter in Österreich Reisepässe, Führerscheine und Personalausweise fallen.

Tipp: Da die Kundenbasis immer internationaler wird: Wissen Sie, ob ein vorgelegter Ausweis echt ist? Wie Sie **ausländische Ausweise prüfen können**, erfahren Sie hier…

Ausweise sind „deshalb so heikel“, weil darauf sehr viele personenbezogenen Daten enthalten sind und **Kriminelle immer häufiger gestohlene Ausweiskopien nutzen,** um durch diesen Identitätsdiebstahl Straftaten in fremdem Namen zu begehen.
Kaum jemand von uns hat sich dabei Gedanken gemacht, was ein Betrüger mit dieser Kopie und den dort darauf befindlichen Daten (Name, Geburtsdatum) alles anstellen kann. Etwa damit auf diesem Namen ein **Konto einrichten und dann für Geldwäsche zu nutzen**. Oder im Internet einkaufen, Kredite aufnehmen, 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, um etwa damit ein Konto oder Sparbuch neu zu eröffnen, einen Leihwagen oder Wohnung zu mieten oder etwa einen Handy-Vertrag abzuschließen, etc.

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Andererseits soll dieser Praxistipp **Sie als Unternehmen, das solche Ausweiskopien von Kunden sammelt** (und für die Identitätsfeststellung nach dem Finanzmarkt Geldwäsche-Gesetz (kurz FM-GwG) sammeln muss, **„aufwecken" und das Gefahrenpotential erkennen lassen.** Denn hierbei handelt es sich um personenbezogene Daten, deren Sicherheit Sie aufgrund der DSGVO sicherstellen müssen. Wird Ihr PC 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.

Was soll man also tun, um die Gefahr zu verkleinern, wenn man seine Ausweiskopie oder sonstigen Identitätsnachweis versenden will/ muss? Dazu rät Watchlist Internet:

1. Kritisch hinterfragen, ob der Geschäftspartner zu Recht einen Ausweis verlangt
2. Ausweis „verändern", um Missbrauchsrisiko zu minimieren

Ad 1) Kritisch hinterfragen:
JA, einer seriösen Bank, Versicherung, etc. wird man auch künftig eine Ausweiskopie zusenden bzw. für die Online-Identifikation verwenden können. Doch wenn ein angebliches **Marktforschungsinstitut anbietet,** 100 Euro pro abgeschlossener Umfrage auszuzahlen, man aber dafür eine Ausweiskopie hochladen muss, dann sofort stoppen. Denn wozu braucht ein Marktforschungsinstitut meinen Pass?
Also immer nachdenken und besonders skeptisch werden, wenn jemand einen Ausweis von Ihnen oder Ihren Kunden haben möchte.

Ad 2) Ausweis „verändern", um Missbrauchsrisiko zu minimieren
„Watchlist Internet", eine der führenden Informationsplattformen zum Thema Internet-Betrug empfiehlt die eingescannte Kopie mit dem Hinweis „KOPIE" und dem Zusatz „nur für Kontoeröffnung bei Bank XY verwendbar" zu versehen. Wie Sie und Ihre Kunden dabei vorgehen sollten, haben wir hier genau beschrieben…
Zwar bekamen wir das letzte Mal, als wir diesen Tipp ausgesendet hatten, die Rückmeldung, dass **einige Versicherer so überarbeitete Kopien nicht akzeptieren würden.**

Aber wir betonen hier nochmals, Watchlist Internet ist nicht irgendein Verein, sondern ein Projekt des Internet Ombudsmann, 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. **Also sollten auch konservative 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 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….

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Und in diesem Zusammenhang könnte man **unwillige Versicherer** auf eine sehr gute Übersicht verweisen, die der **Landesbeauftragte für den Datenschutz in Nordrhein-Westfalen** erstellt hat. Dort werden z.B. sehr übersichtlich die Gründe aufgelistet, wann welches Unternehmen Ausweiskopien für welche Zwecke verwenden darf.
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…

Um **das Problembewusstsein im Zusammenhang mit Ausweisen noch zu steigern,** haben wir folgende **interessante Urteile für Sie recherchiert**.

1. **Topaktuell: UBER: 290 Mio. € Strafe** wegen Übermittlung von Daten in die USA
2. Taxifahrer **fotografiert Führerschein** und versendet ihn über **WhatsApp**
3. Urteil gegen **Bank** wegen **unberechtigter Verarbeitung der Passdaten**

Wir analysieren die Urteile, weil wir daraus sehr gut erkennen können, was im Zusammenhang mit Ausweisen erlaubt ist und keineswegs gemacht werden darf.

Ad A) UBER muss 290 Mio. € Strafe zahlen wegen Übermittlung von Daten in die USA
Knapp vor dem Sommer berichteten einige Medien (u.a. Der Standard, NTV), dass die **holländische Datenschutzbehörde** diese Strafe verhängte, nachdem sich 170 Uber-Fahrer darüber beschwerten, dass zahlreiche personenbezogene Daten (u.a. Fotos, Lohnunterlagen und Ausweise) **in die USA übertragen wurden.**
Auch sollen sensible Daten wie begangene Straftaten oder zur Gesundheit übertragen worden sein.
Dies sei ein **schwerer Verstoß** gegen die EU-Datenschutzgrundverordnung, **so die Behörde.**

Das US-Unternehmen kündigte Berufung an und zeigt sich zuversichtlich, dass im Berufungsverfahren „der gesunde Menschenverstand obsiegen werde", wie NTV zitiert.
Der Chef der niederländischen Datenschutzbehörde, Aleid Wolfsen, erklärte im NTV," in Europa verlange die DSGVO von Unternehmen und Regierungen, persönliche Daten mit Vorsicht zu behandeln". Dies sei „traurigerweise außerhalb Europas nicht selbstverständlich".

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Und weiter: „**Denken Sie an Regierungen, die Daten in großem Stil anzapfen können“** (Anmerkung: Hier sind die USA ganz besonders gemeint, wo Geheimdienste, etc. ohne richterliche Genehmigung alle Daten von Europäern von US-Firmen, wie Google, Facebook und Co. verlangen und somit mitlesen dürfen). „Deshalb sind Unternehmen zu zusätzlichen Maßnahmen verpflichtet, wenn sie die Daten von Europäern außerhalb Europas speichern.“

Daher Tipp: Dieses Urteil zeigt wieder einmal ganz deutlich: Wenn Sie personenbezogene Daten speichern und sonst wie verarbeiten (müssen), achten Sie darauf, dass die **Daten Europa nicht verlassen.** Weil der momentane Zustand – EU-Kommission schließt ein politisches Abkommen mit den USA (Tenor: „Wir sagen mal, die Daten von Europäern sind auch in den USA geschützt“) und hofft darauf, dass der **EU-Gerichtshof** nicht wieder diesen „**Zustand“ als gesetzeswidrig einstuft.**

Ad B) Taxifahrer fotografiert Führerschein und versendet ihn über WhatsApp
Bereits im Jahr 2020 berichteten die Datenschutz-Kollegen von MeineBerater.at über einen „kuriosen“ Fall, der vor der österreichischen Datenschutzbehörde landete. Worum ging es: Ein Fahrgast verfügte nicht über genug Bargeld, um seine Taxi-Fahrt zu bezahlen. **Daraufhin fertigte der Taxifahrer ohne Einwilligung Fotos von Führerschein sowie Bankomatkarte des Fahrgastes an** und leitete diese über **WhatsApp** an eine dritte Person weiter.
Durch diese Handlung **verletzte der Taxifahrer massiv das Recht auf Geheimhaltung** der betroffenen Person. Weder die durchgeführte Datenerhebung, also das Fotografieren, noch das Weiterleiten war rechtmäßig, so die Datenschutzbehörde.
Der Taxifahrer bzw. das Unternehmen, bei dem er beschäftigt war, konnte sich bei dieser Handlung rechtlich weder auf eine **Einwilligung** noch auf den „oft verwendeten Rechtfertigungsgrund“ des **überwiegenden berechtigten Interesses** des Taxiunternehmens stützen.

UND: Erschwerend hinzu kommt noch die **Verwendung von WhatsApp,** von der wir immer wieder **dringend abraten.** WhatsApp hat im beruflichen Umfeld nichts verloren, verbannen Sie es daher von firmeneigenen Endgeräten. Verwendet man WhatsApp, werden Daten automatisch in die USA weitergeleitet (mit Facebook geteilt etc.) – und dafür wird kein Kunde freiwillig seine Einwilligung erteilen.

Was lernen wir daraus – außer, dass WhatsApp nichts auf beruflichen Geräten zu suchen hat? Dieser Fall zeigt ganz deutlich, dass eine unbedachte Handlung eines einzelnen Mitarbeiters auf das Unternehmen zurückfällt und dieses dann die datenschutzrechtlichen Folgen zu tragen hat.
Daher Tipp: Es reicht nicht, wenn Sie eine Firmenrichtlinie für die DSGVO haben, sondern regelmäßiges **Schulen aller Mitarbeiter ist unbedingt wichtig.** Denken Sie nur daran, was ein falscher Klick auf einen Link in einem Mail an Folgen auslösen kann…

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Ad C) Urteil gegen Bank wegen unberechtigter Verarbeitung der Passdaten
Sich einfach auf das FM-GWG zu berufen und einen Pass zu verlangen ist auch nicht die Lösung: Ein **Urteil der Österreichischen Datenschutzbehörde** (DSB) aus dem Jahre 2020 – das meiner Ansicht viel zu wenig bekannt ist – zeigt deutlich auf, wann eine Speicherung eines Lichtbildausweises durch die Bank **nicht erlaubt ist.**

Worum ging es? Der Beschwerdeführer wollte in der Bank 100 € in türkische Lira tauschen. Der Bankmitarbeiter verlangte einen Ausweis, andernfalls man das Wechseln nicht durchführe. Der Mann weigerte sich vorerst, legt dann doch den Führerschein vor. Dieser wurde kopiert und gespeichert. Eine Beschwerde bei der DSB war die Folge.
Die Bank verteidigte sich mit Obliegenheiten aufgrund des **FM-GwG, dem Finanzmarkt-Geldwäschegesetz.** Sie hätte bei bloßem Verdacht hinsichtlich Geldwäsche oder Terrorismusfinanzierung Sorgfaltsmaßnahmen anzuwenden und im Zweifel Identitätsdokumente zu verlangen. Seine Weigerung – Anmerkung: den Pass vorzulegen – sei als auffälliges Kundenverhalten interpretiert worden. Darüber hinaus hätte der Beschwerdeführer bei einer höheren Bundesbehörde gearbeitet habe, daher sei er eine PEP, eine politisch exponierte Person und daher eine Prüfung durchzuführen gewesen.

Gegen diesen Bescheid hat die Beschwerdegegnerin Beschwerde an das Bundesverwaltungsgericht (BVwG) erhoben. Der Bescheid ist aber nach einer mündlichen Verhandlung **seit 13. 7. 2022 rechtskräftig** geworden.
Was lernen wir daraus? Nur weil sich ein Unternehmen auf Geldwäsche, PEP oder sonstigem beruft, muss dennoch die Verarbeitung von personenbezogenen Daten trotzdem nicht erlaubt sein. Daher seien Sie vorsichtig und prüfen Sie, ob die Rechtsvorschriften dies erlauben.

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 Mag. Novotny

ALLE bisherigen IDD und DSGVO-Praxisbeiträge können Sie hier herunterladen…
Oder kostenlos mit "JA zu INFO" an g.wagner@b2b-projekte.at anfordern.

Für Rückfragen:

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

Foto: Stephan Huger