Secur-Data Betriebsberatungs-Ges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at
Offenlegung gem. MedienG: www.secur-data.at/impressum

DSG-Info-Service

November 2020 Ausgabe Nr. 96

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Das Jahr 2020 wird sicherlich als eines der turbulentesten Jahre in die Geschichte eingehen. Direkte negative Auswirkungen auf die Wirtschaft zeichnen sich deutlich ab und eine Vielzahl von Unternehmen wird auf die Probe gestellt. Die Corona-Krise hat Unternehmen aber auch zu vielen Neuerungen, Anpassungen und vor allem zur digitalen Transformation förmlich gezwungen. Diese zusätzliche Digitalisierung ist als Chance für die Zukunft zu sehen, die verbundenen Herausforderungen werden aber wahrscheinlich im Folgejahr zunehmen.

Auch die Firma Secur-Data hat eine Transformation vorgenommen: Ab sofort stehen wir Ihnen mit unserem neuen Webauftritt zur Verfügung. Neben einer äußerlichen Auffrischung präsentieren wir Ihnen verschiedene neue Produkte für Ihr Unternehmen.

Wie gewohnt, möchten wir Sie mit dieser DSG-Info über den aktuellen Stand der Judikatur und Gesetzgebung informieren und Sie auch weiterhin über die neuesten Themen auf dem Laufenden halten.

1. Zweites Strafverfahren der Post

Wie aus dem Datenschutzbericht 2019 bekannt geworden ist, setzt die Datenschutzbehörde aktuell ca. 1,5 Mitarbeiter allein für die Bearbeitung von Beschwerdeverfahren gegen die Post ein. In dem bereits bekannten Strafverfahren, in dem das Rekordbußgeld iHv EUR 18 Mio. wegen der Verarbeitung von Parteiaffinitäten[1] im Rahmen des Direktmarketings- und Adressverlagsgewerbes verhängt wurde, hat auch das Bundesverwaltungsgericht[2] die Entscheidung der Datenschutzbehörde bestätigt.

Nun ist auch bekanntgeworden, dass ein zweites Verfahren gegen die Post anhängig ist.

In diesem neuen Verfahren geht es ebenfalls um die Verarbeitung sog. sensibler Daten iSd Art. 9 DSGVO, und zwar der Zuordnung von Personen bzw. Haushalten zu „Sinus-Geo Milieus“. Verbraucher werden dabei in soziodemografische Zielgruppen eingeteilt, die dann zu gezielten Marketing-Segmenten weiterverarbeitet und vermarktet werden.

[1] DSB-D213.747/0002-DSB/2019, Bescheid vom 11.02.2019: „Post-Bescheid“.

[2] BVwG W258 2217446-1/15E vom 20.08.2020.

Dabei gibt es Sinus-Milieus wie „Bürgerliche Mitte“, „Prekäres Milieu“, „Hedonisten“ oder auch „Young Performer“, die wiederum unterschiedlichen Marketingklassifikationen unterliegen. Die Datenschutzbehörde sah in der Einteilung von Personen in solche Zielgruppen einen Verstoß gegen die Verarbeitung von Daten zu weltanschaulichen Überzeugungen (Art. 9 DSGVO), die ohne ausdrückliche Einwilligung der Betroffenen nicht zu Marketingzwecken verarbeitet werden dürfen.

Die Inanspruchnahme solcher Marketingklassifikationen kann daher einen Verstoß gegen die Grundsätze der Datenverarbeitung darstellen, wenn keine ausreichende Rechtsgrundlage vorliegt. Das Zukaufen von Daten aus Adressverlagen sollte immer unter Berücksichtigung der rechtmäßigen Datenerhebung und Richtigkeit der Daten erfolgen.

Das Erkenntnis der Datenschutzbehörde ist noch nicht veröffentlicht und damit nicht rechtskräftig. Eine Entscheidung durch das Bundesverwaltungsgericht und in weiterer Folge den Verwaltungsgerichtshof bleibt daher offen.

2. Schadenersatz im Datenschutz – Ein Überblick

Das Thema Schadenersatz für rechtswidrige Datenverarbeitung wurde in Österreich bis dato noch nicht ausgiebig durch die Gerichte thematisiert. Zu unterscheiden sind dabei der materielle Schadenersatz für den Ersatz von Vermögensschäden und der immaterielle Schadenersatz für die Erstattung von Schäden, die beispielsweise in der Gefühlswelt, der Freiheit oder Ehre eingetreten sind.

Darüber hinaus gibt es in Österreich die Möglichkeit, wegen einer erheblichen Verletzung der Privatsphäre iSd § 1328a Abs. 1 ABGB zur Zahlung eines Schadenersatzes[3] verpflichtet zu werden, was subsidiär zur DSGVO zur Anwendung kommt.

In einem erstinstanzlichen Verfahren wurde die Post AG zur Zahlung eines immateriellen Schadenersatzes iHv EUR 800 für die unrechtmäßige Datenverarbeitung der vermeintlichen Parteiaffinität eines Betroffenen verurteilt. Das OLG Innsbruck[4] hat diese Entscheidung wegen Beweismängeln zur konkreten Beeinträchtigung des Betroffenen jedoch aufgehoben. Das OLG sah die Erheblichkeitsschwelle eines ersatzwürdigen Gefühlsschadens nicht nachgewiesen.

Das führt zum Ergebnis, dass ein immaterieller Schaden über das reine Gefühl des „Gestörtseins“ hinaus entstanden sein muss. Das Vorliegen einer „tatsächliche[n] Beeinträchtigung in der Gefühlswelt“, die über reinen Unmut hinausgeht, beweisen zu müssen, erschwert zwar Betroffenen, ihre Ansprüche geltend zu machen. Angesichts der zahlreichen Möglichkeiten, gegen die DSGVO zu verstoßen, ohne dabei Betroffenen einen materiellen oder immateriellen Schaden zu verursachen, erscheint jedoch diese Erheblichkeitsschwelle gerechtfertigt, um Bagatellverfahren zu verhindern.

Denn der Verstoß gegen die Regelungen der DSGVO führt nicht automatisch zu einem „Rechtswidrigkeitsschaden“, sondern knüpft Schadenersatz an die Voraussetzung des tatsächlich „erlittenen Schadens“ (vgl. ErwG 146). Das OLG stellte im konkreten Fall fest, dass der Verstoß gegen die DSGVO nicht mit dem Schaden gleichzusetzen ist, sondern vom Kläger konkret „darzulegen [ist], welcher erhebliche

[3] OGH 22.1.2020, 9 Ob A 120/19s – GPS-Ortung für Privatfahrten.

[4] OLG Innsbruck - 13.02.2020, 1 R 182/19b

Nachteil in seinem Gefühlsleben durch die behaupteten Verstöße der DSGVO entstanden ist und welche Persönlichkeitsbeeinträchtigung daraus resultiert“[5].

Für eine erfolgreiche Schadenersatzklage ist laut OLG Innsbruck daher eine nachweisbare Persönlichkeitsbeeinträchtigung aufgrund von Verstößen gegen die DSGVO notwendig, die anhand einer „durchschnittlich im Datenschutz sensibilisierte[n] Maßfigur“ beurteilt wird. Diese „objektiv-subjektive“ Herangehensweise wird folglich zu einer Einzelfalljudikatur führen, deren Klärung dem OGH und EuGH obliegen wird.

In Deutschland ist es ebenfalls noch zu keinem *rechtskräftigen* Ersatz des immateriellen Schadens aufgrund eines Verstoßes gegen die DSGVO gekommen. Das Arbeitsgericht Düsseldorf hat jedoch in seinem Erkenntnis vom 5. März 2020, 9 Ca 6557/18 einer betroffenen Person, die von ihrem Arbeitgeber verspätet eine unvollständige Auskunft über die Datenverarbeitung erhalten hat, einen Schadenersatz von EUR 5.000 zugesprochen.

Die Begründung lag in der aus ErwG 75 abgeleiteten Kontrollmöglichkeit der Datenverarbeitung, deren Verlust zu einem immateriellen Schaden führen kann. Die Ungewissheit über die unvollständige und verspätete Auskunft iSd Art. 12 iVm Art. 15 DSGVO sieht das Gericht als einen Verstoß gegen die DSGVO und damit einen schadenersatzfähigen Anspruch begründet. Nachdem diese Entscheidung nicht rechtskräftig ist, wird das Verfahren vor dem Landesarbeitsgericht NRW (GZ: 14 Sa 294/20) weiterverhandelt.

Ein anderer Fall ist vom Landgericht Darmstadt[6] bekannt. Dort wurde einem Bewerber ein Schadenersatz iHv EUR 1.000 zugesprochen, nachdem Daten aus seinem Bewerbungsverfahren u.a. zu Gehaltsvorstellung und Eintrittsmöglichkeiten an einen Dritten übermittelt wurden. Die Daten wurden über einen Chat in einem Social Network an die falsche Person übermittelt, trotz Kenntnis über den Data Breach wurde keine Verständigung des Betroffenen vorgenommen. Das Gericht sprach *nicht rechtskräftig* einen Schadenersatz von „nur“ EUR 1.000 zu, da die Offenlegung an den Dritten keine weiteren beruflichen oder persönlichen Beeinträchtigungen zur Folge hatte. Was darauf schließen lässt, dass es in einem anders gelagerten Fall durchaus um höhere Summen gehen könnte.

Diese Entscheidungen zeigen, dass eine subjektive Beeinträchtigung aus Verstößen gegen die DSGVO möglich ist und damit den Ersatz von immateriellen Schäden eröffnet. Die Höhe des Anspruches ist dabei wohl zunächst noch eine reine Einzelfallentscheidung.

3. Rekordbußgeld gegen Servicecenter von H&M

Die Hamburger Datenschutzbehörde hat gegen ein Servicecenter der H&M-Gruppe ein Rekordbußgeld iHv EUR 35 Mio. ausgesprochen. Hintergrund waren systematische Datenschutzverstöße in den Bereichen des Mitarbeiterdatenschutzes und der Datensicherheit.

Informationen über Mitarbeiter wurden in internen Datenbanken systematisch verarbeitet und bewertet, insbesondere private Lebensumstände, Krankheiten, Beziehungsstatus sowie Urlaubs- und Krankheitstage wurden gespeichert.

Diese Informationen nutzten Führungskräfte für die Auswertung der Arbeitsleistung und die Bewertung der Mitarbeiterperformance im Unternehmen. Der Fall geriet im Jahr 2019 an die Öffentlichkeit, als die Datenbank, die 60 GB

[5] OLG Innsbruck - 13.02.2020, 1 R 182/19b, RZ 9.

[6] LG Darmstadt, 13 O 244/19, Urteil vom 26.05.2020.

Material umfasste, nach einem Konfigurationsfehler unternehmensweit verfügbar war.

Die Höhe des Bußgelds begründete sich aus der Intensität der Datenschutzverletzung und der Menge an Betroffenen, deren Privatsphäre systematisch verletzt wurde. Das Unternehmen gab an, bereits Abhilfemaßnahmen getroffen zu haben, die unter anderem ein neues Datenschutzkonzept, einen Whistleblower-Schutz sowie ein „konsistentes Auskunfts-Konzept" beinhalten. Darüber hinaus wurde den Betroffenen finanzielle Entschädigung angeboten.

Das Bußgeld zeigt, wie wichtig der richtige Umgang mit Mitarbeiterdaten im Unternehmen ist. Dabei kommt es darauf an, dass die Mittel, die für Performance-Management und Mitarbeiterbewertung gewählt werden, nicht in die Privatsphäre der Mitarbeiter eingreifen, sondern in Einklang mit dem Grundsatz der Verhältnismäßigkeit stehen.

4. Strafe für AOK Baden-Württemberg wegen unzulässiger Werbung

Die Deutsche Krankenkasse „AOK Baden-Württemberg" hat über mehrere Jahre hinweg im Rahmen von Gewinnspielen und Ausschreibungen personenbezogene Daten von Teilnehmern erhoben. Dazu gehörten nicht nur die Kontaktdaten, sondern auch Informationen über die jeweilige Kassenzugehörigkeit, die die AOK für Werbung nutzen wollte.

Hierzu wurden jedoch über 500 Teilnehmer ohne entsprechende Einwilligung angeschrieben und deren Daten für Werbezwecke verwendet. Die AOK betonte zwar, dass es interne Richtlinien und Schulungen zum Datenschutz gegeben habe, konnte allerdings keine Einwilligung der angeschriebenen Betroffenen vorwiesen. Nach Bekanntwerden des Vorfalls wurden die Aktivitäten zwar eingestellt, dennoch wurde ein Bußgeld in Höhe von EUR 1,2 Mio. angesichts mangelhafter technischer und organisatorischer Sicherheitsmaßnahmen verhängt, die dazu geführt haben, dass die Daten ohne Einwilligung verarbeitet wurden.

Fazit: Verantwortliche müssen immer in der Lage sein, die Herkunft der personenbezogenen Daten sowie deren rechtmäßige Erhebung und Verarbeitung nachweisen zu können. Ein angemessenes Datensicherheitsniveau umfasst auch die Trennung von Bestandskundendaten und Daten, die zur Bewerbung von Waren und Dienstleistung dienen.

5. Millionenstrafe für British Airways in UK reduziert

Die angekündigte Strafe von EUR 204 Mio., ca. 1,5 % des Jahresumsatzes, gegen die Airline British Airways ist pandemiebedingt auf 20 Mio. Pfund gekürzt worden. Wie bereits in DSG-Info Nr. 92 geschildert, waren es gravierende Sicherheitslücken auf der Buchungsplattform der Airline, die im Jahr 2018 zu einem Data Breach enormen Ausmaßes geführt haben. Über den Zeitraum von zwei Monaten wurden unbemerkt Daten von über 400.000 Betroffenen über eine Phishing-Plattform abgegriffen und missbräuchlich verwendet.

Damit zeigt sich erneut, wie wichtig die getroffenen Datensicherheitsmaßnahmen im Unternehmen sind. Gerade bei einer großen Anzahl an Betroffenen, insbesondere dort, wo es zu Zahlungsabwicklungen kommen kann, ist besonders darauf zu achten, dass angemessene Sicherheitsmaßnahmen vorliegen.

6. LAG Niedersachen: Kein Auskunftsanspruch bei selbst verfassten E-Mails

Das Landesarbeitsgericht Hannover geht mit einer Entscheidung[7] zu Art. 15 DSGVO einen neuen Weg. Demnach sei der Anspruch auf Auskunft und Kopie sämtlicher durch einen ehemaligen Arbeitnehmer verfassten E-Mails nicht vom Anwendungsbereich des Art. 15 DSGVO umfasst, da die Inhalte der Nachrichten dem Betroffenen bereits bekannt seien. Das Betroffenenbegehren wurde in einem arbeitsrechtlichen Prozess gegen den ehemaligen Arbeitergeber des Betroffenen geltend gemacht und ist mittlerweile kein unüblicher Schritt bei der Trennung von Mitarbeitern.

Das LAG Niedersachen kam jedoch aufgrund der Tatsache, dass der Kläger Verfasser der besagten E-Mails ist und daher Kenntnis über deren Inhalte hat, zum Schluss, dass mit dem Auskunftsbegehren keine den Schutzzweck erfüllende Funktion erreicht würde. Zweck eines Auskunftsbegehrens seien die Überprüfung der Datenverarbeitung und Bereitstellung einer Kontrollmöglichkeit, nicht jedoch eine vollumfängliche Zusendung aller Kopien bei bereits bestehender Kenntnis der Daten.

Dies steht im Widerspruch zu vielen anderen Erkenntnissen sowohl der Gerichte als auch Behörden. In Österreich wurde vom Bundesverwaltungsgericht[8] bestätigt, dass der Grund der Ausübung eines Auskunftsanspruches keine Rolle spielt, solange das Begehren korrekt gestellt wurde. Die Erfüllung der Betroffenenrechte ist eine Pflicht des Verantwortlichen, unabhängig von der Motivlage des Betroffenen.

7. Schrems II – Eine Annäherung für die Praxis

In der Entscheidung des EuGH in der Rechtssache „Schrems II“ wurde das Privacy Shield-Abkommen als Rechtsgrundlage der Datenübermittlung in die USA für ungültig erklärt. Bis dato galt das Privacy Shield-Abkommen als Angemessenheitsbeschluss für den internationalen Datentransfer mit Unternehmen, die sich darunter zertifiziert haben. Dieses Abkommen ermöglichte die Zertifizierung bestimmter Unternehmen, sich einem angemessenen Datenschutzniveau zu unterwerfen und damit den Datentransfer in die USA zu legitimieren.

Neben dem Privacy Shield-Abkommen ist der Abschluss von sog. Standardvertragsklauseln (SCC) als Nachweis des ausreichenden Schutzniveaus für die Übermittlung personenbezogener Daten zwar denkbar. Angesichts der Verpflichtung von US-Unternehmen, die Telekommunikationsdienstleistungen erbringen, sich dem U.S. Code Title 50, Section 1881a „Procedures for targeting certain persons outside the United States other than United States persons“ (**= FISA 702**) sowie der **EO 12.333** zu unterwerfen, ist das aber kein geeignetes Mittel, um ein adäquates Datenschutzniveau zu gewährleisten. US-Unternehmen sind auf Behördenansuchen verpflichtet, Daten, die in den USA oder durch sie in Europa verarbeitet werden, an die entsprechenden Behörden zu übermitteln. Sämtliche Cloud- und Telekommunikationsanbieter wie beispielsweise Amazon (AWS), Apple, Cloudflare, Facebook, Google und Microsoft fallen darunter. Aus diesem

[7] LAG Hannover AZ: 9 Sa 608/19, Urteil vom 09.06.2020

[8] BVwG W258 2205602-1, Urteil vom 24.05.2019, RZ 3.3.5.

Grund ist die Zusammenarbeit mit diesen Anbietern aufgrund der nationalen Rechtslage in den USA selbst bei Einsatz der Standardvertragsklauseln nicht möglich, da kein adäquates Datenschutzniveau garantiert werden kann.

Der Europäische Datenschutzausschuss (European Data Protection Board, EDPB) hat ein „FAQ“ zur Rechtssache Schrems herausgegeben.

Auswege finden sich im Einsatz neuer Anbieter in Europa oder sicheren Drittländern wie Kanada oder dem **Abschluss von Standardvertragsklauseln unter Einbindung verstärkter Datensicherheitsmaßnahmen** in den Bereichen Verschlüsselung und Anonymisierung. Die Datenschutzbehörden betonen jedoch, dass es keine Schonfrist für den weiteren Einsatz von US-Anbietern gibt und die weitere Übermittlung als Verstoß gegen die DSGVO zu verstehen ist. Von Seiten der Diensteanbieter ist zu diesem Zeitpunkt keine Stellungnahme zu erhalten, und auch die US-Regierung zeigt sich derzeit nicht bereit, eine Adaption der Rechtslage für US-Diensteanbieter vorzunehmen.

Verantwortliche müssen jedoch Zeichen setzen, dass sie sich mit der geänderten Sachlage befasst haben und Anstrengungen unternommen haben, dem Urteil des EuGH zu entsprechen. Dazu gehören das Einsetzen einer Task Force und die interne Evaluierung von Auftragsverarbeitern. Der zusätzliche Abschluss von erweiterten Datensicherheitsmaßnahmen sowie Kündigungs- und Regressmöglichkeiten im Schadensfall sind ebenfalls als geeignete Initiativen aus dem EuGH-Urteil zu werten.

Max Schrems ist ebenfalls erneut tätig geworden und hat „101 Beschwerden“ gegen mehrere Verantwortliche in unterschiedlichen Ländern (darunter auch Österreich) bei den Datenschutzbehörden eingebracht. Hauptpunkt der Beschwerden ist der Einsatz von Google und Facebook bzw. anderen US-Anbietern, unter anderem im Bereich des Online-Marketing.

8. Temperatur-Messung von Mitarbeitern

Die Covid-19-Pandemie hat viele Digitalisierungsmaßnahmen im Bereich Home-Office und Telearbeit beschleunigt. Mit steigenden Zahlen besteht das Bedürfnis, die übrigen Mitarbeiter vor einer unbewussten Verbreitung von Covid-19 zu schützen. Hierzu gibt es unterschiedliche Möglichkeiten, die von freiwilligen Auskünften über den Urlaubsort hin zu digitalen Temperatur-Messstationen oder der Teilnahme an Corona-Selbsttests reichen.

Der Europäische Datenschutzbeauftragte (EDPS) hat in seiner Beratungsfunktion der EU-Organe eine „Orientierung zur Kontrolle der Körpertemperatur durch EU-Institutionen im Zusammenhang mit der COVID-19-Krise“ herausgegeben. Dort wird die Feststellung getroffen, dass die „bloße manuelle Messung, ohne nachfolgende Speicherung, Registrierung etc. nicht im Anwendungsbereich des Datenschutzrechts“ liege.

Das bedeutet für die Anwendung von Temperaturmessungen in privaten Unternehmen, dass der Anwendungsbereich der DSGVO nicht eröffnet ist, solange keine Speicherung oder Registrierung von Mitarbeiterdaten erfolgt.

Zu beachten ist jedoch, dass die Verknüpfung von Covid-19-Tests mit Personaldaten oder der Körpertemperatur mit einem Mitarbeiterprofil in den stärker reglementierten Datenverarbeitungsbereich von Art. 9 DSGVO fällt und damit einer strengeren Bewertung der Rechtmäßigkeit unterliegt. Hierbei ist stets die ausdrückliche Einwilligung der Betroffenen notwendig und die Einbindung eines etwaigen Betriebsrates ratsam.

9. Gewinnspiele und Adventkalender: Was gilt es zu beachten?

Mit der sich nähernden Weihnachtszeit kommen auch die Advent-Gewinnspiele zurück. Wir möchten Ihnen einen Überblick über die notwendigen Schritte eines rechtskonformen Gewinnspiels oder Adventkalenders im Internet geben. Dabei gilt es jedenfalls zu unterscheiden, an wen sich das Gewinnspiel richtet. Sofern es sich um minderjähriges Publikum handelt, ist eine Altersverifikation zwingend notwendig bzw. muss sichergestellt werden, dass die Erziehungsberechtigten eine datenschutzrechtliche Einwilligung zur Teilnahme erteilt haben.

1. Erhebung der Daten

Beachten Sie bei der Erhebung der Daten die Grundsätze der Zweckbindung, Datenminimierung und Speicherbegrenzung. Fragen Sie nur die Daten ab, die für die Durchführung des Gewinnspiels notwendig sind und löschen Sie diese im Anschluss. Eine Weiterverarbeitung der Daten nach Abschluss des Gewinnspiels für andere Zwecke kann einen Verstoß gegen die DSGVO darstellen.

2. Einwilligung

Ein Gewinnspiel im Internet erfordert eine datenschutzrechtliche Einwilligung. Diese muss für den Zweck eindeutig bestimmt sein, aktiv und freiwillig erteilt werden. Dabei spielt Transparenz eine wichtige Rolle.

Optional kann das Recht zur Nennung des Namens der Teilnehmer abgefragt werden.

3. Koppelungsverbot

Achten Sie darauf, dass die Einwilligung nicht an eine Dienstleistung oder anderweitige Vertragserfüllung geknüpft ist. Der OGH und die Datenschutzbehörde haben sich bereits klar zum sog. Koppelungsverbot des Art. 7 Abs. 4 DSGVO geäußert. Dabei ist eine Einwilligung dann nicht freiwillig erteilt, wenn sie an die Bedingung der Vertragserfüllung geknüpft ist. Ein jederzeitiges Widerrufsrecht ist ebenfalls nicht als Instrument der Freiwilligkeit zu werten.

Das heißt, dass auch der Erhalt eines Newsletters nicht mit der Teilnahme an einem Gewinnspiel verknüpft werden darf. Dies lässt sich durch separate Checkboxen und Einwilligungen zur Datenverarbeitung gewährleisten.

4. Speicherdauer

Sofern Sie ein Gewinnspiel veranstalten, müssen sie für dessen Gültigkeit auch einen Auslosungszeitpunkt bekanntgeben. Werden die Daten ausschließlich zur Durchführung und Abwicklung des Gewinnspiels erhoben, sollten sie danach gelöscht werden, da der Zweck der Erhebung erreicht wurde. Bei separater Einwilligung zu Newslettern oder anderen Werbemaßnahmen dürfen die Daten ggf. bis zur Geltendmachung des Widerrufsrechts verarbeitet werden.

10. In eigener Sache

Die Firma Secur-Data feierte am 15. September dieses Jahres ihr **45-jähriges Bestehen** in der österreichischen IT- und Datenschutzbranche. Es erfüllt uns mit besonderem Stolz, dass wir über die letzten Jahrzehnte stets unseren Anspruch gewahrt haben, das Datenschutz- und IT-Recht beratend zu gestalten und die Branche zu prägen.

Prof. KommR Pollirer, der mit seinen Publikationen ausgewiesener Experte in Sachen Datensicherheit ist, gilt als Pionier und Wegbegleiter des österreichischen Datenschutzrechts per se. Seine Publikationen zu Datenschutz und IT-Sicherheit sind Standardwerke für sämtliche österreichische Praktiker. Es ist auch seinem kontinuierlichen Engagement zu verdanken,

dass in Österreich stets die praxisnahe Umsetzung des Datenschutzrechts gesucht wurde – ein Grundsatz, den wir auch in allen Beratungstätigkeiten und Kundenlösungen beständig verfolgen.

Wir haben dieses Jubiläum zum Anlass genommen, unserer Website www.secur-data.at eine modernere Gestaltung zu geben und unsere Inhalte und Produkte übersichtlicher zu präsentieren. Daneben sind wir nun mit neuen Produkten für Sie da und möchten Sie weiterhin in den Bereichen Datenschutz und IT-Security begleiten.

Wir laden Sie herzlich ein, sich auf unserer neu gestalteten Website umzusehen und die Neuerungen zu erkunden.

Wir bedanken uns für die bisherige Zusammenarbeit mit unseren Kunden und Partnern und stehen wie gewohnt für Sie zur Verfügung.

••••

Umsetzung der Whistleblowing-Richtlinie

Im Oktober 2019 ist die sog. „**Whistleblowing-Richtlinie**“ beschlossen worden. Die EU-Mitgliedstaaten haben nun 2 Jahre Zeit für die Umsetzung in das nationale Recht. Der österreichische Gesetzgeber hat angesichts der Corona-Pandemie noch keine legistischen Vorhaben geäußert, es ist allerdings im Frühjahr 2021 mit einem Gesetzesentwurf zu rechnen, sodass es ratsam erscheint, sich bereits jetzt mit diesem Thema auseinanderzusetzen.

Geschützt werden Meldungen von Verstößen gegen das EU-Recht und die Adressaten der Richtlinie sind sowohl private Unternehmen mit mehr als 50 Mitarbeitern oder einem Jahresumsatz von über EUR 10 Mio. Öffentliche Stellen sowie Gemeinden über 10.000 Einwohnern sind ebenfalls vom Anwendungsbereich umfasst.

Das Ziel ist ein wirksamer Schutz sowie die Einführung von Mechanismen zur Vermeidung von Vergeltungsmaßnahmen gegen Whistleblower (wie Belästigung am Arbeitsplatz, Diskriminierung bzw. Benachteiligungen oder Entlassung) mit Hilfe von Meldekanälen oder anderen Hinweisgebersystemen.

Wir stehen mit folgenden Beratungsleistungen zu Ihrer Verfügung

- **Auswahl der eingesetzten Technologie**
- **Beratung zu DSGVO-konformer Anwendung**
- **Beachtung arbeitsrechtlicher Problemfelder**
- **Prozessmanagement und Projektbetreuung**

Wir beraten Sie gerne bei der **Einführung eines Whistleblowing-Systems** in Ihrem Unternehmen.

Für eine unverbindliche Beratung können Sie uns unter office@secur-data.at kontaktieren oder unsere Website www.secur-data.at besuchen.