Republik Österreich
Datenschutzbehörde

NEWSLETTER 4/2020

# Amtswegige Datenschutzüberprüfung von Kundenbindungsprogrammen

**Dr. Andreas Zavadil**

Die Datenschutzbehörde hat amtswegige Prüfverfahren zu den Verfahrenszahlen DSB-D213.895 und DSB-D213.983 gegen zwei unterschiedliche Verantwortliche von größeren Kundenbindungsprogrammen aus Österreich geführt. Im Rahmen der Verfahren wurde (neben weiteren Aspekten) die Einhaltung der in der DSGVO normierten Transparenz- und Informationspflichten im Zusammenhang mit der Einholung einer datenschutzrechtlichen Einwilligung überprüft.

Den Verfahren war gemeinsam, dass die Verantwortlichen jeweils ein unternehmens- sowie branchenübergreifendes Kundenbindungsprogramm betreiben, an dem verschiedene Unternehmen aus der Privatwirtschaft teilnehmen können. Bei den Verantwortlichen handelte es sich jeweils um die Betreiber des Programms, denen insbesondere die Mitgliedsverwaltung (und die damit verbundene Datenverarbeitung) zukommt. Ebenso war den Verfahren gemeinsam, dass die Verantwortlichen unterschiedliche Kanäle verwenden (Webpage, App, physischer „Flyer", der in Filialen von Partnern der Verantwortlichen aufliegt), um die Anmeldung zum Programm durchzuführen. Zeitgleich wird im Rahmen dieser Anmeldung auch um Einwilligung ersucht, dass erhobene Daten – vereinfacht formuliert – zum Zwecke der personalisierten Werbung (also Profiling) sowie zu weiteren Analysezwecken verwendet werden können. Die Datenschutzbehörde hat diese Ersuchen um Einwilligung sowie die jeweiligen Kanäle überprüft.

Diesbezüglich war zunächst festzuhalten, dass an die Erfüllung der Kriterien von Art. 4 Z 11 und Art. 7 DSGVO ein hoher Maßstab anzulegen ist. Dies erhellt neben der einschlägigen Judikatur des EuGH insbesondere aus der Überlegung, dass der europäische Gesetzgeber – anders noch als in der Richtlinie 95/46/EG, in der dies bloß rudimentär geregelt war – sich dazu entschlossen hat, Anforderungen an eine datenschutzrechtliche Einwilligung in einer eigenen Bestimmung gemäß Art. 7 DSGVO zu normieren; darüber hinaus ist eine „Verletzung der Bedingungen für die Einwilligung" in Art. 83 Abs. 5 lit. a DSGVO ausdrücklich als Straftatbestand genannt, womit der hohe Stellenwert der Kriterien nochmals bekräftigt wird.

Weiters war festzuhalten, dass man sich bei der Überprüfung datenschutzrechtlicher Einwilligungserklärungen in die Rolle eines durchschnittlichen Betroffenen versetzen muss, der den Anmeldeprozess mit durchschnittlicher Aufmerksamkeit durchläuft und der über keine juristischen oder technischen Kenntnisse verfügt. Dies ergibt sich sowohl aus den einschlä-

gigen Leitlinien der ehemaligen Art. 29-Datenschutzgruppe (vgl. WP259 rev.01, 17/DE, S. 16), als auch aus der Judikatur des EuGH zum Verbraucherschutzrecht (vgl. C-210/96, Gut Springenheide GmbH, Rn 37), die auf datenschutzrechtliche Einwilligungserklärungen übertragbar ist (so verweist ErwGr 42 DSGVO im Zusammenhang mit Einwilligungserklärungen auf die Verbraucherschutz-Richtlinie 93/13/EWG).

Unter Berücksichtigung dieser Überlegungen war zunächst der physische „Flyer" zu überprüfen. Das Ersuchen um Einwilligung war von beiden Verantwortlichen am Ende des Anmeldeformulars zum Kundenbindungsprogramm platziert. In diesem Zusammenhang ist zwar festzuhalten, dass die Verantwortlichen jeweils darauf hinweisen, dass es sich hierbei um eine datenschutzrechtliche Einwilligung handelt und dass die Abgabe dieser Einwilligung nicht für die Anmeldung erforderlich ist. Allerdings ist dieser Hinweis nach Auffassung der Datenschutzbehörde nicht deutlich genug hervorgehoben, sondern befindet sich dieser bloß unauffällig unter- bzw. oberhalb der Unterschriftenzeile. Ebenso – und dies war der entscheidende Punkt – wird ein durchschnittlicher Betroffener bei einem Unterschriftenfeld, das am Ende eines Anmeldeformulars zum Kundenbindungsprogramm platziert ist, davon ausgehen, dass es sich hierbei um eine Unterschrift zur Anmeldebestätigung zum Programm (und nicht etwa um eine datenschutzrechtliche Einwilligung zum Profiling) handelt.

Ebenso wurde die Webpage überprüft. Die Webpage der Verantwortlichen – samt den dazugehörigen Ersuchen um Einwilligung – war im Detail unterschiedlich gestaltet. Als gemeinsamer Nenner lässt sich jedoch festhalten, dass aufgrund der Gesamtkonzeption der Ersuchen ebenso wenig von einer DSGVO-Konformität auszugehen war. Dies insbesondere deshalb, da nach Auffassung der Datenschutzbehörde beim Drücken der „Einwilligungsbuttons" vordergründig auf die Vorteile verwiesen wurde, nicht jedoch hinreichend klar darauf, dass es sich hierbei um eine Einwilligung zum Zwecke des Profiling (und mehr) handelt. Bei der Webpage eines Verantwortlichen kam hinzu, dass der „Button" zur Abgabe einer Einwilligung zeitgleich der Bestätigung der Registrierung diente. Aufgrund dieser Doppelfunktion einer Aktion kann nach Auffassung der Datenschutzbehörde aber nicht von einer unmissverständlichen Einwilligung ausgegangen werden, da unklar bleibt, ob der Betroffene nicht doch lediglich den Anmeldeprozess abschließen wollte (vgl. zur Doppelfunktion von Aktionen auch GA 21. März 2019, C-673/17, Planet 49, Rn 89).

Zwar ist hervorzuheben, dass die Verantwortlichen ihren Informationspflichten nach Art. 13 f DSGVO zwar grundsätzlich nachgekommen sind. Allerdings hat die (an anderer Stelle befindliche) Datenschutzerklärung in den vorliegenden Fällen nichts dazu beigetragen, dass der Abschnitt, in dem die Einwilligung dann tatsächlich eingeholt wird, für den Betroffenen transparenter wird.

Die App des einen Verantwortlichen war hingegen datenschutzkonform: Anders als bei den zu beanstandenden anderen Methoden (Webseite und physischer „Flyer") wird in der App durch einen Screen-für-Screen-Anmeldeprozess sichergestellt, dass sich das Ersuchen um Einwilligung dadurch vom übrigen Anmeldeprozess deutlich abhebt, indem dieses in einem eigenständigen Anmeldeschritt (ohne weitere Elemente) dargestellt wird und einen großen sowie deutlichen Hinweis auf „Profiling" und „Einwilligung" beinhaltet. Eine Überprüfung der App des anderen Verantwortlichen ist noch ausständig.

Da die Ersuchen um Einwilligung nicht den Anforderungen der Verordnung entsprechen, sind diese gemäß Art. 7 Abs. 1 DSGVO unverbindlich und können nicht als Rechtsgrundlage für das Profiling (und mehr) herangezogen werden. Ein nachträgliches „Ändern" der Rechtsgrundlage – insbesondere auf berechtigte Interessen – kommt nach Auffassung der Datenschutzbehörde nicht in Betracht.

Dies insbesondere deshalb, da sich die Verantwortlichen gegenüber den Betroffenen ausschließlich auf die Einwilligung als Rechtsgrundlage gestützt haben (vgl. Art. 13 Abs. 1 lit. c und lit. d DSGVO). Würde man anstelle der Einwilligung im Nachhinein nun eine Ersatzrechtsgrundlage heranziehen können, so würde man das Recht auf Widerruf der Einwilligung konterkarieren, da der Betroffene diesfalls die Datenverarbeitung – so wie bei der Anmeldung suggeriert – nicht mehr einseitig mit Widerruf der Einwilligung beenden kann. Zwar mag es Ausnahmefälle geben, bei denen diese Argumentation nicht fruchtbar ist (etwa, wenn die Einwilligung widerrufen wird, die Datenverarbeitung aber dennoch für einen Gerichtsprozess benötigt wird). Von Art. 17 Abs. 1 lit. b DSGVO nicht umfasst ist aber die gegenständliche Konstellation, in welcher eine Ersatzrechtsgrundlage bloß deshalb „ersatzweise" ins Treffen geführt wird, weil der Verantwortliche ein unzulässiges Ersuchen um Einwilligung formuliert hat.

Im Ergebnis war daher bescheidmäßig auszusprechen, dass die herangezogenen Ersuchen um Einwilligung in dieser Form nicht mehr verwendet werden mögen und wurde weiters die bis dato erfolgte Datenverarbeitung (auf Grundlage der unzulässigen Einwilligungsersuchen) für unrechtmäßig erklärt. Den Verantwortlichen wurde eine Frist zur Anpassung ihrer entsprechenden Datenprozesse eingeräumt. Gegen beide Bescheide wurde Beschwerde erhoben. Es darf um Verständnis ersucht werden, dass eine Veröffentlichung oder Übermittlung der Bescheide mangels Rechtskraft nicht vorgesehen ist.

## Im Fokus

Dr. Andreas Zavadil

**Datenschutzrechtliche Zulässigkeit des „AMS-Algorithmus“**

Mit Bescheid vom 16. August 2020, Verfahrenszahl DSB-D213.1020, setzte sich die Datenschutzbehörde mit der datenschutzrechtlichen Zulässigkeit des sogenannten „AMS-Algorithmus“ auseinander.

Bei diesem handelt es sich um ein Arbeitsmarktchancen Assistenz-System (in Folge: „AMAS“). Das AMAS soll laut Angaben des AMS (als datenschutzrechtlicher Verantwortlicher) seine BeraterInnen – vereinfacht formuliert – bei der Einschätzung der Arbeitsmarktchancen von Arbeitssuchenden unterstützen (Chancenmodell) und soll eine effizientere Einsetzung der Ressourcen der Verantwortlichen gewährleisten. Bei diesem Chancenmodell werden die Wahrscheinlichkeiten (niedrig, mittel, hoch) für aktuell vorgemerkte KundInnen des AMS (Arbeitssuchende) innerhalb eines bestimmten Zeitraums berechnet, in der Zukunft eine bestimmte Anzahl von Tagen beschäftigt zu sein. Die berechneten Wahrscheinlichkeiten können von den BeraterInnen verwendet werden, um passende weitere Maßnahmen mit den KundInnen zu vereinbaren bzw. zu setzen (etwa Weiterbildungsmöglichkeiten).

Im Rahmen der Berechnung werden folgende Datenkategorien verwendet: Altersgruppe, Geschlecht, Staatengruppe, Ausbildung, Gesundheitliche Beeinträchtigungen, Betreuungspflichten, Berufsgruppe, Vorkarriere, regionales Arbeitsmarktgeschehen und Dauer des Geschäftsfalls beim AMS.

Zuallererst war festzuhalten, dass die unter Zuhilfenahme des AMAS erfolgte Datenverarbeitung im Rahmen der Wahrnehmung der dem Verantwortlichen gemäß § 1 Abs. 1 AMSG übertragenen öffentlichen Aufgabe erfolgt. Als Behörde ist es erforderlich, dass sich eine Datenverarbeitung – und damit verbunden, der Eingriff in das Grundrecht auf Datenschutz – nicht bloß auf eine gesetzliche Ermächtigung gründet, die gesetzliche Ermächtigung muss vielmehr hinreichend determiniert bestimmen, unter welchen Voraussetzungen ein Eingriff in das Grundrecht auf Datenschutz zulässig ist (vgl. etwa VfSlg. 18146/2007). Es obliegt der Datenschutzbehörde, zu überprüfen, ob eine Datenverarbeitung Deckung in gesetzlichen Bestimmungen findet.

Das AMS hat sich im Hinblick auf die Datenverarbeitung auf die Rechtsgrundlage gemäß §§ 25 Abs. 1, 29 und 31 Abs. 5 AMSG gestützt. Es stellte sich die Frage, ob diese angeführte Rechtsgrundlage dem Determinierungsgebot von Gesetzen entspricht. So muss die Rechtsgrundlage der Datenverarbeitung nämlich sowohl nach der Judikatur des VfGH 29.11.2017, G 223/2016 mwN) sowie nach dem Verständnis des europäischen Verordnungsgebers (vgl. ErwGr 41 zweiter Satz DSGVO) klar und präzise sowie ihre Anwendung für die Rechtsunterworfenen vorhersehbar sein.

Davon ausgehend war in Folge festzuhalten, dass für den Rechtsunterworfenen zwar sicherlich nachvollziehbar ist, dass das AMS einige – in § 25 Abs. 1 AMSG aufgezählte – Datenarten zwangsläufig verarbeiten muss, damit gewisse Leistungen (beispielsweise die Bearbeitung eines Antrags für den Bezug von gewissen Leistungen aus der Arbeitslosenversicherung) erbracht werden können. Nach Auffassung der Datenschutzbehörde nicht nachvollziehbar wird es für den Rechtsunterworfenen hingegen sein, allein auf Grundlage von § 25 Abs. 1 AMSG – selbst wenn man diesen im Lichte der §§ 29 und 31 Abs. 5 leg. cit. auslegt – davon auszugehen, dass die in § 25 Abs. 1 leg. cit. genannten Datenarten zum Zwecke der Bewertung von Arbeitsmarktchancen (also Profiling) verarbeitet werden.

Einzuräumen war, dass nicht jede einzelne Verarbeitungstätigkeit einer Behörde abschließend gesetzlich angeführt werden kann. Eine Generalermächtigung für die Datenverarbeitung, wie in den §§ 25 ff AMSG vorhanden, kann nach Auffassung der Datenschutzbehörde aber nicht dazu führen, dass ein derart vergleichsweise großer Eingriff in das Grundrecht auf Datenschutz gerechtfertigt ist. Vielmehr ist bei dem Bestimmtheitsgrad, der an solche Gesetze anzulegen ist, auch der (der DSGVO inhärente) risikobasierte Ansatz zu berücksichtigen. Mit anderen Worten: Je größer der Eingriff in das Grundrecht auf Datenschutz ist, umso klarer muss dieser Eingriff für den Betroffenen vorhersehbar sein und umso strenger wird der Maßstab für die Determiniertheit der entsprechenden Rechtsgrundlage.

Dies ergibt sich insbesondere auch aus einer systematischen Betrachtung der DSGVO. Der europäische Verordnungsgeber geht nämlich davon aus, dass es sich beim Profiling um eine derart spezifische Verarbeitungsform handelt, sodass mit der allgemeinen Begriffsdefinition der „Verarbeitung“ in Art. 4 Z 2 DSGVO nicht das Auslangen gefunden werden konnte und dass der Begriff „Profiling“ nochmals spezifisch in Art. 4 Z 4 leg. cit. zu bestimmen war. Wenn nun der europäische Verordnungsgeber eine solche Differenzierung (allgemeine Verarbeitung und spezifische Verarbeitung in Form von Profiling) trifft, so muss dieser Maßstab auch für nationale Gesetze gelten, auf deren Grundlage ein solches Profiling durchgeführt wird.

All diese Überlegungen finden auch in Art. 21 DSGVO Deckung. Denn wenn eine Rechtsgrundlage nicht klar und präzise sowie für den Betroffenen vorhersehbar ist (vgl. ErwGr 41 zweiter Satz DSGVO), so ist es ihm unmöglich, seine „besondere Situation“ im Rahmen des

relativen Widerspruchrechts nach Art. 6 Abs. 1 lit. e iVm Art. 21 Abs. 1 DSGVO darzulegen.

Im gegenständlichen Fall wurde auch die aktuelle Ausnahmesituation rund um COVID-19 berücksichtigt. So ist nach Auffassung der Datenschutzbehörde aufgrund der steigenden Ressourcenbelastung des AMS sowie des Umstands, dass persönliche Gespräche (regionsbedingt) nicht mehr stattfinden (und somit der „persönliche Eindruck" der BeraterInnen nicht gegeben ist) davon auszugehen, dass die Rechenergebnisse des AMAS weitgehend bloß unhinterfragt übernommen werden. Weiters ist davon auszugehen, dass der Mensch (also BeraterInnen) durch derartige Rechenergebnisse in seiner Entscheidung jedenfalls zu einem derart hohen Grad beeinflusst wird, dass durch diese Datenverarbeitung von einer „erheblichen Beeinträchtigung" iSd Art. 22 Abs. 1 DSGVO auszugehen ist, selbst wenn die Rechenergebnisse des AMAS nicht bloß unhinterfragt übernommen werden. Es ist daher auch von einer Anwendbarkeit der Schutzbestimmungen des Art. 22 DSGVO auszugehen.

Vor dem Hintergrund dieser Überlegungen war davon auszugehen, dass für die Datenverarbeitung im Zusammenhang mit dem AMAS keine (ausreichende) Rechtsgrundlage (samt notwendigen, gesetzlichen Schutzgarantien) besteht. Die Datenverarbeitung war daher mit Wirkung vom 1. Jänner 2021 zu untersagen, sofern bis zu diesem Zeitpunkt keine geeignete Rechtsgrundlage für die Datenverarbeitung durch den Gesetzgeber geschaffen wird. Die aufschiebende Wirkung einer Bescheidbeschwerde wurde ausgeschlossen. Gegen diesen Bescheid wurde Beschwerde erhoben. Es darf um Verständnis ersucht werden, dass eine Veröffentlichung oder Übermittlung des Bescheids mangels Rechtskraft nicht vorgesehen ist.

## Ausgewählte Entscheidungen der DSB

### 2020-0.396.410 (D124.2061), Auskunftsrecht eines gerichtlich bestellten psychologischen Sachverständigen

Im Bescheid vom 29. Juni 2020, GZ: 2020-0.396.410 (D124.2061), hatte sich die DSB mit dem Auskunftsrecht eines gerichtlich bestellten psychologischen Sachverständigen zu beschäftigen.

Der Beschwerdegegner wurde vom zuständigen Landesgericht für Strafsachen im Verfahren gegen den Beschwerdeführer als psychologischer Sachverständiger bestellt und mit der Erstellung eines Gutachtens zum Beschwerdeführer beauftragt. Nach der Übermittlung des Gutachtens an das Landesgericht, wandte sich der Beschwerdeführer mit einem Auskunftsbegehren an den Beschwerdegegner. Der Beschwerdegegner kam dem Auskunftsbegehren nicht nach, sondern verwies darauf, dass er als gerichtlich bestellter Sachverständiger funktioneller Teil der Rechtspflege sei, weshalb auch die Strafprozessordnung auf ihn anzuwenden wäre. Die Strafprozessordnung würde Parteien die Gelegenheit zur Akteneinsicht geben, eine Akteneinsicht beim Gutachter sei hingegen nicht vorgesehen.

Die Datenschutzbehörde verwies in ihrer Entscheidung zunächst auf die Judikatur des Bundesverwaltungsgerichts, wonach gerichtlich beeidete Sachverständige zumindest gemeinsam mit dem Gericht, das sie mit der Gutachtenserstellung beauftragt hat, als Verantwortliche im Sinne des Art. 4 Z 7 DSGVO zu betrachten sind (vgl. das Erkenntnis des BVwG vom 27. September 2018, GZ W214 2196366-2). Die Datenschutzbehörde verwies sodann darauf, dass die Bestellung des Beschwerdegegners zwar im Rahmen eines anhängigen Strafverfahrens geschehen sei, allerdings bei der Gutachtenerstellung von keiner „justiziellen Tätigkeit" ausgegangen werden kann, weshalb die Datenschutzbehörde auch zur Entscheidung zuständig ist. Während in der DSGVO Daten in Patientenakten, Informationen wie Diagnosen, Untersuchungsergebnisse oder Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen ausdrücklich vom Recht auf Auskunft als umfasst angesehen werden, hat der österreichische Gesetzgeber im Psychologengesetz 2013 keine Beschränkung für das Recht auf Auskunft vorgesehen. Da die DSGVO auch keine Einschränkung des Rechts auf Auskunft zugunsten eines gesetzlich normierten (Akten)Einsichtsrechts vorsieht, kam die Datenschutzbehörde zum Ergebnis, dass der Beschwerdegegner gegenüber dem Beschwerdeführer zur Auskunftserteilung verpflichtet ist und der Beschwerdegegner dem Beschwerdeführer eine dem Art. 15 DSGVO entsprechende Auskunft zu erteilen hat.

Der Bescheid ist in Rechtskraft erwachsen.

### 2020-0.225.643 (D124.2138), Einreichen der Originalrechnungen einer Apotheke, um in den Genuss einer Versicherungsleistung zu kommen

Mit Bescheid vom 12. Juni 2020, GZ: 2020-0.225.643 (D124.2138), hatte sich die Datenschutzbehörde mit einer Beschwerde im Recht auf Geheimhaltung (§ 1 DSG) auseinanderzusetzen.

Der Beschwerdeführer hat als Landesbeamter eine Zusatzversicherung bei der Beschwerdegegnerin. Die Beschwerdegegnerin, ein österreichisches Versicherungsunternehmen, verlangte für die Leistungserbringung die Übermittlung der Apothekenbelege im Original, auf welchen die bezogenen Medikamente des Beschwerdeführers namentlich angeführt und ersichtlich waren.

Aufgrund der Anordnung des § 34 VersVG trifft den Beschwerdeführer eine Auskunfts- und Belegeobliegenheit gegenüber der Beschwerdegegnerin. Die Übermittlung der Gesundheitsdaten kann sich diesfalls auf

§ 11a Abs. 1 Z 3 und Abs. 2 Z 2 VersVG stützen. Die Beschwerdegegnerin hingegen trifft die Beweispflicht dafür, dass die angeforderten Unterlagen zur Feststellung des Versicherungsfalles oder des Umfanges der Leistungspflicht tatsächlich erforderlich sind. Als Konkretisierung des § 34 VersVG konnte Punkt 7.1. der Allgemeinen Versicherungsbedingungen gewertet werden. Die Beschwerdegegnerin führte aus, dass durch eine bloße Rezeptgebührenbestätigung eventuelle irrtümliche Doppeleinreichungen nicht eruiert werden könnten, wodurch eine korrekte Bearbeitung im Interesse der Gesamtversichertengemeinschaft nicht garantiert werden könne.

Insofern erscheint es durchaus „denkmöglich", dass die Beschwerdegegnerin die Originalrechnungen für die Beurteilung des genauen Umfangs ihrer Leistungspflicht benötigt.

Im Ergebnis liegt keine Verletzung im Recht auf Geheimhaltung vor.

Der Bescheid ist rechtskräftig.

### 2020-0.127.361 (D124.365), Einladung zur Akteneinsicht als Reaktion auf ein Auskunftsbegehren

Im Bescheid vom 9. Juli 2020 hat sich die Datenschutzbehörde mit der Frage auseinandergesetzt, ob die Beschwerdegegnerin den Beschwerdeführer dadurch im Recht auf Auskunft verletzt hat, indem sie ihn in Reaktion auf ein Auskunftsbegehren zur Akteneinsicht eingeladen hat.

Der Beschwerdeführer richtete ein Auskunftsbegehren an die Beschwerdegegnerin und beantragte darin „volle Auskunft über seine personenbezogenen Daten". Die Beschwerdegegnerin beantwortete das Auskunftsbegehren, indem sie den Beschwerdeführer zur Akteneinsicht eingeladen hat und ihm diesbezüglich einen Termin mitteilte. Weiters wurde der Beschwerdeführer darüber informiert, dass er sich gemäß § 17 AVG von Akten oder Aktenteilen an Ort und Stelle Abschriften selbst anfertigen und auf seine Kosten Kopien oder Ausdrucke erstellen lassen könne.

Der Beschwerdeführer ist zu dem im Schreiben genannten Termin nicht erschienen. Die Beschwerdegegnerin benachrichtigte daraufhin den Beschwerdeführer mit Schreiben, dass aufgrund des unentschuldigten Nichterscheinens das „Datenauskunftsverfahren" eingestellt werde.

Die Datenschutzbehörde gab der Beschwerde statt und trug der Beschwerdegegnerin auf, dem Beschwerdeführer eine dem Art. 15 DSGVO entsprechende Auskunft zu erteilen.

Die Datenschutzbörde begründete dies zunächst damit, dass der DSGVO eine Subsidiaritätsregelung nach § 44 Abs. 5 DSG im Anwendungsbereich des 3. Hauptstücks des DSG (welches gegenständlich nicht zur Anwendung kommt) fremd ist.

Daraus ist abzuleiten, dass nunmehr mittels eines Auskunftsbegehrens grundsätzlich auch Auskunft über den Inhalt von Urkunden und Aktenbestandteilen begehrt werden kann, sofern darin personenbezogene Daten der betroffenen Person enthalten sind und der sachliche Anwendungsbereich der DSGVO eröffnet ist (vgl. Art. 4 Abs. 1 leg. cit).

Ein Verantwortlicher hat gemäß Art. 12 Abs. 1 geeignete Maßnahmen zu treffen, um einer betroffenen Person alle Informationen gemäß den Art. 13 und 14 und alle Mitteilungen gemäß den Art. 15 bis 22 und Art. 34 DSGVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Diese Informationen sind gemäß Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Antrag zur Verfügung zu stellen.

Die Beschwerdegegnerin reagierte daher jedenfalls unzureichend auf das Auskunftsbegehren, weshalb seitens der Datenschutzbehörde eine Rechtsverletzung festgestellt wurde und der Beschwerdegegnerin ein entsprechender Leistungsauftrag erteilt wurde.

Dieser Bescheid ist rechtskräftig.

### 2020-0.349.984 (D205.023), Scannen und Speichern von Ausweisdaten aufgrund von Abholung einer Briefsendung mittels „gelben Zettels" ist nicht unverhältnismäßig bei begrenzter Speicherdauer von sechs Monaten und berechtigten Interessen

Im Bescheid vom 26. Juni 2020 zur GZ: 2020-0.349.984 (D205.023) hatte sich die Datenschutzbehörde mit einer Beschwerde im Recht auf Geheimhaltung (§ 1 DSG) mit der Verarbeitung von Ausweisdaten aufgrund der Behebung einer Einschreibsendung zu befassen.

Der Beschwerdeführer behob in einer Filiale eine Postsendung mittels „ gelben Zettels", da er vom Postboten zu Hause nicht angetroffen wurde. Daraufhin wurde er aufgefordert, einen Lichtbildausweis vorzulegen. In weiterer Folge wurden die Ausweisdaten: Ausweisart, Ausweisnummer, Ausstellungsbehörde, Geburtsdatum sowie der korrespondierende Name elektronisch mittels Scangerät erfasst und für 6 Monate gespeichert. Eine Kopie des Ausweisdokuments selbst wurde hingegen nicht erstellt.

Im Verfahren vor der Datenschutzbehörde brachte die Beschwerdegegnerin vor, dass nach Ablauf der Aufbewahrungsfrist von 6 Monaten die gegenständlichen Daten gelöscht worden seien und begründete die Speicherfrist u.a. mit den gesetzlichen Gewährleistungsfristen. Demnach habe sie in der Lage seien müssen,

sich in allfälligen Verfahren bezüglich Schadensersatzansprüchen oder vor der Datenschutzbehörde freibeweisen zu können, indem sie ihrer Sorgfaltspflicht nachgekommen sei und die Identität des Übernehmers nachweislich geprüft habe.

Die Datenschutzbehörde wies die Beschwerde als unbegründet ab und erkennt an, dass die Verarbeitung der Ausweisdaten des Beschwerdeführers dazu dienen konnte, im Falle eines Rechtsstreits die Übergabe an den richtigen Empfänger nachweisen zu können. Die von der Beschwerdegegnerin verarbeiteten Datenkategorien sind keinesfalls überschießend und die Speicherdauer mit sechs Monaten ist nicht als unverhältnismäßig anzusehen. Daher überwiegen die berechtigten Interessen der Beschwerdegegnerin gegenüber den Grundrechten und Grundfreiheiten des Beschwerdeführers und die Verarbeitung erfolgte rechtmäßig auf Grundlage von berechtigten Interessen nach Art 6 Abs. 1 lit. f DSGVO.

Dieser Bescheid ist rechtskräftig.

## Ausgewählte Entscheidungen der Gerichte

### BVwG-Erkenntnis vom 20. August 2020, GZ W258 2217446-1/15E (Österreichische Post AG)

Mit diesem Teilerkenntnis bestätigte das BVwG teilweise einen Bescheid der Datenschutzbehörde, wonach es sich bei den Daten zur „Parteiaffinität" um besondere Kategorien personenbezogener Daten iSd Art. 9 DSGVO handle, die dem darin normierten Verarbeitungsverbot unterliegen und demnach unrechtmäßig verarbeitet wurden.

Begründend führte das BVwG zusammengefasst aus, der Unionsgesetzgeber hatte in der Verwendung des Ausdrucks „alle Informationen" das Ziel vor Augen, dem Begriff der „personenbezogenen Daten" eine weite Bedeutung beizumessen. Weiters ergebe sich aus der „Parteiaffinität" eine hinreichende Wahrscheinlichkeit des Hervorgehens der politischen Meinung, weshalb besondere Kategorien personenbezogener Daten iSd Art. 9 DSGVO vorliegen. Werden Personen mit einer hohen „Parteiaffinität" für eine bestimmte politische Meinung empfänglich angesehen und sollen deshalb gezielt mit Werbung über politische Parteien beworben werden, würden dazu spiegelbildlich die Gefahren stehen, die Art. 9 DSGVO vermeiden möchte.

Das BVwG stellte sodann klar, dass § 151 Abs. 6 GewO keine Regelung iSd Art. 9 Abs. 2 lit. g DSGVO ist, welche eine Verarbeitung besonderer Kategorien personenbezogener Daten zulässig machen würde. Man könne nämlich kein erhebliches öffentliches Interesse iSd Art. 9 Abs. 2 lit. g annehmen, wenn durch die Rechtsnorm lediglich die Tätigkeit eines bestimmten Wirtschaftsbereichs erleichtert werden soll. Die Allgemeinheit wäre in derartigen Fällen ohne die in Rede stehende Maßnahme regelmäßig nicht ernsthaft beeinträchtigt, weshalb die Verarbeitung der Datenarten zur „Parteiaffinität" nicht auf Art. 9 Abs. 2 lit. g DSGVO iVm § 151 Abs. 6 GewO gestützt werden könne.

Da sich die Österreichische Post AG auch auf keine der anderen Ausnahmebestimmungen des Art. 9 Abs. 2 DSGVO vom Verarbeitungsverbot besonderer Kategorien von Daten des Art. 9 Abs. 1 DSGVO berufen könne, insbesondere habe sie keine Zustimmung für die Verarbeitung von den Betroffenen eingeholt, erweise sich die Verarbeitung der Daten zur „Parteiaffinität" als rechtswidrig.

Das Teilerkenntnis ist nicht rechtskräftig.

### EuGH-Urteil vom 16. Juli 2020, C-311/18 (Schrems II)

Ausgangspunkt des Verfahrens war ein Rechtsstreit zwischen der irischen Aufsichtsbehörde und Maximilian Schrems im Hinblick auf die von Herrn Schrems begehrte Untersagung der Übermittlung seiner personenbezogenen Daten durch Facebook Irland an Facebook Inc. in die Vereinigten Staaten.

Der Gerichtshof prüfte einerseits die Gültigkeit der Angemessenheitsentscheidung betreffend die USA (Beschluss 2016/1250, sog. „Privacy-Shield") und andererseits den Beschluss 2010/87 über Standarddatenschutzklauseln für Auftragsverarbeiter (sog. „SDK-Beschluss"). Im Ergebnis wurde das Privacy-Shield (wie bereits dessen Vorgänger „Safe-Harbor") für ungültig erklärt. Als maßgeblich für seine Entscheidung nennt der Gerichtshof umfangreiche, nicht auf das zwingend erforderliche Maß beschränkte Eingriffs- und Zugriffsbefugnisse von U.S.-amerikanischen Behörden auf personenbezogenen Daten, welche aus dem Unionsgebiet in die Vereinigten Staaten übermittelt werden, sowie unzureichende Rechtsschutzmöglichkeiten.

Im Hinblick auf den SDK-Beschluss stellte der Gerichtshof fest, dass die Prüfung anhand der Charta der Grundrechte nichts ergeben hat, was seine Gültigkeit berühren könnte. Gleichzeitig sprach der Gerichtshof aber aus, dass Standarddatenschutzklauseln alleine in bestimmten Fällen kein ausreichendes Schutzniveau bieten und daher die Schaffung von zusätzlichen Maßnahmen bzw. Garantien geboten sein kann.

Der Europäische Datenschutzausschuss hat zum Urteil C-311/18 bereits am 23. Juli 2020 ein Dokument mit häufig gestellten Fragen veröffentlicht und befindet sich dazu eine ergänzende Orientierungshilfe in Bezug auf zusätzliche Maßnahmen zu den SDK in Arbeit. Weitere Informationen sind auch auf der Website der Datenschutzbehörde abrufbar.

## Gesetzesbegutachtung – Stellungnahmen

**Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:**

- Bundesgesetz, mit dem das E-Government-Gesetz und das Passgesetz 1992 geändert werden
- Bundesgesetz, mit dem zivilrechtliche und zivilprozessuale Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden (Hass-im-Netz-Bekämpfungs-Gesetz – HiNBG)
- Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen
- Bundesgesetz, mit dem das Epidemiegesetz 1950, das Tuberkulosegesetz und das COVID-19-Maßnahmengesetz geändert werden
- Entwurf eines Landesgesetzes, mit dem das Gesetz über die Gewährung von Sozialunterstützung (Steiermärkisches Sozialunterstützungsgesetz – StSUG) erlassen und das Steiermärkische Sozialhilfegesetz, das Steiermärkische Wohnunterstützungsgesetz, Steiermärkische Behindertengesetz und das Steiermärkische Grundversorgungsgesetz geändert werden
- Neufassung der Verordnung des Fachverbandes der gewerblichen Dienstleister über die Befähigungsprüfung für das Sicherheitsgewerbe eingeschränkt auf das Gewerbe der Berufsdetektive (Berufsdetektive-Befähigungsprüfungsordnung);
- Bundesgesetz, mit dem das Kontenregister- und Konteneinschaugesetz, das Finanzmarkt-Geldwäschegesetz, das Bankwesengesetz, die Bundesabgabenordnung, das Finanzmarktaufsichtsbehördengesetz und das Wertpapieraufsichtsgesetz 2018 geändert werden
- Bundesgesetz, mit dem ein Investitionskontrollgesetz erlassen und das Außenwirtschaftsgesetz 2011 geändert wird
- Bundesgesetz, mit dem das Hochschul-Qualitätssicherungsgesetz geändert wird, ein Bundesgesetz über Privathochschulen erlassen wird und das Fachhochschul-Studiengesetz sowie das Hochschulgesetz 2005 geändert werden

**Weblink:**

- Parlament aktiv: alle Stellungnahmen

## News

**Folgende neue Mitarbeiterinnen und Mitarbeiter nahmen ihre Tätigkeit in der DSB auf:**

Herr **Eduard Brauchinger** war ab 1985 für das Bundesministerium für Inneres tätig und unterstützt nun den Personal- und Budgetbereich.

Herr **Mag. Marek Gerhalter** studierte Rechtswissenschaften an der Karl-Franzens-Universität Graz und war danach mehrere Jahre in Rechtsabteilungen international agierender Unternehmen tätig. Er absolviert derzeit den postgradualen Universitätslehrgang Informations- und Medienrecht an der Universität Wien und unterstützt das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

Herr **Lukas Matschinger** unterstützt tatkräftig das Kanzleiteam.

Frau **Mag. Vanessa Neudecker** war nach dem Studium an der Universität Wien sowie diversen Praktika zuletzt als Mitarbeiterin in der Rechtsabteilung eines Telekommunikationsunternehmens tätig. Nun unterstützt sie das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

Frau **Mag. Sairah Batul Rizvi** studierte Rechtswissenschaften an der Universität Wien und unterstützt das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

Frau **Mag. Elina Vera Schuster, LL.M** war nach ihrem Studium der Rechtswissenschaften in Wien und York (UK) zuletzt als Referentin für Energiepolitik an der Ständigen Vertretung von Österreich bei der EU in Brüssel tätig. Sie unterstützt jetzt das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

**Impressum:**
Medieninhaber, Herausgeber und Redaktion: Österreichische Datenschutzbehörde (DSB), Barichgasse 40-42, 1030 Wien, E-Mail: dsb@dsb.gv.at, Web: http://www.dsb.gv.at

**Offenlegung gemäß § 25 Mediengesetz:**
Der Newsletter der DSB ist ein wiederkehrendes elektronisches Medium (§ 1 Abs. 1 Z 5a lit. c MedienG); die gesetzlich gebotenen Angaben sind über folgenden Link abrufbar: http://www.dsb.gv.at/impressum.