

Newsletter 3/2022



Republik Österreich
Datenschutz
behörde

Liebe Leserinnen und Leser!

Die DSB wünscht allen viel Freude beim Lesen!

FAQ zum Thema Datenschutz und Cookies

Dr. Andreas Zavadil

Die Datenschutzbehörde hat FAQ zum Thema Datenschutz und Cookies veröffentlicht. In den FAQ wird auf praxisrelevante Fragen eingegangen, wie zum Beispiel die Gestaltung eines Cookie-Banners, die Zulässigkeit des Modells „pay or okay“ oder unter welchen Voraussetzungen eine Einwilligung für das Setzen und Auslesen von Cookies erforderlich ist. Die FAQ wurden in „nicht juristischer“ Sprache geschrieben, damit das Thema auch für Laien verständlich ist. Die FAQ sind auf der Website der Datenschutzbehörde (Menüpunkt: „Download & Links“) zu finden und werden laufend ergänzt. In weiterer Folge werden die wichtigsten Punkte der FAQ in Kurzform erläutert.

Man versteht unter Cookies kleine Textdateien, die am Endgerät – also etwa am Computer oder Smartphone – bzw. im Browser abgespeichert werden, wenn eine Website im Internetbrowser aufgerufen wird. Diese Textdateien können u.a. vom Webserver einer solchen Website ausgelesen werden. Wird etwa eine Website in fünf verschiedenen Sprachversionen angeboten und wird beim erstmaligen Aufruf der Website die Sprachversion „Deutsch“ ausgewählt, so wird am Endgerät nun eine Textdatei („Cookie“) samt der Information hinterlegt, dass die Website in der deutschen Sprache angezeigt werden soll. Wenn die Cookies nicht gelöscht werden und wenn die Website mit demselben Browser erneut aufgerufen wird, so weiß die Website aufgrund des hinterlegten Cookies, dass die Website in deutscher Sprache angezeigt werden soll.

Aus rechtlicher Sicht ist beim Setzen oder Auslesen von Cookies Art. 5 Abs. 3 der Richtlinie 2002/58/EG idgF. zu beachten, welcher auf nationaler Ebene in § 165 Abs. 3 TKG 2021 umgesetzt wurde. Zusammengefasst dürfen Cookies beim Aufruf einer Website nur dann ohne Einwilligung gesetzt oder ausgelesen werden, 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 („technisch notwendige Cookies“). Für alle „technisch nicht notwendigen Cookies“ muss daher eine Einwilligung eingeholt werden. Die Bedingungen für eine solche Einwilligung richten sich nach Art. 4 Z 11 und Art. 7 DSGVO. In den FAQ sind Beispiele zu finden, wann aus Sicht der Datenschutzbehörde von einer „technischen Notwendigkeit“ von Cookies auszugehen ist.

Auf nationaler Ebene obliegt der Vollzug eines Verstoßes gegen § 165 Abs. 3 TKG 2021 den Fernmeldebehörden. Eine Zuständigkeit der Datenschutzbehörde kann aber dennoch gegeben sein, wenn als Folge des Einsatzes von Cookies personenbezogene Daten gemäß Art. 4 Z 1 DSGVO verarbeitet werden. Dies kann insbesondere bei sog. „Tracking-Cookies“ der Fall sein, die das Surfverhalten von Nutzern aufzeichnen, um in Folge personalisierte Werbung anzuzeigen. Es gilt zu beachten, dass derartige Aufzeichnungen in manchen Fällen auch mit einem Profil auf einer Social Media Plattform in Verbindung gebracht werden können.

In der Praxis stellt sich oft die Frage, wie ein Cookie-Banner (also die Schaltfläche, mit welcher die Einwilligung eingeholt wird) rechtskonform gestaltet sein muss. In den FAQ sind Handlungsempfehlungen für die Gestaltung eines Cookie-Banners vorhanden. Die Datenschutzbehörde vertritt insbesondere den Standpunkt, dass die Nichtabgabe einer Einwilligung (bzw. das Weitersurfen ohne Einwilligung) genauso einfach sein muss wie die Abgabe der

Einwilligung. Mit anderen Worten: Für die Nichtabgabe einer Einwilligung dürfen nicht mehr Interaktionen mit dem Cookie-Banner notwendig sein, als für die Abgabe der Einwilligung. Von der betroffenen Person kann nicht verlangt werden, dass sie auf einer Schaltfläche erst auf einer zweiten oder dritten Ebene die Entscheidung treffen kann, keine Einwilligung abzugeben. Darüber hinaus dürfen betroffene Personen weder unmittelbar noch subtil zur Abgabe einer Einwilligung gedrängt werden (kein „nudging“). Es entspricht keiner fairen Praxis, den Button zur Nichtabgabe einer Einwilligung (bzw. zum Weitersurfen ohne Einwilligung) derart zu gestalten oder zu positionieren, dass dieser Button weniger prominent ist, als der Button zur Abgabe einer Einwilligung.

Schließlich widmen sich die FAQ auch der Frage, ob eine „Cookiewall“ zulässig ist. Bei einer solchen „Cookiewall“ kann für den Zutritt zur Website entweder Geld bezahlt werden, alternativ kann die Einwilligung für den Einsatz von Cookies (üblicherweise zum Ausspielen von personalisierter Werbung) abgegeben werden. Umgangssprachlich bezeichnet man dies auch als „pay or okay“. Die Datenschutzbehörde hat in der Vergangenheit mit Bescheid vom 20. August 2019, GZ: DSB-D122.974/0001-DSB/2019 bereits ausgesprochen, dass ein derartiges Modell grundsätzlich zulässig sein kann. Zwar gibt es zu dieser Frage noch keine Judikatur des Europäischen Gerichtshofs. Für die Entscheidung der Datenschutzbehörde spricht, dass offenbar auch der europäische Gesetzgeber davon ausgeht, dass personenbezogene Daten – zumindest im gewissen Ausmaß – für den Erhalt einer Leistung bereitgestellt werden können (vgl. die Richtlinie (EU) 2019/770 idgF.). In den FAQ sind Anforderungen zu finden, die bei „pay or okay“ jedenfalls zu beachten sind.

Im Fokus

Google Analytics II

Dr. Andreas Zavadil

Mit Bescheid vom 22. April 2022, GZ: D155.026, 2022-0.298.191 („Google Analytics II“), hat die Datenschutzbehörde wiederholt ausgesprochen, dass der Einsatz des Tools Google Analytics – jedenfalls im beschwerdegegenständlichen Zeitraum – nicht mit den Vorgaben von

Kapitel V DSGVO für den Internationalen Datenverkehr vereinbar war. Es stand die Frage im Raum, ob bei der Beurteilung der Zulässigkeit von Datenübermittlungen an ein Drittland ein „risikobasierter Ansatz“ zu verfolgen ist. In diesem Beitrag wird beleuchtet, was unter einem „risikobasierten Ansatz“ zu verstehen ist und ob ein solcher für derartige Datenübermittlungen maßgeblich ist.

Die Zulässigkeit der Übermittlung personenbezogener Daten an ein Drittland hängt immer von einer Einzelfallprüfung ab. Dies ergibt sich bereits aus der Überlegung, dass Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO für einen konkreten Sachverhalt und zwischen individuellen Parteien abzuschließen sind. Im Einzelfall ist auch zu überprüfen, ob die sich aus den Standarddatenschutzklauseln ergebenden Verpflichtungen eingehalten werden können und ob das Recht des jeweiligen Drittstaats diesen Verpflichtungen entgegensteht.

Dies soll an folgenden Beispielen illustriert werden:

Wenn eine bestimmte Stelle zum Beispiel nicht als Anbieter elektronischer Kommunikationsdienste im Sinne von 50 U.S. Code § 1881(b)(4) zu qualifizieren ist, so bestehen die seitens des EuGH mit Urteil vom 16. Juli 2020, C-311/18 problematischen Zugriffsmöglichkeiten von US-Behörden nicht. Ist im Einzelfall zum Beispiel eine dem Stand der Technik entsprechende Verschlüsselung der Daten gegeben und bestehen seitens der US-Sicherheitsbehörden keine Zugriffsmöglichkeiten auf den kryptographischen Schlüssel, wären die seitens des EuGH aufgezeigten Probleme beseitigt. Wäre Österreich zum Beispiel ein Drittstaat, so müsste vor der Datenübermittlung nach Österreich überprüft werden, ob die konkret übermittelten Datenarten etwa dem Anwendungsbereich nach dem (nunmehrigen) Staatsschutz- und Nachrichtendienst-Gesetz, BGBl. I Nr. 5/2016 idGF., unterliegen und ob die Zugriffsmöglichkeiten der Direktion Staatsschutz und Nachrichtendienst (DSN) verhältnismäßig sind.

Eine derartige Einzelfallprüfung ist jedoch vom „risikobasierten Ansatz“ zu unterscheiden. Vertreter des risikobasierten Ansatzes wollen bei dieser Einzelfallprüfung als zusätzlichen Faktor das mit der Datenübermittlung in die USA verbundene Risiko berücksichtigen. Aus den im Bescheid vom 22. April 2022 angeführten Gründen ist eine derartige Rechtsposition abzulehnen. In weiterer Folge werden die wesentlichen Argumente der Datenschutzbehörde dargestellt, für eine weiterführende Begründung ist auf den genannten Bescheid zu verweisen:

Aus dem Wortlaut von Art. 44 DSGVO kann ein risikobasierter Ansatz nicht abgeleitet werden, tatsächlich wird das Wort „Risiko“ auch kein einziges Mal in Kapitel V der Verordnung verwendet. An jenen Stellen der DSGVO, an denen tatsächlich ein risikobasierter Ansatz zu verfol-

gen ist („je mehr Risiko, desto mehr Schutzmaßnahmen“), wird dies ausdrücklich klargestellt. Eine analoge Heranziehung eines risikobasierten Ansatzes im obigen Sinn kommt daher nicht in Betracht. Die DSGVO enthält Vorgaben, bei denen – genauso wie bei Art. 44 DSGVO – gerade von keinem risikobasierten Ansatz auszugehen ist. So gelten etwa die in Art. 7 DSGVO normierten Bedingungen für eine Einwilligung immer und unabhängig vom Verarbeitungsrisiko. Mit anderen Worten: Der in Art. 7 DSGVO normierte Maßstab für das Einholen einer Einwilligung ist immer derselbe, egal ob mit der Einwilligung (mehr oder weniger belanglose) Email-Adressen erhoben werden, oder (was wohl ein höheres Risiko darstellt) umfangreiche Finanzdaten einer Person. Auch einige (wenn nicht alle) in Art. 5 DSGVO verankerten Grundsätze der Datenverarbeitung kennen keinen risikobasierten Ansatz. So sind etwa gemäß dem Grundsatz der Datenminimierung immer nur die für die Zweckerreichung notwendigen Daten zu verarbeiten. Mit anderen Worten: Daten, die für die Zweckerreichung nicht notwendig sind, dürfen auch dann nicht verarbeitet werden, wenn deren Verarbeitung möglicherweise ein geringes Risiko darstellt.

Auch der EuGH hat bei der Ungültigerklärung von „Privacy Shield“ (und auch bei „Safe Harbor“) nicht danach differenziert, ob „Privacy Shield“ für ein Wirtschaftsunternehmen im Einzelfall möglicherweise doch ein „angemessenes Datenschutzniveau“ schafft, etwa, weil bloß nicht-sensible Daten oder nicht-strafrechtlich relevante Daten verarbeitet werden. Standard-datenschutzklauseln können demnach nur dann als Instrument für den Internationalen Datenverkehr „geeignet“ sein, wenn dadurch ein Datenschutzniveau geschaffen wird, das der Rechtsansicht des EuGH Rechnung trägt.

Die Datenschutzbehörde verkennt nicht, dass der Wegfall von Privacy Shield zu vielen Fragen geführt hat. Dennoch kann dies nicht dazu führen, dass die Rechtsansicht des EuGH übergangen wird.

Ausgewählte Entscheidungen der DSB

2022-0.244.681 (D550.540), Unrechtmäßige Abfragen im e-Impfpass

Mit **Straferkenntnis** vom 05.04.2022 verhängte die Datenschutzbehörde eine **Geldbuße in Höhe von EUR 3.300,-** in Reaktion auf eine unrechtmäßige Verarbeitung sensibler Daten (Gesundheitsdaten). Die Beschuldigte hat Gesundheitsdaten von drei Betroffenen verarbeitet,

indem sie auf die Daten im e-Impfpass zugriff, um sich über den Impfstatus der Betroffenen zu informieren. Die Beschuldigte nahm die Verarbeitung in ihrer Funktion als niedergelassene Ärztin vor und war grundsätzlich für solche Abfragen freigeschalten. Die Verarbeitung erfolgte ohne Wissen und Einwilligung der Betroffenen und konnte auch sonst auf keine der restlichen Ausnahmetatbestände gemäß Art. 9 Abs. 2 DSGVO gestützt werden.

Die Beschuldigte führte ins Treffen, dass sie als Arbeitgeberin einer gesetzlichen Fürsorgepflicht gemäß § 1157 ABGB unterliegt und die Abfragen nur deshalb vornahm, weil sie darüber informiert wurde, dass eine ihrer Sekretärinnen an einer geplanten Familienveranstaltung teilnehmen wird. Im Sinne einer besseren Risikoeinschätzung für ihre Ordination informierte sich die Beschuldigte daher über den Impfstatus der Betroffenen, die ebenfalls an der Feier teilnahmen. Die Datenschutzbehörde hielt eingangs fest, dass der Ausnahmetatbestand nach Art. 9 Abs. 2 lit. h DSGVO iVm § 1157 ABGB grundsätzlich eine taugliche Rechtsgrundlage darstellen kann. Im konkreten Fall erfolgte die Verarbeitung jedoch nicht im Einklang mit den Grundsätzen der Datenverarbeitung. Die konkrete Verarbeitung war jedenfalls **nicht erforderlich** und erfolgte **zweckwidrig**. Die Beschuldigte hatte ihre Sekretärin unabhängig von der Abfrage bereits angewiesen, sich nach der Familienfeier täglich zu testen.

Die Datenschutzbehörde stellte im Ergebnis einen Verstoß gegen Art. 5 Abs. 1 lit. a, b und c sowie Art. 9 Abs. 1 iVm Art. 83 Abs. 1 und 5 lit. a DSGVO fest.

2022-0.286.157 (D213.1560), Warnung im Administrativverfahren

Mit Bescheid vom 30. Mai 2022 hat sich die Datenschutzbehörde mit der Frage auseinandergesetzt, ob Mitglieder eines Dienststellenausschusses Daten des Personalverzeichnisses verwenden dürfen, um postalische Werbeschreiben für den Beitritt zu einer Gewerkschaft zu versenden.

Die Datenschutzbehörde hat ein amtswegiges Prüfverfahren gegen zwei Mitglieder eines Dienststellenausschusses (als Verantwortliche) eingeleitet. Diese haben gemäß § 9 Abs. 3 lit. i PVG zur Erfüllung ihrer Aufgaben Zugriff auf das Personalverzeichnis sowie die darin enthaltenen Daten der Bediensteten. Im gegenständlichen Fall wurden diese Daten seitens der Verantwortlichen verwendet, um für den Beitritt zu einer Gewerkschaft zu werben.

Es wurde festgestellt, dass eine derartige Datenverarbeitung keine Deckung im PVG findet und daher unrechtmäßig war. Dies ergibt sich aus einem Vergleich mit Rechtsgrundlagen, die für andere - gesetzliche - Interessenvertretungen gelten: So ist etwa in § 17a AKG die aus-

drückliche Erlaubnis der Verwendung von personenbezogenen Daten der Arbeiterkammer-Mitglieder für (Wahl)Werbung vorgesehen. Eine entsprechende Regelung für die Wirtschaftskammer findet sich in § 86 Abs. 3 WKG. Die Schaffung einer gesetzlichen Grundlage zur - wie der hier erfolgten - Datenverarbeitung zwecks Anwerbung als Gewerkschaftsmitglied obliegt dem Gesetzgeber.

Vor diesem Hintergrund waren die Verantwortlichen gemäß Art. 58 Abs. 1 lit. d DSGVO auf diesen Verstoß hinzuweisen, damit das Verhalten nicht wiederholt wird und um die Verantwortlichen gemäß Art. 57 Abs. 1 lit. d DSGVO für ihre datenschutzrechtlichen Pflichten zu sensibilisieren.

2022-0.263.348 (D485.009), Antrag auf vorherige Konsultation nach Art. 36 DSGVO betreffend das COVID-19-Impfpflichtgesetz

Ein Dienstleistungsunternehmen im Gesundheitsbereich brachte vor, es werde durch das Bundesgesetz über die Pflicht zur Impfung gegen COVID-19 (COVID-19-Impfpflichtgesetz – COVID-19-IG), BGBl. I Nr. 4/2022 idF BGBl. I Nr. 22/2022, zur datenschutzrechtlichen Verantwortlichen für die personenbezogene Verarbeitung von Ausnahmen von der generellen COVID-19-Impfpflicht im Zentralen Impfregeister sowie für die Übermittlung der Impfdaten und Ausnahmen an den Gesundheitsminister (unter anderem zur Verhängung von Strafen gegenüber Nichtgeimpften) gemacht. Im Zuge des Begutachtungsverfahrens des COVID-19-IG sei keine Datenschutz-Folgenabschätzung vorgenommen worden. Das hohe Risiko könne auch nicht durch entsprechende Maßnahmen eingedämmt werden. Die Datenschutzbehörde werde um Entscheidung ersucht, ob bzw. unter welchen Umständen die im COVID-19-IG vorgesehenen Verarbeitungstätigkeiten im Einklang mit der DSGVO durchgeführt werden können.

Mit Bescheid vom 21.4.2022 hat die Datenschutzbehörde den Antrag auf vorherige Konsultation zurückgewiesen, da die Voraussetzungen dafür nicht gegeben sind. Die von der Verantwortlichen vorgebrachten Bedenken betreffen nämlich im Wesentlichen die Rechtsgrundlage der vorgesehenen Datenverarbeitungen im Hinblick auf deren befürchtete Verfassungs- bzw. Unionsrechtswidrigkeit. Die behauptete Verfassungs- oder Unionsrechtswidrigkeit eines Gesetzes kann jedoch vor allem deshalb nicht Gegenstand eines Konsultationsverfahrens sein, da es einem Verantwortlichen im Falle einer gesetzlich vorgesehenen Datenverarbeitung gar nicht möglich ist, diese zu beeinflussen und allfällige Restrisiken faktisch zu mindern. Auch die Befugnisse einer Aufsichtsbehörde zielen darauf ab, faktisch Einfluss auf die Datenver-

beitung nehmen zu können. Die Kompetenz, über die Verfassungswidrigkeit eines Gesetzes zu entscheiden oder zu prüfen, ob dieses mit dem Unionsrecht übereinstimmt, obliegt nicht der Aufsichtsbehörde.

Der Bescheid ist nicht rechtskräftig.

Ausgewählte Entscheidungen der Gerichte

BVwG-Erkenntnis vom 17. Mai 2022, GZ W256 2225038-1/8E

Mit gegenständlichem Erkenntnis des BVwG wurde die Beschwerde gegen den Bescheid der Datenschutzbehörde vom 23. August 2019 als unbegründet abgewiesen.

Im vorliegenden Fall begehrte die Beschwerdeführerin von der Datenschutzbehörde die Genehmigung zur Erstellung und den Betrieb einer Stammbaum-Datenbank, welche auf der Website der Beschwerdeführerin abrufbar sei und an Geschichte und Familienforschung interessierten Personen die Möglichkeit zur (eigenen) Familienforschung einräumen solle. Dabei stützte sie sich auf § 7 Abs. 3 DSG. Der Antrag auf Genehmigung wurde von der Datenschutzbehörde abgewiesen.

Das BVwG führte im Wesentlichen aus, dass entgegen der Überschrift bzw. der Bezugnahme auf Archivzwecke insbesondere § 7 Abs. 3 DSG im Kern gar nicht auf den Archivierungsfall abzielt. Sowohl § 7 Abs. 3 als auch Abs. 4 verwenden den Begriff der "Untersuchung". Diese Formulierungen stellen klar, dass sich der Anwendungsbereich des § 7 Abs. 3 DSG auf die Einholung einer Genehmigung zur Verwendung von personenbezogenen Daten aus fremden Datenbeständen, und zwar allein zum Zweck der Vornahme einer Untersuchung durch den Antragssteller als Verantwortlicher beschränkt. Die Erhebung und Verarbeitung von Daten, um diese einer Öffentlichkeit allenfalls zu Forschungszwecken zugänglich zu machen, kann dementsprechend nicht vom Anwendungsbereich des § 7 Abs. 3 DSG umfasst sein.

VwGH-Beschluss vom 24.02.2022, ZI. Ra 2020/04/0187

Das Höchstgericht hat ein anhängiges Revisionsverfahren der DSB (gegen das Erkenntnis des Bundesverwaltungsgerichts [BVwG] vom 26. November 2020, GZ: W258 2227269-1/14E) unterbrochen. Zuvor hatte das BVwG, der neuesten Rechtsprechung des Verwaltungsgerichtshofs zu Art. 83 DSGVO und § 30 DSG folgend (VwGH 12.5.2020, Ro 2019/04/0229), ein

Straferkenntnis der DSB aufgehoben. Nach Ansicht des BVwG fehlten im Straferkenntnis die zur Beurteilung des schuldhaften Verhaltens einer natürlichen Person, deren Verhalten der juristischen Person zugerechnet werden kann, notwendigen Feststellungen. Die DSB vertritt die Ansicht, dass zur Bestrafung einer juristischen Person (z.B. einer Ges.m.b.H.) kein individuelles schuldhaftes Fehlverhalten, etwa des Geschäftsführers, nachgewiesen werden muss. Inzwischen ist beim EuGH zu C-807/21 ein Vorabentscheidungsersuchen des Kammergerichts Berlin anhängig, das (u.a.) die Auslegung des Art. 83 DSGVO in der Frage der Notwendigkeit einer solchen Feststellung zum Gegenstand hat. In Deutschland war die Bestimmung in Verbindung mit § 30 dt. OWiG (Ordnungswidrigkeitengesetz) anzuwenden. Diese Norm ist dem Inhalt nach mit § 30 DSG vergleichbar.

Die DSB setzt anhängige Verwaltungsstrafverfahren, die von der Lösung dieser Rechtsfrage abhängen, bis zur Entscheidung des EuGH aus.

Gesetzesbegutachtung - Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung, mit der die Verordnung über die Lehrpläne der Mittelschulen sowie die Verordnung über die Lehrpläne der allgemeinbildenden höheren Schulen geändert werden (Digitale Grundbildung in den Lehrplanbestimmungen)
 - Bundesgesetz, mit dem das Schulorganisationsgesetz, das Schulunterrichtsgesetz, das Schulzeitgesetz 1985 und das Land- und forstwirtschaftliche Bundesschulgesetz geändert werden
 - Änderung des Studienförderungsgesetzes 1992
 - Novelle des Tierschutzgesetzes
 - Änderung der Staatsbürgerschaftsverordnung 1985
 - Ausschussbegutachtung (242/AUA) Parteiengesetz
 - Abgabenänderungsgesetz 2022 (AbgÄG 2022)
 - Klimabonus-Abwicklungsverordnung – KliBAV
-

News

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

Frau **Dina Abdel-Aziz** verstärkt seit Juli 2022 und Herr **Kevin Breinreich** seit Mai 2022 die juristischen Teams zur Führung der nationalen Verfahren.

Folgende Mitarbeiter beendeten ihre Tätigkeit in der DSB:

LL.B. (WU) Rainer **Cheng**, LL.M. (WU) Bernhard **Granadia**, Lukas **Matschinger**, Philippe **Schmit**, Mag. Mathias **Veigl**

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/ueber-die-website/impressum-copyright.html>

Copyright und Haftung:

Der auszugsweise Abdruck dieser Publikation ist nur mit Quellenangabe gestattet. Alle sonstigen Rechte sind ohne schriftliche Zustimmung des Medieninhabers unzulässig. Sämtliche Angaben in dieser Publikation erfolgen trotz sorgfältiger Bearbeitung ohne Gewähr. Eine Haftung der Datenschutzbehörde sowie der Autorinnen und Autoren ist ausgeschlossen. Rechtsausführungen stellen die unverbindliche Meinung der Autorinnen und Autoren dar. Sie können der Rechtsprechung der unabhängigen Gerichte keinesfalls vorgeifen.

Ihre Rückmeldungen übermitteln Sie bitte an dsb@dsb.gv.at.