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

Juni 2021 Ausgabe Nr. 99

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

Wir freuen uns, Sie mit unserer DSG-Info wieder über einige wichtige Ereignisse auf dem Gebiet des Datenschutzes informieren zu dürfen.

Nach einem kurzen Versuch einer Standortbestimmung über drei Jahre DSGVO in Österreich und der damit in Zusammenhang stehenden regen Tätigkeit der DSB sowie der Gerichte, ist als wichtigstes Ereignis die seit Jahren erwartete Verabschiedung der neuen DSGVO-Standardvertragsklauseln zu nennen. Weiters bedingt der Brexit, dass nunmehr britische Unternehmen, die in der EU personenbezogene Daten in Zusammenhang mit Waren und Dienstleistungsangeboten verarbeiten und über keine Tochtergesellschaft in der EU verfügen, einen Vertreter in der Union benennen müssen.

Unangenehm könnte eine Aktion der deutschen Aufsichtsbehörden für österreichische Unternehmen werden, die die internationalen Datentransfers von in Deutschland ansässigen Unternehmen prüft, sowie eine weitere Aktion des österreichischen Datenschutzaktivisten Max Schrems, der mit der Datenschutz-NGO NOYB an mehr als 500 Unternehmen Beschwerden in Zusammenhang mit dem Einsatz fehlerhafter Cookie-Banner verschickt hat.

Last but not least berichten wir noch über zwei interessante EuGH-Vorlageverfahren aus Österreich und einen Verordnungsvorschlag der EK für eine Europäische Digitale Identität.

Wir wünschen viel Vergnügen beim Lesen!

1. Drei Jahre DSGVO in Österreich – Status quo

Die DSGVO ist seit dem 25. Mai 2018 anwendbar und wir sind der Meinung, es ist Zeit, Bilanz zu ziehen. Festzustellen ist, dass sich auch nach drei Jahren noch immer viele Unternehmen bei der Anwendung dieser Rechtsmaterie schwertun und Unsicherheit herrscht. Eine im Herbst 2020 durchgeführte Studie des Deutschen Bundesverbandes Bitkom ergab, dass lediglich 20 % der befragten Unternehmen angaben, die Bestimmungen der DSGVO „erfolgreich“ umgesetzt zu haben, 37 % hatten die DSGVO „größtenteils“ und 35 % zumindest „teilweise“ umgesetzt. Als Grund für dieses Ergebnis wurde vor allem **Rechtsunsicherheit** beklagt. Wir gehen davon aus, dass die Situation in Österreich nicht allzu stark von jener in Deutschland abweicht. Als großer Vorteil wirkt sich in Österreich jedoch die Tatsache aus, dass es nur **eine Aufsichtsbehörde** (DSB) gibt, wogegen die deutschen Unternehmen mit **18**

Aufsichtsbehörden konfrontiert sind, die durchaus die Bestimmungen der DSGVO unterschiedlich auslegen und die gerichtlichen Instanzen ebenfalls kasuistische Erkenntnisse verfassen.

Positiv anzumerken ist, dass die DSB ihr Wort gehalten hat und verhältnismäßig und mahnend in den Ring gestiegen ist. Sie hat dort, wo Strafen notwendig waren, Bußgelder verhängt und ist in Beschwerdeverfahren umfassend tätig geworden.

Die Anzahl der Datenschutzbeschwerden ist in Österreich – als vergleichsweise kleines Land in der EU – relativ hoch und beschäftigt die DSB intensiv. Aber nicht nur bei den Beschwerden (**1.603 im Jahr 2020**) ist die DSB hierzulande viel beschäftigt. Auch die amtswegigen Prüfverfahren (**337 im Jahr 2020, 215 im Jahr 2019**) steigen stetig an und zeigen, dass die DSB nicht nur die großen Fische ins Auge fasst, sondern ihr Augenmerk auch auf KMUs legt. Angesichts der Pandemie und den gesteigerten Sicherheitsrisiken durch Home-Office und die abrupte Einführung neuer IT-Strukturen, sind **860 gemeldete Data Breaches** auch eine stattliche Anzahl, der die DSB im vergangenen Jahr nachgegangen ist. Von einer gewissen Dunkelziffer ganz zu schweigen.

Die Anzahl der Verfahren vor dem Bundesverwaltungsgericht, also der Rechtsmittelinstanz, steigt naturgemäß mit jedem neuen Beschwerdeverfahren ebenfalls an und führt manchmal auch zu vollständigen Behebungen der ursprünglichen Erkenntnisse. Doch in Anbetracht der Neuartigkeit der Gesetzeslage sind dogmatische Auslegungen vor Gericht der beste Ort für Klärungen der Rechtslage, und so kommt es nicht nur im Verwaltungsrecht (**DSB, BVwG, VwGH, VfGH**) zu einer richterlichen Rechtsfortbildung, auch der **Oberste Gerichtshof** hat in drei Jahren bereits einige zivilrechtliche Erkenntnisse zum Datenschutz und der DSGVO verfasst.

Mittlerweile sind sogar schon zwei Verfahren im Zusammenhang mit der Datenverarbeitung eines Adressverlages zur **Vorabentscheidung** an den **Europäischen Gerichtshof** ausgesetzt. Dazu mehr unter Punkt 6.

Erfreulicherweise verbessert sich die Situation in Österreich in großen Schritten, sodass wir optimistisch in die Zukunft schauen und uns weiterhin um einen praxisnahen Umgang mit den Themen Datenschutz und Datensicherheit für Sie bemühen werden.

2. Neue Standardvertragsklauseln (Standard Contractual Clauses – SCC) erlassen

Die EU-Kommission hat neue DSGVO-Standardvertragsklauseln verabschiedet. Es handelt sich hierbei um Musterverträge, die zwischen einem Verantwortlichen in der EU und einer Entität in einem Drittland abgeschlossen werden und die Anpassung des Datenschutzniveaus für die Übermittlung personenbezogener Daten zum Ziel haben. Bekanntermaßen ist dies unter den Gesichtspunkten der EuGH-Entscheidung im Schrems-II-Verfahren zu sehen, wobei die Notwendigkeit neuer SCCs bereits seit der Geltung der DSGVO bekannt war. Die neuen SCCs betreffen die Übermittlung von personenbezogenen Daten in **Drittländer** zwischen **zwei Verantwortlichen** oder zwischen **Auftragsverarbeitern**.

Anders als in der Vergangenheit betreffen die Regelungen inhaltlich die Übermittlung von personenbezogenen Daten in Drittländer ohne Angemessenheitsbeschluss oder anderer

geeigneter Garantien. Der Aufbau der Muster-verträge[1] findet in **Modulen** statt.

Modul I	Modul II	Modul III	Modul IV
Controller to Controller	**Controller to Processor**	**Processor to Processor**	**Processor to Controller**

Durch die flexible Gestaltung der Verträge, die auch Gerichtsstände, Haftungsregeln und Zuständigkeiten der jeweiligen Aufsichtsbehörde beinhalten, können Unternehmen ihren Datentransfers mit mehr Rechtssicherheit begegnen.

Sobald diese Standardvertragsklauseln im Amtsblatt der Europäischen Union offiziell veröffentlicht wurden, besteht eine insgesamt absolute 18-monatige Übergangsfrist zum Neuabschluss und Ersatz der Verträge. Nach Ablauf dieser Frist müssen alle ehem. Verträge durch die neuen SCCs ersetzt worden sein, um den Anforderungen des internationalen Datenverkehrs zu genügen. Sollten Sie nicht im Rahmen der Schrems-II Evaluierung bereits eine Übersicht von internationalen Datentransfers besitzen, ist dies nunmehr nachzuholen und zu dokumentieren.

Bei der Übermittlung von Daten in die USA und in andere „unsichere" Drittländer bleibt die Prüfung des angemessenen Datenschutzniveaus darüber hinaus weiterhin aufrecht. Hierzu hat der Europäische Datenschutzausschuss Empfehlungen für zusätzliche Klauseln verfasst, die gemeinsam mit den neuen SCCs implementiert werden sollten.

3. Datenschutz post-Brexit

Der Brexit hat für einige Baustellen im Rechts- und Wirtschaftsverkehr gesorgt. Eine wesentliche offene Frage bleibt die Anwendbarkeit der DSGVO und des britischen nationalen Datenschutzrechts im internationalen Datenverkehr. Seit 31. Jänner 2020 ist das Vereinigte Königreich bekanntlich aus der EU ausgetreten. Die EU-Kommission hatte sich zum Ziel gesetzt, zeitnah mit einem sog. „**Angemessenheitsbeschluss**" zu reagieren, um Datentransfers nach Großbritannien wie in sichere Drittländer (zB Kanada, Japan etc.) zu behandeln. Dieser ist nun fast ein halbes Jahr seit dem Brexit auch dringend nötig, denn zum gegenwärtigen Zeitpunkt gilt noch eine Übergangsfrist bis zum bis **30. Juni 2021**, der den Datenaustausch von EU-Unternehmen mit Großbritannien noch zu den gleichen Bedingungen wie vor dem Brexit behandelt.

Formal gesehen bleiben daher nur noch wenige Wochen Zeit, um zu klären, wie mit Datenströmen über den Ärmelkanal umzugehen ist.

[1] Englische Version: https://ec.europa.eu/info/sites/default/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf

Was müssen Unternehmen, die Daten nach Großbritannien übermitteln, künftig beachten?

Für die Datenübermittlungen aus Großbritannien Richtung EU hat sich formal nichts geändert, da hier die DSGVO weiterhin territorial und sachlich anwendbar bleibt. Neu ist jedoch, dass Unternehmen nun verpflichtet sind, einen sog. **Vertreter gem. Art. 27 DSGVO** zu bestellen, wenn keine eigene britische Tochtergesellschaft in der Union existiert.

Der Status quo

Die EU-Kommission hält sich bisher zu ihrem vorgeschlagenen Angemessenheitsbeschluss (wie berichtet in DSG-Info 97) bedeckt. Dieser ist seit Februar veröffentlicht und zur Konsultation an die Mitgliedsstaaten und den Europäischen Datenschutzausschuss übermittelt worden. Das Europäische Parlament hat massive Bedenken an der sicheren Behandlung von Daten der EU-Bürger im Zusammenhang mit dem Zugriff von Geheimdiensten und Sicherheitsbehörden geäußert. Es handelt sich um ein ähnliches Problem, das damals schon zum Fall des **Privacy Shield Abkommens** geführt hat.

Auch der **Europäische Datenschutzausschuss** hat in seiner Stellungnahme Kritik über den vorgeschlagenen Angemessenheitsbeschluss geäußert. Zum einen sei nicht geregelt, wie weitergehende Übermittlungen aus Großbritannien Richtung Drittstaaten wie die USA reguliert werden, um insbesondere das Schrems-II-Erkenntnis nicht zu konterkarieren. Weiters ist das britische Datenschutzrecht durch seinen nationalstaatlichen Charakter wesentlich einfacher abzuändern und bedarf daher eines konstanten Monitorings, da die Tendenzen in Richtung eines Datenschutzrechts zugunsten der staatlichen Überwachung und des Zugriffs durch Sicherheitsbehörden gehen. Letztlich ist es auch der konkrete Eingriff von Geheimdiensten und Sicherheitsbehörden in Migrationsfragen, der die Bedenken des EP und EDSA nährt.

Der Kommission bleibt nicht mehr viel Zeit, auf die Kritik des EP und des Datenschutzausschusses zu reagieren. Sollte es zu keiner Einigung kommen und gegenüber Großbritannien kein ausreichendes Datenschutzniveau festgestellt werden, müssen Unternehmen ihre Verträge zum 1. Juli 2021 anpassen und die oben erwähnten SCCs in Erwägung ziehen. Der Datentransfer ist dann nicht ohne zusätzliche Bedingungen (zB Abschluss von Standardvertragsklauseln oder Binding Corporate Rules) zulässig.

4. Koordiniertes Vorgehen zu internationalen Datentransfers

Die deutschen Aufsichtsbehörden haben sich zu einer „koordinierten Aktion" zur Überprüfung der Vorgaben aus dem Schrems-II-Erkenntnis zusammengeschlossen. Mehrere Behörden (Berlin, Brandenburg, Bayern, Niedersachsen, Baden-Württemberg, Bremen, Hamburg, Rheinland-Pfalz, Saarland) verschicken nun Fragebögen, die der Prüfung internationaler Datentransfers dienen soll. Die Fragebögen finden Sie unter anderem hier:

- Bewerberportale
- Konzerninterner Datenverkehr
- Mailhoster
- Tracking
- Webhoster

Betroffen sind zunächst nur in Deutschland ansässige Unternehmen, allerdings ist auch aus österreichischer Sicht vor allem in Konzernverhältnissen mit Prüfmaßnahmen zu rechnen. Es ist Unternehmen im Lichte der aktuellen Entwicklungen im internationalen Datentransfer besonders angeraten, auf korrekte Abläufe und

Dokumentationen zu achten, um hier im Falle einer Kontaktaufnahme schnell Antworten liefern zu können.

Sollten Sie Unterstützung bei der Dokumentation oder dem Abschluss zusätzlicher Maßnahmen benötigen, stehen wir Ihnen zur Verfügung. Die Fragebögen können auch einen Anlassfall zur eigenen Überprüfung der „Schrems-II"-Compliance sein.

5. Verstärkte Kontrollen beim Einsatz von Cookies

Die Datenschutz-NGO NOYB hat über 500 Unternehmen Beschwerden im Zusammenhang mit dem Einsatz von Cookies geschickt. Aus Sicht der Datenschutzaktivisten ist es unzulässig, dass Cookie-Banner mit „Nudging" oder anderen Mitteln Nutzer von der Ablehnung abhalten sollen. Die NGO hat hierfür sogar eine Software entwickelt, die automatisch Beschwerden generiert, wenn Besuchern auf der Website mehr als nur ein Opt-in abverlangt wird bzw. eine Behinderung bei der Entscheidungswahl vorliegt.

Seit der Entscheidung des EuGH in der RS. Planet49 ist der Einsatz von Cookies ausschließlich mittels einer aktiv erteilten, informierten und bestimmten Einwilligung des Nutzers zulässig. Dies fußt zum einen auf der telekommunikationsrechtlichen Grundlage der e-Privacy-RL, die in Österreich in § 96 Abs. 3 TKG umgesetzt worden ist, zum anderen auf der DSGVO, die in Bezug auf Werbung und Tracking eine Einwilligung verlangt. In diesem Zusammenhang betont die DSB auch ihre ausdrückliche Zuständigkeit[2], trotz e-Privacy-RL, da jede „denkmögliche Verletzung des Rechts auf Geheimhaltung nach § 1 Abs. 1 DSG " unabhängig vom Telekommunikationsrecht in ihren Aufgabenbereich fällt.

Als weitere Problematik gestaltet sich die datenschutzrechtliche Rollenverteilung von komplexen Tracking-Systemen, die durch Anbieter zu riesigen Datenpools angereichert und weiterverarbeitet werden. Die vergebenen Cookie-IDs werden durch einige Anbieter wechselseitig über Websites hinweg getrackt, ermöglichen umfassendes Profiling, und erzeugen unter Umständen für Website-Betreiber und Anbieter eine Joint-Controllership-Situation, der vertraglich und datenschutzrechtlich begegnet werden muss.

Unabhängig davon liegen oftmals auch internationale Datentransfers vor, die unter den obigen Gesichtspunkten einen Abschluss von SCCs notwendig machen. Unternehmen sollten darauf achten, dass sie unter anderem diese Grundsätze der Cookie-Nutzung einhalten:

- Cookies sollten erst nach bejahender Entscheidung des Nutzers gesetzt werden
- Entscheidung des Nutzers muss informiert, freiwillig und aktiv erfolgen
- das Cookie-Banner darf nicht irreführend sein
- die Datenschutzinformation muss transparent und verständlich sein
- der Widerruf muss jederzeit grundlos möglich sein
- Cookies sollten datenschutzfreundlich voreingestellt sein

[2] DSB, 30. 11. 2018, D122.931/0003 DSB/2018 – derStandard.at/Cookiewall.

6. Zwei EuGH-Verfahren aus Österreich – Auskunft und Schadenersatz

1. Welchen Umfang hat eine Auskunftserteilung?

OGH 18.02.2021, 6 Ob 159/20f

EuGH C-154/21

Die Beklagte ist ein österreichischer Adressverlag. Der Kläger ersuchte die Beklagte am 15. Jänner 2019 unter Verweis auf Art. 15 DSGVO um Auskunft darüber, welche personenbezogenen Daten über ihn in der Vergangenheit gespeichert wurden, sowie um Information, wo die Speicherung dieser Daten erfolgt. Weiters wollte er wissen, ob es zu einer Weitergabe seiner Daten gekommen ist und wer die konkreten Empfänger gewesen seien.

Die Antwort des Adressverlags über die Übermittlungsempfänger der Daten des Klägers fiel pauschal aus. Insgesamt seien die Daten an „*werbetreibende Unternehmen im Versandhandel und stationären Handel, IT Unternehmen, Adressverlage und Vereine wie Spendenorganisationen, NGOs oder Parteien*“ übermittelt worden. Diese Antwort reichte dem Kläger nicht aus und er begehrte in drei Instanzen hinweg die konkrete Offenlegung der Empfänger mit Verweis auf das Recht auf Auskunft gem. **Art. 15 Abs. 1 lit. c DSGVO**.

Der OGH setzte das Verfahren aus und legte die Frage über den Umfang des Auskunftsrechts dem EuGH vor. Dieser hat nun zu bewerten, in welchem Ausmaß das Auskunftsrecht gem. Art. 15 DSGVO besteht. Offen ist also, ob es ausreicht „**Kategorien von Empfängern**“ zu benennen oder im Auskunftsfall **alle tatsächlichen Empfänger** anzugeben.

Die konkrete Vorlagefrage lautet: „*Ist Art 15 Abs 1 lit c […] dahingehend auszulegen, dass sich der Anspruch auf die Auskunft über Empfängerkategorien beschränkt, wenn konkrete Empfänger bei geplanten Offenlegungen noch nicht feststehen, der Auskunftsanspruch sich aber zwingend auch auf Empfänger dieser Offenlegungen erstrecken muss, wenn Daten bereits offengelegt worden sind?*“

Die DSB sieht in der Interessenabwägung zwischen Geheimhaltungspflichten und Recht auf Auskunft zwar ein Spannungsverhältnis, bejaht jedoch grundsätzlich die konkrete Benennung der Übermittlungsempfänger. In der Sache hat sich auch der OGH bejahend zu einer umfassenden Offenlegung geäußert und verweist auf ErwG 63 der DSGVO sowie den Schutzzweck der Norm, über die Datenverarbeitung informiert zu werden.

Das Verfahren wird unter der Aktenzahl **EuGH C-154/21** geführt.

2. Welchen Bewertungsgrundlagen unterliegt immaterieller Schadenersatz?

OGH 15.04.2021, 6 Ob 35/21x

Ein Adressverlag hatte eine Vielzahl von Daten betroffener Personen mittels statistischer Hochrechnungen u.a. auch als Affinität zu politischen Parteien zugeordnet. Dies geschah zunächst ohne Kenntnis oder Einwilligung der betroffenen Personen. Die vorgenommenen statistischen Hochrechnungen sind im Frühjahr des Jahres 2019 durch das Geltendmachen von Auskunftsbegehren vereinzelt an die Betroffenen bekannt gemacht worden. So wurden einige Personen politischen Parteien zugeordnet, ohne dass sie sich mit diesen tatsächlich identifizierten. Dem Kläger wurde im gegenständlichen Verfahren, ohne dass er eine Einwilligung zur Datenverarbeitung erteilt hatte, eine hohe Affinität zur Partei „FPÖ“ zugeschrieben. Nicht nur die Zuordnung, sondern auch die Speicherung und Weitergabe seiner Daten, die ihm seitens der Beklagten zugeschriebenen wurden, haben den Kläger „verärgert, erbost und beleidigt“. Aus diesem

Grund klagte er den Adressverlag auf den Ersatz dieses immateriellen „Gefühls"-Schadens im Zusammenhang mit der unrechtmäßigen Datenverarbeitung.

Der Oberste Gerichtshof setzte auch dieses Verfahren aus und legte dem EuGH Fragen zur Auslegung und Anwendung des in Art. 82 DSGVO geregelten Schadenersatzanspruchs vor.

Die konkreten Vorlagefragen lauten:

„1. Erfordert der Zuspruch von Schadenersatz nach Art 82 DSGVO (Verordnung [EU] 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Datenschutz-Grundverordnung]) neben einer Verletzung von Bestimmungen der DSGVO auch, dass der Kläger einen Schaden erlitten hat oder reicht bereits die Verletzung von Bestimmungen der DSGVO als solche für die Zuerkennung von Schadenersatz aus?

2. Bestehen für die Bemessung des Schadenersatzes neben den Grundsätzen der Effektivität und Äquivalenz weitere Vorgaben des Unionsrechts?

3. Ist die Auffassung mit dem Unionsrecht vereinbar, dass Voraussetzung für den Zuspruch immateriellen Schadens ist, dass eine Konsequenz oder Folge der Rechtsverletzung von zumindest einigem Gewicht vorliegt, die über den durch die Rechtsverletzung hervorgerufenen Ärger hinausgeht?"

Im Wesentlichen können die drei Vorlagefragen folgendermaßen zusammengefasst werden:

1. DSGVO-Verstoß = Schadenersatzanspruch?

Ist ein Verstoß gegen die DSGVO ausreichend, um einen Schadenersatzanspruch zu bejahen, ohne dass ein konkreter Schaden vorliegt?

2. Strafschadenersatz und Bagatellgrenzen?

Welche unionsrechtlichen Anforderungen bestehen an die Bemessung eines Schadenersatzes neben den Grundsätzen der Effektivität und Äquivalenz?

3. Erheblichkeitsschwelle?

Welche Erheblichkeit benötigt der Zuspruch eines immateriellen Schadens in der Gemüts- und Gedankenwelt eines Betroffenen?

Das Thema trifft im Kern auch eine deutsche Vorlagefrage des dt. Bundesverfassungsgerichts[3]. Im dortigen Verfahren geht es um die Frage, ob das Erreichen einer Erheblichkeitsschwelle (in concreto hier ein unrechtmäßiges Werbe-E-Mail) Voraussetzung für einen ersatzfähigen immateriellen Schaden nach Art. 82 DSGVO ist.

7. EU schlägt digitale Europäische E-Identität und eWallet vor

Um sich im Internet ausreichend zu authentifizieren, bestehen unterschiedliche Möglichkeiten und Wege. Oftmals wird das sog. Single-Sign-On mittels Plugin wie beispielsweise von Facebook, LinkedIn oder Google genutzt, um ein Nutzerkonto zu erstellen, ohne sich neu registrieren zu müssen. Die Dienste verifizieren den Nutzer über die Verknüpfung des Nutzerkontos auf Facebook mit dem neuen Anbieter. Dies führt allerdings auch dazu, dass diese Dienste stets Kenntnis über bestehende Verknüpfungen und möglicherweise auch ausgetauschte Daten erhalten können. Mit dem Vorschlag der EU-Kommission für eine

[3] BVfG 14. Januar 2021 - 1 BvR 2853/19.

Europäische Digitale Identität möchte die EU diesen Social Plugins eine institutionelle Konkurrenz machen.

Die Kommission hat am 3. Juni 2021 ihren Vorschlag für eine Verordnung zum Aufbau eines Rahmens für eine Europäische Digitale Identität (EU-ID-Rahmen) vorgestellt. Anhand der nationalen digitalen Identifizierung sollen europaweit Online-Dienste genutzt werden können, ohne dabei auf private Identifizierungsmethoden zugreifen zu müssen oder nicht notwendige personenbezogene Daten weiterzugeben. Dabei sollen die Mitgliedstaaten verpflichtet werden, Bürgern sowie Unternehmen eine sog. digitale Brieftasche (**e-Wallet**) zur Verfügung zu stellen. In diesem „digitalen Börserl" kann dann die nationale digitale Identität mit Nachweisen wie Führerschein, Zeugnissen u.ä. verknüpft werden. Die Nutzung stellt lediglich ein Angebot dar und bleibt für Bürger freiwillig.

Im Sinne einer raschen Umsetzung soll unverzüglich mit den Vorarbeiten begonnen werden. Vor diesem Hintergrund hat die EU-Kommission parallel zum Verordnungsvorschlag eine Empfehlung vorgelegt, in der sie die Mitgliedstaaten auffordert, bis September 2022 ein gemeinsames Instrument zu schaffen. Dieses Instrument soll die technische Architektur, Normen, Leitlinien und bisherige Best-Practices umfassen und bis Oktober 2022 veröffentlicht werden.

8. In eigener Sache

Wir möchten die Gelegenheit nutzen, mit Ihnen auch eine „persönliche Bilanz" zu drei Jahren DSGVO bei der Secur-Data zu teilen. Im Jahr 2020 haben wir unsere Website vollständig umgestaltet und arbeiten weiter an einem verbesserten Webauftritt für unsere Kunden. Darüber hinaus bieten wir mittlerweile in der Praxis erprobte und nachhaltige **Löschkonzepte** an, die an die aktuelle Rechtsprechung zu gesetzlichen Fristen und Aufbewahrungsdauer angepasst werden und für Unternehmen jeder Größe geeignet sind. Darüber hinaus wurde ein detaillierter **Datenschutz-Compliance-Check** entwickelt, der insgesamt 13 Prüffelder umfasst, für die wir umfangreiche Prüffragen entwickelt haben, so gibt es zB einen eigenen **Website-Compliance-Check**.

Angesichts der sich stetig veränderten Rechtslage ist das Thema Schulung und Weiterbildung im Datenschutz unerlässlich. Daher haben wir unser bekanntes **Datenschutzhandbuch** für Mitarbeiter erweitert und werden im Spätsommer wieder **Fortbildungen und Seminare** anbieten können.

••••