Mag. Günter Wagner
B2B Projekte
für Finanz- und Versicherungsbranche

DSGVO: Was wurde gerne bestraft?
Das "kleine 1x1 des Datenschutzes" zum Nacharbeiten!

Seit 25.5.2018 gibt es keine Ausrede mehr:
Mit **existenzbedrohenden Strafen** von bis zu 20 Mio. Euro oder 4 % des Konzern-Umsatzes versucht die EU auch die schwarzen Schafe an die Leine zu nehmen. Datenschutz hat nun oberste Priorität. Wir müssen also die **Sicherheit der Daten** (egal ob Kunden, Partner, Mitarbeiter) **garantieren.** Umfangreiche Vorkehrungsmaßnahmen waren und regelmäßige **Kontrollen sind nötig.**

Daher geben wir einen kleinen **Rückblick auf "3-Jahre-DSGVO",** berichten darüber, was **gerne bestraft** wurde und liefern eine **kleine Checkliste "Das kleine 1x1" zum Prüfen, ob das Wichtigste** der DSGVO in Ihrem Unternehmen **erfüllt wurde** (falls Ja, bitte **prüfen, ob alles noch aktuell ist).**

Achtung: Neben den **hohen Strafen und möglichem Image-Verlust** droht künftig eine **neue Gefahr** bei Verletzungen der DSGVO**, nämlich Schadenersatzklagen (das deutsche Verfassungsgericht hat dazu eine "positive" Entscheidung getroffen).**

Um Ihr Problembewusstsein noch zu steigern, sehen wir uns zu Beginn an, **welche Vergehen** von den unterschiedlichen **Datenschutzbehörden "gerne" bestraft wurden.** Die Strafen können sich von einigen Tausend Euro bis hin zu **hunderttausende Euros betragen! Bitte checken Sie,** ob Sie hier alles optimal erfüllen.

Die **bisher erschienen Praxis-Beiträge zur DSGVO von Mag. Novotny** beschäftigten sich mit folgenden Themen:

DSGVO 1: DSB-Urteil zur **maximalen Speicherdauer:** Wie Freibeweisen ohne Unterlagen? Hier weiterlesen...
DSGVO 2: **TOMs:** Was lernen wir aus **Megastrafe?** Hier weiterlesen...
DSGVO 3: **Ausweiskopien:** Nie unverändert speichern oder versenden! Hier weiterlesen...
DSGVO 4: **Millionenstrafe wegen telefonischer Auskunft!** Was lief schief? Wie besser machen? Hier weiterlesen...
DSGVO 5: Was fordert **EuGH zur Einwilling bei Cookie**-Nutzung auf **Webseite?** Abmahnungen vermeiden! Hier weiterlesen...
DSGVO 6: Rückblick auf Datenschutz-Urteile 2020. Hier weiterlesen…
DSGVO 7: Teil2: Wann und wie darf man **Kunden und Interessenten** seit Wirksamkeit der DSGVO **noch kontaktieren?** Hier weiterlesen...
DSGVO 8: **Datenpanne: Zu viele Mail-Adressen** unter AN oder CC: Was ist zu tun? Hier weiterlesen...
DSGVO 9: **WhatsApp, Facebook aber auch berufliche soziale Medien: Hände weg.** Hier weiterlesen…

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

Mag. Günter Wagner
B2B Projekte
für Finanz- und Versicherungsbranche

DSGVO: Was wurde gerne bestraft?
Das "kleine 1x1 des Datenschutzes" zum Nacharbeiten!

A) Auswahl einiger wichtiger Urteile, zum Besser werden!

Die diversen Datenschutzbehörden trafen Entscheidungen, die auch für uns in Österreich relevant und zu befolgen sind, weil die DSGVO eine Europäische Verordnung ist, die europaweit gleich anzuwenden ist. Hier zum Erinnern eine kurze Auswahl von Entscheidungen, über die wir in den BAV-Newslettern bereits berichtet haben.

+) **50-Millionen**-Euro-DSGVO-Strafe gegen Google bestätigt
Google kam sogar noch mit einem blauen Auge davon, denn die Höchststrafen können laut DSGVO bis zu EUR 20 Mio. pro Unternehmen oder sogar 4% des Umsatzes bei Konzernen betragen (bei Google hätte das also weit mehr als EUR 50 Mio. ausmachen können!).

+) **9,55 Mio. wegen telefonischer Auskunft an Unberechtigte**
Beim deutschen Telekommunikationsunternehmen „1&1“ war es offensichtlich üblich, dass man Anrufern, wenn sie Namen und Geburtsdatum eines Kunden nennen konnten, Auskünfte erteilte, die „weitreichende Informationen zu weiteren personenbezogenen Kundendaten“ enthalten konnten. Erstaunlich ist, dass so eine Mega-Strafe verhängt wurde, **trotzdem** die Behörde anerkannte, dass das Unternehmen im Verfahren **kooperativ** gewesen sei. Aber: „Das Unternehmen hatte keine hinreichenden technisch-organisatorischen Maßnahmen ergriffen, um zu verhindern, dass Unberechtigte bei der telefonischen Kundenbetreuung Auskünfte zu Kundendaten erhalten können.“

+) 400.000 wegen Verfehlungen bei den TOMs
Ein portugiesisches Krankenhaus wurde zu dieser „geringen“ Strafe verurteilt, weil man sich kooperativ gegenüber der Behörde zeigte und aktiv an der Behebung der Mängel mitgearbeitet wurde. Die **Verfehlungen betrafen die TOMs,** also die technischen und organisatorischen Maßnahmen, die im Zuge der DSGVO-Umsetzung realisiert werden mussten. Konkret wurden beim Ausscheiden von Mitarbeitern **nicht sofort deren Zugriffsmöglichkeiten sofort deaktiviert.**

+) Verheimlichtes Datenleck wird teuer
Der Essenslieferant Foodora (gehört in Österreich Mjam) **meldete nicht, dass man gehackt** wurde. Als Jahre später die Daten von 727.000 Kunden im Internet zum Kauf angeboten wurden, drohen nun der Mutter eine Strafe von 4% des weltweiten jährlichen Umsatzes. Daher bei Daten-Hoppalas und Hacker-Angriffen sofort prüfen, ob eine Meldung nötig ist und dies binnen 72 Stunden (egal ob Wochenende oder Feiertag) der Datenschutzbehörde melden.

+) **25.000-Euro**-Strafe, **weil Datenschutzbeauftragter fehlte**
Ein spanischer Lieferdienst wurde – nach der Beschwerde zweier Betroffener – verurteilt. Aufgrund der zahlreichen und umfangreichen Datenverarbeitungen hätte man einen Datenschutzbeauftragten bestellen müssen, hat dies aber nicht getan.

+) **EUR 5.000**, **weil kein Auftragsverarbeiter-Vertrag** mit Dienstleister bestand. Daher: Prüfen Sie, ob Sie von allen Ihren Dienstleistern einen AVV 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

+) **EUR 5.000 Schadenersatz** wegen **verspäteter Auskunftserteilung**
Das Arbeitsgerichts Düsseldorf sprach einem ehemaligen Angestellten wegen einer zu späten und unvollständigen Auskunftsbeantwortung zu (Verletzung der Auskunftspflicht).

+) **Datenpanne beim E-Mail-Versand:** Zu viele Mail-Adressen unter AN: statt BCC:
E-Mail-Adressen sind personenbezogene Daten und dürfen daher Dritten – wie hier in dieser Massenaussendung – nicht offen zugängig gemacht werden. Passen Sie daher auch bei der automatische Namensergänzung von Outlook auf, dass aus den Anfangsbuchstaben eines Namens nicht ein falscher Namen aus Ihren Kontakten gewählt und das Mail an einen unbeteiligten Dritten gesendet wird. Beides ist eine Datenpanne.

B) Das "kleine 1x1 des Datenschutz": Haben Sie alles erledigt? Adaptionen nötig?

Wir haben nun anlässlich des 3-Jahrestags der DSGVO gemeinsam mit Mag. Novotny ein **„Kleines 1x1“ mit dem Allerdringlichsten** erstellt, damit Sie auf einem Blick erkennen können, ob Sie bereits alles erledigt haben.

Denn: Solche Jahrestage wie eben 3-Jahre-seit-Inkrafttreten sollten **ein Anlass** sein, um sich wieder von Grund auf mit der DSGVO zu beschäftigen und **alles zu kontrollieren:**
Etwa: **Stimmen die Formulare noch** (etwa das Verfahrensverzeichnis), die man damals ausgefüllt hat oder hat man z.B. neue Partner (z.B. eine neue Druckerei?), neue Datenanwendungen (etwa neue Software?).
Verwendet man eine **Software**, die damals dank Privacy Shield-Abkommens zwischen EU und USA legal war. Aber nun nach EuGH-Urteil **nicht mehr legal** ist? Was muss man nun eigentlich tun?
Hat man die **korrekte Adresse der Datenschutzbehörde** (hat sich geändert!), um im Notfall eine Datenpanne binnen 72 Stunden melden zu können? Usw. usf.

Wir nehmen den Jahrestag zum Anlass, um Sie auf die wichtigsten Punkte der DSGVO hinzuweisen und auf die wichtigsten Urteile und Strafen hinzuweisen.

Warum soll man das alles einhalten?

Gründe hierfür können die angedrohten Strafen, die Möglichkeit dass man von Konkurrenten bei der DS-Behörde angeschwärzt wird, Image- und Reputations-Verlust oder seit kurzem auch Schadenersatzforderungen und Schmerzensgeld sein.
Diese neue Gefahr der Schadenersatzforderungen und Schadenersatz wurde durch erste Urteile bzw. **Entscheidungen des deutschen Bundesverfassungsgerichts** (BVerfG vom 14. Januar 2021) noch größer!

Daher bitte die DSGVO nicht aus den Augen lassen. Aber was braucht man auf jeden Fall?

Das „Kleine 1x1 des Datenschutzes“

Auch 3-Jahre nach Wirksamwerden der DSGVO ist noch vieles unklar, noch nicht ausjudiziert. Was auch daran liegt, dass große Datenkraken gegen erste Strafen in Berufung gingen und noch kein Urteil dazu vorliegt.

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

Aber es gibt einige Punkte, die unbedingt erfüllt sein sollten. Der deutsche Datenschutz-Experte Sebastian Kraska sprach im Computer-Magazin com! professionell unlängst vom „Kleinen 1x1 des Datenschutzes“. Und weiter „Unternehmen **können nicht auf das Verständnis der Aufsichtsbehörden hoffen, wenn** sie nicht zumindest diese Basisthemen abdecken“, so Kraska. Zum Nachlesen hier klicken…

Wir haben uns von diesem „1x1“ inspirieren lassen, seine Auflistung der „wichtigsten Punkte“ **für Österreich adaptiert und um eigene Punkte ergänzt.** Aber eine Garantie, dass damit die DSGVO in jedem Fall korrekt erfüllt ist, wenn das abgehakt wurde, gibt es natürlich nicht. Aber ein guter Start wäre es allemal…

Folgende Punkte sollten Unternehmen laut Kraska und Mag. Novotny **auf jeden Fall sofort umsetzen,** wenn sie es nicht schon längst getan haben:

1. **Datenschutzerklärung** erstellen und alles dokumentieren
   Dank DSGVO müssen Sie nachweisen können, dass Sie die notwendigen organisatorischen Maßnahmen gesetzt haben und sich an die Vorgaben halten.

2. **Verarbeitungsverzeichnis** erstellen und aktuell halten
   Darin sind alle Tätigkeiten zu erfassen, bei denen eine Datenverarbeitung stattfindet. Denken Sie auch an Software, Webseite, usw. (da hier auch Daten erfasst werden).

3. **Auftragsverarbeiter-Verträge** abschließen
   Lagern Sie Datenverarbeitung an Dritte aus, weil etwa ein Mailing an Ihre Kunden durch eine Druckerei erfolgt, dann müssen Sie mit diesem Auftragsverarbeiter eine Vereinbarung treffen, um ihn zur Einhaltung der DSGVO zu verpflichten.

4. **Angemessenes Schutzniveau** sicherstellen
   Die DSGVO gilt für jedes Unternehmen, egal ob Konzern oder EPU. Aber es gilt das Prinzip der Verhältnismäßigkeit, d.h. an den Kleinen werden weniger Anforderungen gestellt, als an den Konzern. Welche technisch organisatorische Maßnahmen Sie setzen, legen Sie in den TOMs fest.

5. **Informations-Pflichten und Betroffenen-Rechte erfüllen**
   Also etwa auf der Webseite die Datenschutzerklärung veröffentlichen. Die Cookie-Banner DSGVO-konform gestalten und korrekt darüber informieren. Bei der Erhebung personenbezogener Daten sind die Betroffenen unter anderem über Art, Umfang, Dauer und Zweck der Verarbeitung und deren Rechte zu informieren.

6. **Datenschutzbeauftragter /-koordinator**
   Brauchen Sie einen DS-Beauftragten oder reicht ein DS-Koordinator?
   Diese Entscheidung ist zu treffen und die Person ist namentlich im Verfahrensverzeichnis und mit Kontaktdaten auch öffentlich (z.B. via Webseite) bekannt zu geben.

7. **Mitarbeiter schulen und zum Datenschutz verpflichten**
   Eine falsche Auskunft am Telefon oder Fehlhandlung kann teuer werden und sollte daher durch regelmäßige Schulungen vermieden werden.

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

Daher gilt es die **Mitarbeiter zum Datenschutz,** also Geheimhaltung, vertraglich zu verpflichten.

8. **Datenschutz-Folgenabschätzung**
   Diese Folgenabschätzung beschreibt **die Verarbeitungsvorgänge** (siehe Punkt 2), deren Notwendigkeit, die Verhältnismäßigkeit, damit verbundene Risiken und geplante Abhilfemaßnahmen.

9. **Betroffenenrechte einhalten**
   Durch die DSGVO haben „Betroffene“ (gemeint sind Personen/Firmen, deren Daten Sie verarbeiten) Rechte etwa auf Auskunft, Löschung, Bereinigung oder Sperrung. Ignorieren dieser Rechte oder Fehler beim Tun können sehr teuer werden. Es gilt organisatorisch Prozesse zu definieren (was passiert bei Anfragen, wer darf antworten, etc.).

10. **Datenverlust – Databreach – binnen 72 Stunden melden**
    Gehen personenbezogene Daten verloren oder werden gestohlen, ist dies der DS-Behörde binnen 72 Stunden zu melden. Frist läuft, egal ebenfalls unverzüglich- zu informieren.

Quellen: computerwelt, Computer-Magazin com! professionell

Alle bisherigen IDD und DSGVO-Praxisbeiträge können Sie **hier herunterladen...**
Den aktuellen Beitrag können Sie als PDF anfordern. Dazu einfach ein E-mail an g.wagner@b2b-projekte.at mit Betreff "Ja zu Infos".

beste Grüße von Mag. Stephan Novotny und Günter Wagner

Für Rückfragen:

MAG. STEPHAN M. NOVOTNY

Rechtsanwalt-Attorney at Law / Akademischer Versicherungskaufmann / Collaborative Law Lawyer
Weihburggasse 4/2/26, A-1010 Wien
Tel: +43 / 1 / 512 93 37,
Fax +43 / 1 / 512 93 37 93, Mob. +43 / 664 / 143 29 11
kanzlei@ra-novotny.at www.ra-novotny.at