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

Dezember 2021 Ausgabe Nr. 101

Liebe Leserinnen und Leser,

das Jahr neigt sich dem Ende zu und wir möchten Sie in dieser DSG-info auf signifikante Gesetzesänderungen aufmerksam machen. Der europäische Gesetzgeber hat zur Stärkung der Verbraucherrechte zwei Richtlinien erlassen, die mit 1. Jänner 2022 in ein neues nationales Gesetz umgesetzt werden. Seit 1. November dieses Jahres ist die Novelle des TKG in Kraft, die den Europäischen Kodex für die elektronische Kommunikation[1] mit einiger Verspätung umsetzen soll.

Leider können wir Ihnen bis Redaktionsschluss keine Erörterung des konkreten Whistleblowing-Gesetzes geben. Der österreichische Gesetzgeber hat bis jetzt kein entsprechendes Durchführungsgesetz zur Whistleblowing-RL in nationales Recht umsetzt. Allerdings ist uns der Begutachtungsentwurf bekannt, den wir in dieser Ausgabe überblicksartig erörtern werden.

In Deutschland wurde ein sog. „Cookie-Gesetz" erlassen, das TTDSG, das die Rechtslage im Hinblick auf die korrekte Umsetzung der e-Privacy RL und das EuGH-Urteil in der Rechtssache Planet-49 gewährleisten soll.

Zudem möchten wir Ihnen einen Überblick über die neuen Standardvertragsklauseln geben, die nunmehr für Neuabschlüsse gelten und mit einer zwingenden Übergangsfrist versehen sind, um alte Verträge zu novellieren.

Viel Freude beim Lesen und frohe Festtage!

1. Verbrauchergewährleistungsgesetz – VGG gilt ab 1. Jänner 2022

Das europäische Verbraucherrecht und das E-Commerce-Recht befinden sich erneut im Umbruch. Dies betrifft zum einen die Richtlinie 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (**„Digitale Inhalte-RL"**)[2] und zum anderen die Richtlinie 2019/771 über bestimmte vertragsrechtliche Aspekte des Warenkaufs (**„Warenkaufs-RL"**)[3].

Inhaltlich handelt es sich dabei um die vertragliche Regulierung digitaler Inhalte und Dienstleistungen, aber auch die Veränderung von Gewährleistungsrechten aus dem allgemeinen Warenkauf kommen zum Tragen. Umgesetzt

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32018L1972&from=DE

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0770&from=DE

[3] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0771

wurden die Richtlinien als **Verbraucherrechtsnovelle** durch das Gewährleistungsrichtlinien-Umsetzungsgesetz – **GRUG,**[4] mit dem das Verbrauchergewährleistungsgesetz – **VGG** – erlassen wird. Darüber hinaus kommt es zu Änderungen im ABGB und KSchG, um die Begriffe anzupassen.

1. **Das neue Sondergewährleistungsrecht des VGG gilt nur für Verbrauchergeschäfte über**
   - den Kauf von Waren (dh beweglichen körperlichen Sachen), auch wenn sie erst herzustellen sind (Werklieferungsverträge) und
   - die Bereitstellung digitaler Leistungen (Inhalte und Dienstleistungen) gegen Zahlung oder Überlassung personenbezogener Daten (§ 1 Abs. 1 VGG).
2. **Das VGG gilt unter anderem nicht für Verträge über**
   - unbewegliche Sachen
   - den Kauf lebender Tiere
   - analoge Dienstleistungen: Das sind „klassische" Dienstleistungen wie z. B. Beratungsleistungen. Für sie gilt das VGG auch dann nicht, wenn digitale Mittel eingesetzt werden, um das Ergebnis der Dienstleistung zu erzeugen oder es dem Verbraucher zu liefern oder übermitteln.
   - bestimmte Glücksspieldienstleistungen wie Lotterien, Kasinospiele, Pokerspiele und Wetten, einschließlich Spielen, die eine gewisse Geschicklichkeit voraussetzen
   - bestimmte Finanzdienstleistungen
   - Sachen, die im Rahmen einer gerichtlichen Versteigerung verkauft werden

[4] BGBl I 175/2021, https://ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2021_I_175/BGBLA_2021_I_175.pdfsig

3. Die Änderungen im Überblick

Im Wesentlichen geht es vor allem um Verträge, die digitale Inhalte und Dienstleistungen zwischen Unternehmern und Verbrauchern behandeln (Apps, Smart Tech, E-Books, Cloud-Services), und deren Einhaltung, Aufrechterhaltung und Beendigung.

Wesentliche Änderung im Warenhandel ist eine **Verlängerung der Vermutungsregel für die Mangelhaftigkeit** einer Ware. Statt der bisherigen 6 Monate ab Übergabe soll es nun eine **Frist von 1 Jahr** (optional 2 Jahre) geben. Dies stellt Sie als Unternehmen durchaus vor Handlungsbedarf zur Änderung ihrer AGB und Prozesse. Betroffen sind jedoch nur Verträge, die **ab dem 1. Jänner 2022** geschlossen werden.

Eine wichtige Änderung betrifft die **Geltendmachung von Gewährleistungsrechten**: Diese müssen nicht mehr gerichtlich geltend gemacht werden.

Zudem ermöglicht das Gesetz nunmehr das „Bezahlen mit personenbezogenen Daten" als Entgelt. Hierbei werden sich noch einige Problemstellungen auftun, die durch die Gerichte zu klären sind.

Es kommt zu einer Änderung der Begrifflichkeiten des ehemaligen Gewährleistungsrechts. Auf der primären Ebene bleibt es bei Verbesserung und Austausch. Auf der sekundären Ebene kommt es nunmehr zu einer Preisminderung und Auflösung des Vertrages (vormals Wandlung). Alle Behelfe können durch eine formfreie Erklärung geltend gemacht werden. Das bedeutet, dass die gerichtliche Geltendmachung des Gewährleistungsrechts nicht mehr erforderlich ist, wodurch die Position der Verbraucher gestärkt werden soll.

Eine weitere Neuerung ist die Einführung einer „Verjährungsfrist“ für Gewährleistungsansprüche. Der Gewährleistungszeitraum für einen Mangel an der Ware, der bei der Übergabe schon vorlag, beträgt wie bisher 2 Jahre. Davon zu unterscheiden ist die Frist, diese Ansprüche auch gerichtlich geltend zu machen. Konkret tritt 3 Monate nach Ablauf des Gewährleistungszeitraums eine Verjährung des Anspruches ein. Daraus ergibt sich eine **Änderung der datenschutzrechtlichen Aufbewahrungsfristen**, da nunmehr eine dreimonatige Verjährungsfrist hinzukommt.

2. TKG-Novelle 2021

Das TKG 2003 wurde durch die Umsetzung der EECC-RL novelliert und ist nun mehr das TKG 2021.

Damit wurden zwei datenschutzrelevante Paragrafen verschoben, jedoch inhaltlich im Wesentlichen nicht verändert. Dies betrifft zum einen den „Cookie-Paragraf“ (§ 96 Abs. 3) sowie den „Spam-Paragraf“ (§ 107). Sie finden im Anhang einen entsprechenden Textvergleich.

Aus § 96 Abs. 3 TKG 2003 wurde § 165 Abs. 3 TKG 2021 („Datenschutz – Allgemeines“).

Aus § 107 TKG 2003 wurde § 174 TKG 2021 („Unerbetene Nachrichten“).

Die weiteren Änderungen des TKG betreffen im Wesentlichen Telekommunikationsanbieter.

3. Whistleblowing – Entwurf eines Gesetzesvorschlages

Wir können Ihnen vor Jahresende bedauerlicherweise nicht die österreichische Umsetzung des Whistleblowing-Gesetzes (künftig WbG) präsentieren. Der Gesetzgeber hat es verabsäumt, ein Gesetz zur Whistleblowing-RL bis 17. Dezember 2021 zu verabschieden. Es liegt ein **Entwurf** vor, der jedoch keine zeitgerechte Verabschiedung durch den Nationalrat ermöglicht.

Fristen

Das Gesetz soll noch im 1. Quartal 2022 in Kraft treten. Für die Errichtung eines Hinweisgebersystems wird es je nach Anzahl der Mitarbeiter Übergangsfristen geben. So sieht die Gesetzesvorlage für Unternehmen mit weniger als 250 Mitarbeiter eine Übergangsfrist bis zum **18. Dezember 2023** vor. Die noch im Gesetzesentwurf enthaltene Frist mit 1. Jänner 2022 für Unternehmen mit mehr als 250 Mitarbeiter scheint aufgrund der verspäteten Umsetzung überholt.

Anwendungsbereich

Der persönliche Anwendungsbereich ist weit gefasst und umfasst sowohl bestehende als auch ehemalige Mitarbeiter sowie Bewerber und Praktikanten. Das Spektrum der zu erfassenden Rechtsverletzungen ist noch nicht vollständig erfasst. Umfasst sind jedoch ua. das öffentliche Auftragswesen, Finanzdienstleistungen, Umweltschutz, öffentliche Gesundheit, Verbraucherschutz sowie der Schutz der Privatsphäre und personenbezogener Daten sowie die Sicherheit von Netz- und Informationssystemen.

Inhaltliche Punkte

Die Schutzwürdigkeit der Hinweisgeber bemisst sich nach jenem Umfang und der Art der von ihnen gemachten Hinweise rechtlicher Missstände. Jeder Hinweis ist auf seine Stichhaltigkeit zu überprüfen und kann dann zurückgewiesen werden, wenn er nicht in den Geltungsbereich fällt oder keine Anhaltspunkte für seine Stichhaltigkeit hervorgehen.

Eine Rückmeldung an einen Hinweisgeber hat **spätestens nach 3 Monaten** zu erfolgen, mit der Angabe entsprechender beabsichtigter Maßnahmen, wie Nachforschungen oder Untersuchungen bzw. einer Begründung, warum kein weiteres Vorgehen erfolgt.

Interne oder externe Meldestelle

Konzernunternehmen mit jeweils weniger als 250 Mitarbeitern können die Aufgaben der internen Stelle auf eine gemeinsame Stelle übertragen oder mit diesen Aufgaben Dritte beauftragen.

Datenschutz

Bei der Errichtung des Hinweisgebersystems ist nach den Maßstäben des Art. 25 DSGVO (Privacy by Design and Default) sicherzustellen, dass technisch sowohl die Anonymität der Hinweisgeber als auch deren personenbezogene Daten ausreichend geschützt sind. Die Vertraulichkeit der Identität von Dritten, die vom Hinweisgeber genannt werden, muss gewährleistet sein.

In organisatorischer Hinsicht muss das Hinweisgebersystem finanziell und technisch im ausreichenden Umfang abgesichert sein. Bei der Entgegennahme und Prüfung von Hinweisen muss das System unabhängig und neutral vorgehen und damit weisungsfrei im Unternehmen angesiedelt werden.

Für die bei der Hinweisgebung verarbeiteten Daten besteht eine Aufbewahrungsfrist von 30 Jahren.

Ausnahmen

Einem Hinweis muss nicht nachgegangen werden, wenn kein sachlicher Anwendungsbereich eröffnet ist (offener Umfang) oder der Hinweis keine stichhaltigen Anknüpfungspunkte aufweist, um diesen zu prüfen.

Rechtsfolgen

Hinweisgeber sind rechtlich vor Vergeltungsmaßnahmen (Kündigungen, Schadenersatz) geschützt, wenn Schutzwürdigkeit besteht.

Unternehmen können sich nicht auf Geheimhaltungsverpflichtungen oder die Verletzung von Geschäfts- oder Betriebsgeheimnissen berufen. Es ist eine Beweislastumkehr zugunsten des Hinweisgebers geplant.

Darüber hinaus soll es **Strafbestimmungen** für Unternehmen geben, die Hinweisgebungen behindern, aber auch für Hinweisgeber, die wissentlich falsche Hinweise melden.

Status Quo

Die RL selbst enthält zwar lediglich Mindeststandards wie die Einrichtung eines internen Meldesystems bzw. die Eröffnung des Anwendungsbereichs (sachlich beschränkt auf die Rechtsmaterien). Die Konsequenz der Säumigkeit durch den österr. Gesetzgeber bedeutet aber im Wesentlichen, dass die RL unmittelbar anwendbar sein kann.

Durch den Unionsrechtsvorrang auch bei verspäteter, fehlerhafter oder falscher Umsetzung entfalten sich bestimmte Rechte und Pflichten unmittelbar. Sollte es in einem Unternehmen also zu Repressalien oder negativen Maßnahmen gegen sog. Whistleblower ab dem 17. Dezember 2021 kommen, würde dies wohl unmittelbar nach EU-Recht zu bewerten sein und es können die in der RL vorgesehenen Schutzwirkungen zum Tragen kommen.

4. Standardvertragsklauseln ab sofort im Einsatz

Wie in Ausgabe Nr. 99 bereits angekündigt, hat die EU-Kommission am 4. Juni 2021 neue EU-Standardvertragsklauseln („SCC 2021“) beschlossen.

Bis zum **27. September 2021 bereits vereinbarte** alte EU-Standardvertragsklauseln können noch bis **27. Dezember 2022** als Grundlage für den internationalen Datentransfer genutzt werden. Im Falle von

Vertragsänderungen und bei **Neuverträgen** müssen **ab dem 27. September 2021** die bisherigen EU-Standardvertragsklauseln gegen die SCC 2021 ausgetauscht werden.

Spätestens mit 27. Dezember 2022 sind **alle** betroffenen Datenübermittlungen auf die neuen Standardvertragsklauseln umzustellen.

Hier ist also bereits umfassender Handlungsbedarf vorhanden, bei dem wir Ihnen gerne zur Seite stehen.

Die SCC 2021 unterteilen sich in vier Module und ermöglichen die nachfolgenden Datentransfers:

Modul 1 **Controller to Controller**	**Modul 2** **Controller to Processor**	**Modul 3** **Processor to Processor**	**Modul 4** **Processor to Controller**
zwischen einem in der EU niedergelassenen Verantwortlichen und einem Nicht-EU-Verantwortlichen	zwischen einem EU-Verantwortlichen und einem Nicht-EU-Auftragsverarbeiter	zwischen einem EU-(Sub-) Auftragsverarbeiter und einem Nicht-EU-Sub-Auftragsverarbeiter	zwischen einem Nicht-EU-Verantwortlichen und einem EU-Auftragsverarbeiter

Künftig wird somit eine Vielzahl an Konstellationen im internationalen Datentransfer von diesen Klauseln abgedeckt. Ein wesentlicher Vorteil ist dabei die Klausel 7 als sog. „Koppelungsklausel / Docking Clause“. Diese ermöglicht auf freiwilliger Basis den Beitritt eines Dritten als Datenexporteur oder -importeur, ohne dass dies den Abschluss eines separaten Vertrages erforderlich macht.

Zudem kann der Einsatz der SCC 2021 auch den Abschluss einer Art. 28-Vereinbarung (Auftragsverarbeitungsvereinbarung) ersetzen, da die Klauseln den Mindestanforderungen entsprechen.

Für Unternehmen neu: Garantieerklärung und Transfer Impact Assessment

Klausel 14 formuliert die gemeinsame Verpflichtung zwischen Datenimporteur im Drittland und datenexportierendem Unternehmen, ein sog. „Transfer Impact Assessment“ (TIA) durchzuführen. Mit den im Einsatz befindlichen Unternehmen muss Kontakt aufgenommen werden, um dieses TIA durchführen zu können.

5. TTDSG – neues deutsches Cookie-Gesetz

Ab dem 1. Dezember 2021 gelten in Deutschland die gesetzlichen Regelungen des neuen Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG). Unter den Begriff „Telemedien“ fallen beispielsweise Websites und Apps. Es handelt sich hierbei um eine richtlinienkonforme Anpassung an die E-Privacy-RL sowie die Erkenntnisse des EuGH (zB in der RS Planet49).

Konkret soll der Einsatz von Tracking-Technologien wie Cookies, Web Storage, Browser-Fingerprinting unabhängig von der Frage, ob dabei personenbezogene Daten verarbeitet werden, stets einer Einwilligung bedürfen. Dies zeigt die Abgrenzung zwischen DSGVO und E-Privacy-RL zur Endnutzer-Datenverarbeitung und stellt klar, dass der Einsatz von Tracking-Technologien auch unabhängig von der

Einschätzung, ob personenbezogene Daten verarbeitet werden, reguliert ist.

Die Ausnahme von der Einwilligungspflicht stellen unbedingt erforderliche Cookies dar. Der Gesetzgeber lässt allerdings Interpretationsspielraum, was unter diesen sog. „notwendigen" Cookies zu verstehen ist. Jedenfalls unzulässig erscheint die Nutzung von Nutzertracking zu Werbezwecken oder zur Produkt- und Dienstleistungsoptimierung (Webanalyse).

Dazu kommt eine gesetzliche Erweiterung der Einwilligungsverwaltung durch sog. „PIMS", die in **§ 26 TTDSG unter „Anerkannte Dienste zur Einwilligungsverwaltung, Endnutzereinstellungen" normiert werden.** Deutschen Unternehmen wird nunmehr ein Einwilligungsverwaltungssystem nahegelegt, das jedoch von einer unabhängigen Stelle bezogen werden muss. Die Regelungen für „Personal-Information-Management-Services – PIMS" als Einwilligungsverwaltungsdienste, die in Zukunft Cookie-Banner ersetzen sollen, müssen von Seiten der Bundesregierung noch verfasst werden. Bis dato gibt es noch keine näheren Informationen zu den Anforderungen an die Anerkennung solcher Dienste.

Ziel ist die datenschutz- und nutzerfreundliche Voreinstellung zur Einholung und Verwaltung der Einwilligungen auf Websites, ähnlich der ursprünglichen „Do-Not-Track"-Einstellungen im Browser. Diese Verwaltung wird jedoch zu einem Dritten ausgelagert, der mit den Daten keine eigenen Zwecke verfolgen darf.

Zum einen legt der deutsche Gesetzgeber damit einen konkreten Rechtsrahmen zur Setzung von Cookies fest, der im Einklang mit der EuGH-Rechtsprechung steht. Zum anderen wird der Einsatz von Cookies bei Endnutzern mit einem unabhängigen Gatekeeper versehen.

Der Gesetzgeber hält damit fest, dass beim Setzen von Cookies nur noch die Einwilligung zur Anwendung gelangt. Eine Ausnahme bilden Cookies und Skripts, die für die Bereitstellung eines Dienstes „unbedingt erforderlich" sind. Die Deutsche Gesellschaft für Datenschutz und Datensicherheit e.V. stellt eine **Praxishilfe**[5] zur Verfügung.

6. Datenschutzerkenntnisse im Überblick

EuGH-Urteil zu Inbox-Werbung

Der Europäische Gerichtshof (EuGH) hat in der RS C-102/20 v. 25.11.2021 entschieden, dass sog. „Inbox-Werbung" denselben Regelungen unterliegt wie E-Mail-Werbung und daher einwilligungsbedürftig ist. Hierzu seien die als E-Mail getarnten Werbenachrichten mit dem Hinweis „Anzeige" bereits unter dem Begriff „elektronische Post" zu subsumieren. Aus diesem Grund stellt die Anzeige solcher Werbungen in einem E-Mail-Postfach ohne Einwilligung der Nutzer eine Verletzung ihrer Privatsphäre durch unerbetene Nachrichten für Zwecke der Direktwerbung dar.

VG Wiesbaden verbietet Cookiebot-Einsatz

Das berüchtigte Verwaltungsgericht Wiesbaden hat wieder zugeschlagen und diesmal eine nicht unwesentliche Entscheidung in gleich zwei datenschutzrechtlich sensiblen Bereichen getroffen. Zum einen entschied es über den Einsatz eines sog. „Cookie-Consent"-Tools und zum anderen auch als eines der ersten deutschen Gerichte über konkrete Verbote nach der Schrems II-Entscheidung.

[5] https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ttdsg-im-ueberblick

Das VG Wiesbaden hat in seiner Entscheidung (6 L 738/21.WI v. 1.12.2021)[6] mittels einstweiliger Verfügung den Einsatz des Consent-Management-Tools „Cookiebot" verboten. Der rechtskonforme Einsatz von Cookiebot ist wegen der Übermittlung von Daten an das Herkunftsland des Anbieters (USA), das nach der Schrems II-Entscheidung des EuGH nicht mehr als sicheres Drittland gilt, nicht mehr möglich.

Eine Hochschule in Deutschland nutzte dieses Tool, um die Einholung der Einwilligung auf ihrer Website zu dokumentieren und zu verwalten. Der Hochschule wurde per einstweiliger Verfügung untersagt, Cookiebot zum Zweck des „Einwilligungsmanagements" zu verwenden.

Diese Entscheidung basiert auf mehreren Gründen. Zum einen handelt es sich bei Cookiebot um einen Drittanbieter, der eindeutig personenbezogene Daten verarbeitet. Während es in der Marketing-Welt umstritten war, ob Cookie-IDs als Personenbezug zu werten sind, stellt das VG Wiesbaden dies nunmehr klar: Die Verknüpfung aus der vollständigen IP-Adresse des Besuchers, die an eine Nutzer-ID gebunden ist und auf dem Endgerät des Besuchers verbleibt, stellt einen eindeutigen Personenbezug dar. Aus diesem Grund liegt eine Datenverarbeitung vor, die den Anwendungsbereich der DSGVO eröffnet. Die Daten werden an Server übermittelt, die wiederum von einem externen Drittunternehmen betrieben werden, das seinen Sitz (nicht zwingend seine Server) in den USA hat. Aus diesem Grund besteht eine Datenübermittlung in die USA und muss anhand der in der RS Schrems II aufgestellten Kriterien auf ihre Rechtmäßigkeit geprüft werden.

[6] https://verwaltungsgerichtsbarkeit.hessen.de/pressemitteilungen/cookie-dienst

Irische Datenschutzbehörde[7] zu AGB als Verarbeitungsgrundlage

Im Verfahren zwischen der irischen Datenschutzbehörde und Max Schrems gegen Facebook wurde ein Entscheidungsentwurf geleakt. Die irische Behörde hält Facebooks Argument, dass die Datennutzung für Werbe- und Personalisierungszwecke auch in den AGB als vertragliche Rechtsgrundlage festgehalten werden kann, für zulässig. Max Schrems sieht hingegen das Erfordernis, dies anhand einer informierten Einwilligung vornehmen zu können. Dieser Entscheidungsentwurf hat keine Bindewirkung, denn er dient der Vorlage bei anderen Aufsichtsbehörden, die gegen diese Entscheidung auch Einspruch erheben können.

EuGH-Vorlagefrage: Bonitätsprüfung als Profiling mit der DSGVO vereinbar?

Ein deutsches Verwaltungsgericht hat die Frage,[8] ob die Score-Berechnung der deutschen SCHUFA mit den Vorgaben der Datenschutzgrundverordnung (DSGVO) zur automatisierten Entscheidungsfindung vereinbar ist, dem EuGH vorgelegt. Der EuGH muss nun klären, ob es sich beim Scoring und der Weitergabe der Ergebnisse an Dritte um einen Fall des Art. 22 DSGVO handelt. In Deutschland wurde aus Art. 22 DSGVO eine nationale Vorschrift abgeleitet, die nun möglicherweise als unionsrechtswidrig einzustufen ist, da keine Öffnungsklausel vorliegt. In Österreich erfolgt die Bonitätsprüfung anhand des § 152 GewO und ist Wirtschaftsauskunfteien vorbehalten.

Max Schrems legt Beschwerde gegen Acxiom und CRIF wegen Datenhandel ein

Der Datenschutzverein von Max Schrems hat Beschwerde gegen den Adresshändler Acxiom und die Kreditauskunft CRIF Bürgel eingereicht. Der Vorwurf: Acxiom verkaufe die Adressdaten

[7] https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf

[8] VG Wiesbaden, 6 K 788/20.WI.

von Millionen deutschen Bürgern an CRIF Bürgel, ohne die Betroffenen zu informieren oder deren Einwilligung einzuholen.

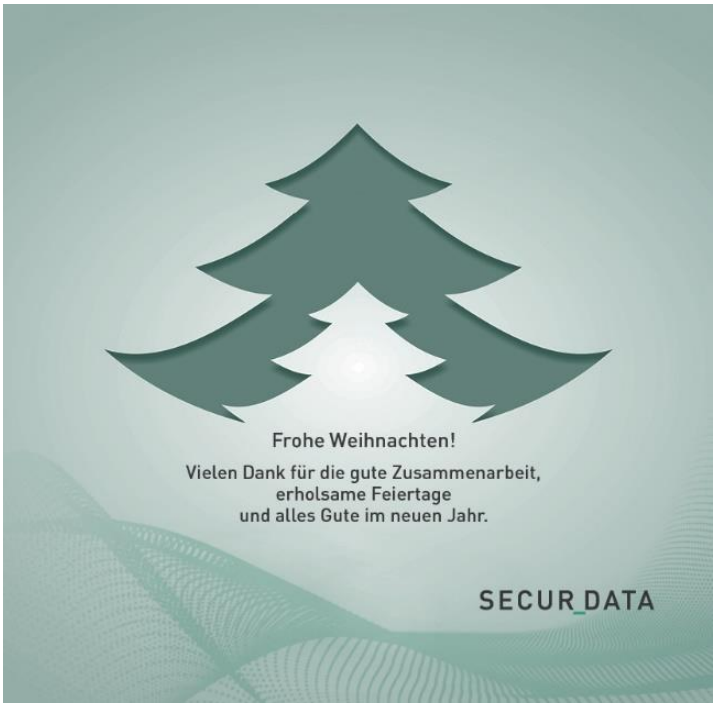
Die personenbezogenen Daten wurden zum Zweck des Direktmarketings erhoben bzw. gesammelt und nun an die CRIF weiterveräußert, um damit Kreditauskünfte zu erteilen. Der Datenschutzverein wirft Acxiom daher vor, personenbezogene Daten rechtswidrig an CRIF Bürgel zu verkaufen. Darüber hinaus würden die Betroffenen nicht oder nicht ausreichend über diese Datenströme informiert. Die Kreditauskunft CRIF Bürgel hätte Datensätze von mehr als 62 Millionen Privatpersonen.

DSGVO: Bußgeld gegen Vattenfall wegen intransparenter Kundenanalysen

Der Hamburgische Datenschutzbeauftragte (HmbBfDI) hat gegen den Energieversorger Vattenfall ein Bußgeld in Höhe von EUR 901.000 verhängt, da dieser seine potenziellen Kunden mit „wechselauffälligem Verhalten" analysiert und abgeglichen hat. Vattenfall soll zwischen August 2018 und Dezember 2019 bei bestimmten Verträgen einen Abgleich der Interessenten und Alt-Kunden vorgenommen haben, wenn ein Bonus für einen Neuabschluss gewährt werden sollte. Dabei wurde geprüft, ob Interessenten bereits einmal Kunden waren und eine Art „Bonushopping" betreiben würden. Dieser Datenabgleich zwischen den Kundendaten erfolgte ohne Information an die Betroffenen, was der HmbBfDI als Verstoß gegen das Transparenzgebot angesehen und daher für den Ausspruch des Bußgeldes herangezogen hat.

7. Seminarankündigung 2022

Wir möchten Sie auf diesem Wege noch über unsere Seminartermine für das Jahr 2022 informieren. Auch wenn die Pandemie noch einige Überraschungen bereithalten kann, planen wir die Durchführung unserer Informationssicherheits- und Datenschutzseminare am 30. und 31. März 2022.



Anhang:

§ 96 Abs. 3 TKG 2003

(3) Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft im Sinne des § 3 Z 1 E-Commerce-Gesetz, BGBl. I Nr. 152/2001, sind verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er verarbeiten wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Ermittlung dieser Daten ist nur zulässig, wenn der Teilnehmer oder Nutzer seine Einwilligung dazu erteilt hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Der Teilnehmer ist auch über die Nutzungsmöglichkeiten auf Grund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren. Diese Information hat in geeigneter Form, insbesondere im Rahmen Allgemeiner Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen. Das Auskunftsrecht nach dem Datenschutzgesetz und der DSGVO bleibt unberührt.

§ 165 Abs. 3 TKG 2021 („Datenschutz – Allgemeines“)

(3) Betreiber öffentlicher Kommunikationsdienste und Anbieter eines Dienstes der Informationsgesellschaft im Sinne des § 3 Z 1 E-Commerce-Gesetz, BGBl. I Nr. 152/2001, sind verpflichtet, den Nutzer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er verarbeiten wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Eine Ermittlung dieser Daten ist nur zulässig, wenn der Nutzer oder Benutzer seine Einwilligung dazu aktiv und auf Grundlage von klaren und umfassenden Informationen erteilt hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Nutzer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Der Nutzer ist auch über die Nutzungsmöglichkeiten auf Grund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen zu informieren. Diese Information hat in geeigneter Form, insbesondere im Rahmen Allgemeiner Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen.

§ 107 TKG 2003

(1) Anrufe – einschließlich das Senden von Fernkopien – zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers sind unzulässig. Der Einwilligung des Teilnehmers steht die Einwilligung einer Person, die vom Teilnehmer zur Benützung seines Anschlusses ermächtigt wurde, gleich. Die erteilte Einwilligung kann jederzeit widerrufen werden; der Widerruf der Einwilligung hat auf ein Vertragsverhältnis mit dem Adressaten der Einwilligung keinen Einfluss.

(1a) Bei Telefonanrufen zu Werbezwecken darf die Rufnummernanzeige durch den Anrufer nicht unterdrückt oder verfälscht werden und der Diensteanbieter nicht veranlasst werden, diese zu unterdrücken oder zu verfälschen.

§ 174 TKG 2021 („Unerbetene Nachrichten“)

(1) Anrufe – einschließlich das Senden von Fernkopien – zu Werbezwecken ohne vorherige Einwilligung des Nutzers sind unzulässig. Der Einwilligung des Nutzers steht die Einwilligung einer Person, die vom Endnutzer zur Benützung seines Anschlusses ermächtigt wurde, gleich. Die erteilte Einwilligung kann jederzeit widerrufen werden; der Widerruf der Einwilligung hat auf ein Vertragsverhältnis mit dem Adressaten der Einwilligung keinen Einfluss.

(2) Bei Telefonanrufen zu Werbezwecken darf die Rufnummernanzeige durch den Anrufer nicht unterdrückt oder verfälscht werden und der Diensteanbieter nicht veranlasst werden, diese zu unterdrücken oder zu verfälschen.

(2) Die Zusendung einer elektronischen Post – einschließlich SMS – ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt.

(3) Eine vorherige Einwilligung für die Zusendung elektronischer Post gemäß Abs. 2 ist dann nicht notwendig, wenn

1. der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und
2. diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und
3. der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und
4. der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Eintragung in die in § 7 Abs. 2 E-Commerce-Gesetz genannte Liste, abgelehnt hat.

(Anm.: Abs. 4 aufgehoben durch BGBl. I Nr. 133/2005)

(5) Die Zusendung elektronischer Post zu Zwecken der Direktwerbung ist jedenfalls unzulässig, wenn

1. die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird, oder
2. die Bestimmungen des § 6 Abs. 1 E-Commerce-Gesetz verletzt werden, oder
3. der Empfänger aufgefordert wird, Websites zu besuchen, die gegen die genannte Bestimmung verstoßen oder
4. keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

(6) Wurden Verwaltungsübertretungen nach Absatz 1, 2 oder 5 nicht im Inland begangen, gelten sie als an jenem Ort begangen, an dem die unerbetene Nachricht den Anschluss des Teilnehmers erreicht.

(3) Die Zusendung einer elektronischen Post – einschließlich SMS – ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt.

(4) Eine vorherige Einwilligung für die Zusendung elektronischer Post gemäß Abs. 3 ist dann nicht notwendig, wenn

1. der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und
2. diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und
3. der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und
4. der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Eintragung in die in § 7 Abs. 2 E-Commerce-Gesetz genannte Liste, abgelehnt hat.

(5) Die Zusendung elektronischer Post zu Zwecken der Direktwerbung ist jedenfalls unzulässig, wenn

1. die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird, oder
2. die Bestimmungen des § 6 Abs. 1 E-Commerce-Gesetz verletzt werden, oder
3. der Empfänger aufgefordert wird, Websites zu besuchen, die gegen die genannte Bestimmung verstoßen oder
4. keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

(6) Wurden Verwaltungsübertretungen nach Absatz 1, 3 oder 5 nicht im Inland begangen, gelten sie als an jenem Ort begangen, an dem die unerbetene Nachricht den Anschluss des Nutzers erreicht.