Creditreform Compliance

Compliance & Risk Newsletter

Ausgabe I/2020
April 2020

Inhaltsverzeichnis

Corona und Datenschutz – was Arbeitgeber beachten sollten

Die „Corona-Krise“ (Virus: Covid-19) stellt Unternehmen und deren Beschäftigte vor die Herausforderung, den Gesundheitsschutz und die Betriebsabläufe im Einklang zu bewältigen. Bisher gibt es keine ausreichenden Erfahrungen zum Umgang mit vergleichbaren besonderen Situationen. Die rechtlichen Anforderungen im Hinblick auf den Datenschutz jedoch sind relativ eindeutig, auch wenn Datenschutzbehörden und weitere Gremien geneigt sind, den individuellen Bedürfnissen einzelner Branchen zum Erhalt des Wirtschaftslebens gerecht zu werden.

Welche Maßnahmen sind grundsätzlich unbedenklich?

Kommen unterschiedliche Maßnahmen in Betracht, sind aus datenschutzrechtlicher Sicht stets die Maßnahmen am günstigsten, die keinen unmittelbaren Zusammenhang zu personenbezogenen Daten haben. Solche einfachen Mittel könnten insbesondere sein:

- Strenge Hygienemaßnahmen, bspw. Pflicht zur häufigen Desinfektion der Hände
- Kein Empfang von Fremdbesuchern in den Geschäftsräumlichkeiten
- Keine Wahrnehmung von Außenterminen, bspw. Verbot von Dienstreisen
- Hinweise an die Beschäftigten, jeweils für sich vor dem Betreten der betrieblichen Räumlichkeiten zu klären, ob sie einschlägige Krankheitssymptome wie z.B. Fieber aufweisen, Kontakt zu infizierten Personen hatten oder sich selbst kürzlich in einem Risikogebiet aufgehalten haben

Sollen weitere Maßnahmen, speziell vor dem Hintergrund der arbeitsrechtlichen Fürsorgepflicht des Arbeitgebers getroffen werden, richtet sich die Zulässigkeit dieser Maßnahmen nach Art. 9 Datenschutz-Grundverordnung (DSGVO), der den Umgang mit besonders schützenswerten personenbezogenen Daten regelt. Darunter fallen gerade auch Gesundheitsdaten, die im Kontext der Covid-19-Krisenabwehr Verarbeitungsgegenstand sein können. Begrüßenswert ist demnach, dass seitens der Datenschutzkonferenz (Zusammenschluss der deutschen Datenschutz-Aufsichtsbehörden) erste Hinweise und Informationen hierzu veröffentlicht wurden. Nach deren Ansicht können, auch wenn eine Verarbeitung von Gesundheitsdaten grundsätzlich nur restriktiv möglich ist, für verschiedene Maßnahmen von Arbeitgebern, die der Eindämmung der Corona-Pandemie oder zum Schutz von Beschäftigten dienen, datenschutzkonform Daten erhoben und verwendet werden.

Geeignete und im gegebenen Kontext datenschutzrechtlich zulässige Maßnahmen dürften außerdem sein:

- Weitreichende Homeoffice-Regelungen, um die Minimierung des physischen Umgebungskontakts zu erreichen
- Befragung der Mitarbeiter hinsichtlich einer positiven Testung auf das Covid-19-Virus
- Befragung der Mitarbeiter, ob sie Kontakt zu einem positiv auf das Covid-19-Virus getesteten Menschen hatten
- Befragung der Mitarbeiter, ob sie sich in einem Risikogebiet (derzeit: u.a. Kreis Heinsberg (Nordrhein-Westfalen), Norditalien einschl. Südtirol, Österreich insb. Ischgl, Wuhan (VR China), einige

Regionen Frankreichs und Spaniens) aufgehalten haben
- Befragung der Mitarbeiter, ob sie Kontakt zu einem Menschen mit Aufenthalt in einem Risikogebiet hatten

Gleiches gilt für den Zutritt von Gästen und Besuchern.

Nach Auffassung einiger Juristen sind ebenfalls freiwillige Körpertemperaturmessungen (sog. „Fiebermessung“) zulässig; ob der Maßstab der Freiwilligkeit bei dem arbeitgeberseitigen Anbieten dieser Maßnahme gegenüber Beschäftigten tatsächlich gewahrt ist, erscheint sehr zweifelhaft. Jedenfalls kann die besondere Situation einen sozialen Druck gegenüber den Beschäftigten auslösen, was einer Freiwilligkeit entgegenstehen dürfte. So ist der Arbeitgeber zwar verpflichtet, den Gesundheitsschutz seiner Beschäftigten so weit möglich sicherzustellen, die hierzu getroffenen Maßnahmen müssen dabei jedoch immer verhältnismäßig sein.
Daher können diese Messungen der Körpertemperatur lediglich eine Entscheidungsgrundlage für den Arbeitgeber schaffen, ob Personen Zutritt zum Unternehmensgelände gewährt werden soll. Die Daten müssen dabei vertraulich behandelt und ausschließlich zweckgebunden verwendet werden. Folglich sollten die Messwerte nach Zutritt der Beschäftigten unmittelbar gelöscht werden. Welches Vorgehen letztlich gewählt wird, ist anhand der Gesamtumstände und unter einer Abwägung der Risiken durch das Unternehmen selbst zu entscheiden.

Generell unzulässige Maßnahmen dürften sein:

- Jegliche pauschalen bzw. allgemeinen Befragungen zum Gesundheitszustand
- Jegliche pauschale bzw. allgemeine Befragungen zu Aufenthaltsorten
- Mitteilung an Kollegen über die positive Testung eines anderen Beschäftigten auf Covid-19 unter Angabe seiner Identität; stattdessen sollten abteilungs- oder teambezogene Hinweise erteilt werden, um die weitere Ausbreitung des Virus zu verlangsamen
- Aufforderung an Beschäftigte, Kollegen zu melden, die typische Symptome zeigen

© Adobe Stock / Mike Fouque

Fazit

Als abstrakte Grundregel, ob eine Maßnahme eher zulässig oder unzulässig ist, kann demnach herausgearbeitet werden: Eine Maßnahme, die sich auf einen abstrakten Personenkreis bezieht und die Betroffenen gleichermaßen betrifft sowie untereinander den Schutz ihrer Daten wahrt, ist eher zulässig. Regelungen hingegen, die sich auf konkret feststellbare natürliche Personen beziehen und den Schutz ihrer Identität untereinander aufheben, sind typischerweise unzulässig. Entscheidend ist stets das Ergebnis einer jeden Einzelfallprüfung, die aber auch immer die besonderen praktischen Herausforderungen ihrer Branche zu berücksichtigen hat.

(Alexander Schmidt, Senior Consultant Data Protection Services, Creditreform Compliance Services GmbH)

Ungeregelter BREXIT – ein Datenschutz-desaster?

Der Brexit

Bereits am 23. Juni 2016 entschied sich eine knappe Mehrheit der Wähler Großbritanniens für einen Austritt des Vereinigten Königreichs aus der Europäischen Union (nachfolgend „EU“).
Nach gefühlt nicht enden wollenden Verhandlungen wurde das Austrittsabkommen schließlich zu Beginn dieses Jahres unterzeichnet. Jenes Abkommen trat mit Ablauf des 31. Januars in Kraft, so dass das Vereinigte Königreich in der Nacht zum 01. Februar 2020 offiziell aus der EU ausgetreten ist. Zu beachten ist, dass im Austrittsabkommen eine Übergangsphase bis zum Ende des Jahres 2020 fixiert wurde.

Bedeutung der Übergangsfrist

Die Übergangsfrist soll den unterschiedlichen betroffenen Akteuren (z.B. Unternehmen) die Möglichkeit bieten, sich auf die bevorstehenden Änderungen und Auswirkungen durch den Brexit vorzubereiten. Die Folge ist eine Fortgeltung des Unionsrechts für Großbritannien bis zum Ende dieser Frist. Da auch die EU-Datenschutz-Grundverordnung (nachfolgend „DSGVO“) als Unionsrecht einzustufen ist, gilt auch sie bis auf Weiteres für das Vereinigte Königreich. Zurücklehnen sollte man sich trotzdem nicht, denn im Austrittsabkommen ist explizit geregelt, dass die Frist nur noch bis zum 01. Juli 2020 einmalig um ein oder zwei Jahre verlängert werden kann.
Geschieht dies bis zu dem besagten Datum nicht und wird Großbritannien auch kein ausreichendes Datenschutzniveau im Rahmen eines Angemessenheitsbeschlusses der EU-Kommission nach Art. 45 Abs. 1 S. 1 DSGVO zugestanden, müssen diverse Vorkehrungen getroffen werden, um Datenflüsse auf rechtlich sichere Füße zu stellen.

Zwar wird aussagegemäß ein Angemessenheitsbeschluss bis Ende 2020 angestrebt, wer sich allerdings entsprechende Verfahren der letzten Jahre ansieht, der wird schnell feststellen, dass dieser Beschluss im Rekordtempo ergehen müsste. Erschwerend hinzu kommt der Umstand, dass durchaus infrage gestellt werden darf, ob die EU-Kommission den Briten ein angemessenes Datenschutzniveau bescheinigen wird, zumal die Regierung neuerdings auf ein eigenständiges und unabhängiges Regelwerk zum Datenschutz setzen will. Ferner ist der datenschutzrechtlich äußerst fragwürdige „Investigatory Powers Act“ zu nennen, der u.a. Dinge wie Vorratsdatenspeicherung und umfassende Überwachungsmaßnahmen legitimiert.
Ohne einen Angemessenheitsbeschluss wird Großbritannien aus datenschutzrechtlicher Sicht zum sog. unsicheren Drittland, wodurch es für eine legitime Datenübertragung geeigneter Garantien im Sinne der Art. 44 ff. DSGVO bedarf. Werden personenbezogene Daten in ein Drittland übertragen, ohne dass die vorbezeichneten Vorschriften beachtet werden, liegt ein Datenschutzverstoß vor, der ein erhebliches Bußgeld nach sich ziehen kann.

© Adobe Stock / Thaut Images

Was ist zu beachten?

Auch hier gilt es Ruhe zu bewahren, jedoch nicht untätig zu sein, denn es gibt verschiedene Möglichkeiten Datenflüsse in und aus dem Vereinigten Königreich auch im Fall eines ungeregelten Brexits rechtssicher abzubilden. Für Unternehmen bestehen demnach folgende Möglichkeiten:

- genehmigte Verhaltensregeln gemäß Art. 40 DSGVO
- Standardvertragsklauseln der EU-Kommission nach Art. 46 Abs. 2 lit. c DSGVO
- Binding Corporate Rules nach Art. 47 DSGVO
- individuell verhandelte Vertragsklauseln oder Verwaltungsvereinbarungen

In gewissen Ausnahmesituationen kann eine Datenübermittlung in ein Drittland auch ohne Vorliegen geeigneter Garantien erfolgen. Entsprechend der sehr eng auszulegenden Ausnahmetatbestände von Art. 49 DSGVO kann dies beim Vorliegen der folgenden Voraussetzungen der Fall sein:

- Einwilligung der Betroffenen liegt vor
- Datenübertragung erforderlich zur Vertragserfüllung
- wichtige Gründe des öffentlichen Interesses liegen vor
- Verfolgung von Rechtsansprüchen
- Schutz lebenswichtiger Interessen
- Wahrung zwingender berechtigter Interessen

Zusätzlich kann es geboten sein, u.a. das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO sowie Datenschutzhinweise und Datenschutzerklärungen im Sinne der Art. 13, 14 DSGVO oder auch Auskunftsschreiben gemäß Art. 15 DSGVO entsprechend der neuen Gegebenheiten zu ergänzen.

Unter Umständen können außerdem Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO erforderlich werden.

Fazit

Ähnlich wie seinerzeit bei der DSGVO selbst besteht auch hinsichtlich des Brexits zunächst eine Übergangsfrist. Diese Übergangsphase endet zum Jahresende 2020 nach nur 11 Monaten vergleichsweise schnell. Unternehmen sollten sich bis dahin auf die Möglichkeit eingestellt haben, dass Großbritannien dann als unsicheres Drittland im Sinne der DSGVO zu klassifizieren sein wird.
Organisationen sind daher gut beraten, frühzeitig die richtigen Stellschrauben zu drehen, auch wenn ein möglicher Angemessenheitsbeschluss nicht gänzlich ausgeschlossen ist. Folglich sollten Vorbereitungen getroffen werden, um nicht ggf. Datenübermittlungen einstellen und damit auch Geschäftsbeziehungen beenden zu müssen.

(Benjamin Spallek, Director Data Protection Services, Creditreform Compliance Services GmbH)

Kommt das Unternehmensstrafrecht in Deutschland doch noch?

Bestechung, Schmiergeldzahlungen, Beschleunigungszahlungen – Die Facetten von Korruption und Non-Compliance im Allgemeinen sind zahlreich. Was vor einigen Jahren vielleicht noch zur Normalität oder dem „guten Ton“ zählte, um einen Auftrag für das Unternehmen an Land zu ziehen, wird heute intensiv verfolgt – von den Wettbewerbern, den Aufsichtsbehörden und nicht zuletzt den Kunden und der Gesellschaft. Lange, zähe und vor allem teure Gerichtsprozesse und Ermittlungsverfahren haben z.B. Siemens und Daimler über sich ergehen lassen müssen, weil einigen Mitarbeitern solche „Vertriebspraktiken“ nachgesagt und später auch nachgewiesen wurden.

Bislang wird Unternehmenskriminalität in Deutschland auf Grundlage des Ordnungswidrigkeitengesetzes (OWiG) sanktioniert. Die Bußgelder gegen Unternehmen und ihre gesetzlichen Vertreter sind i.d.R. auf 10 Mio. Euro limitiert. Schon seit vielen Jahren wird dies als unzureichend kritisiert. Seit August 2019 kursiert – jedoch noch inoffiziell – der Entwurf eines Verbandssanktionengesetzes. Unternehmen und ihre gesetzlichen Vertreter sollen auf dieser Grundlage für strafrechtliche Verstöße aus dem Unternehmen heraus haftbar gemacht werden. Hiermit gäbe es dann bspw. kein Opportunitätsprinzip mehr bei der Frage, ob in einem konkreten Fall ermittelt wird. Vielmehr greift dann das Legalitätsprinzip mit der Ermittlungspflicht für Strafverfolgungsbehörden. Neben den finanziellen Sanktionen sieht der Referentenentwurf zudem die Auflösung eines Unternehmens als mögliche weitere Konsequenz vor.

Eine Frage drängt sich hier zwangsläufig auf: Wie kann ich mein Unternehmen vor solchen Konsequenzen schützen? Der Referentenentwurf regelt nicht nur Sanktionsmöglichkeiten für den Fall, dass Unternehmen den gesetzlichen Rahmen nicht einhalten. Er zeigt auch auf, wie man sein Unternehmen vor solchen Folgen bewahren könnte. Haftungsreduzierend wird nämlich bewertet, ob das beschuldigte Unternehmen zum Tatzeitpunkt über ein angemessenes Compliance-Management-System verfügte. Sollte das Unternehmen hierüber nicht verfügen oder durch die Verstöße Mängel am Compliance-Management-System festgestellt worden sein, ist dies noch kein Grund aufzugeben. In gleicher Weise wird berücksichtigt, ob das Compliance-Management-System nach Bekanntwerden der Verstöße nachjustiert oder implementiert wurde, für den Fall, dass es bislang noch nicht vorhanden war. Jedem wird zugestanden, dass er aus seinen Fehlern lernt. Die Botschaften des Referentenentwurfs sind klar:

- Compliance ist lange kein „Nice-to-have“ mehr!
- Compliance betrifft jedes Unternehmen, nicht nur ausgewählte Branchen oder Unternehmen ab einer gewissen Größe!
- Es ist nie zu spät ein Compliance-Management-System einzurichten!

Mit einem finalen Inkrafttreten ist wohl in nächster Zeit nicht zu rechnen. Allerdings kursieren in Fachkreisen Informationen, dass sich CDU und SPD vor kurzem über den Entwurf und einige Streitpunkte geeinigt haben sollen. Sicher scheint nur, dass das Gesetz, als Bestandteil des aktuellen Koalitionsvertrages, noch in der aktuellen Legislaturperiode verabschiedet wird.

(Carina Bühne, Senior Consultant Compliance & AML, Creditreform Compliance Services GmbH)

Auswirkungen der DSGVO auf Suchmaschinenoptimierung – ist SEO datenschutzkonform?

Die Datenschutz-Grundverordnung (DSGVO) hat EU-weit Auswirkungen auf Unternehmen. Den Verantwortlichen für die digitale Sicherheit in Unternehmen ist die DSGVO wahrscheinlich bereits bekannt, aber welche Auswirkungen haben die Vorschriften auf die SEO-Maßnahmen eines Unternehmens? Ist SEO datenschutzkonform? In diesem Beitrag erläutern wir was SEO genau ist, wie die Umsetzbarkeit von SEO-Maßnahmen durch die DSGVO beeinflusst wird und erläutern, weshalb SEO datenschutzkonform umsetzbar ist.

SEO was ist das?

Die Search Engine Optimization (zu Deutsch Suchmaschinenoptimierung) bezeichnet Maßnahmen und Strategien, welche die eigene Webseite relevanter für Suchmaschinen wie Google macht. Mit einer gut ausgearbeiteten und umgesetzten SEO-Strategie lassen sich bessere Rankings bei Suchanfragen erzielen. Im besten Fall wird die Webseite dann, bei Eingabe bestimmter Suchbegriffe, sogenannter Keywords, auf der ersten Seite angezeigt. Dies ist wichtig, da Suchende im Internet vor allem auf die Ergebnisse auf den ersten Seiten klicken. Ab Seite 4 ist man aus der Sicht des Suchenden praktisch unsichtbar. Ein gutes Ranking auf den vorderen Suchergebnisseiten führt somit zu mehr Traffic auf der eigenen Webseite und schlussendlich auch zu einer Steigerung der Neukunden und des Umsatzes.

© Adobe Stock / Song_about_summer

Umsetzbarkeit von SEO-Maßnahmen in Hinblick auf die DSGVO

Mit der eigenen Webseite in den Top Ergebnissen der Suchmaschinen platziert zu werden, ist kein Zufallsprodukt. Die Algorithmen der Suchmaschinen, wie Google, Yahoo oder Bing, nehmen eine Bewertung der Relevanz aller indizierten Webseiten weltweit vor. Auf den ersten Positionen werden dann die Webseiten eingeblendet, die anhand verschiedenster Kriterien, als am relevantesten zur entsprechende Suchanfrage eingestuft werden.

Die Suchmaschinenoptimierung hat zum Ziel, eine Website gemäß diesen Kriterien zu optimieren, um das Ranking nachhaltig zu verbessern. Hierfür können u.a. folgende SEO-Maßnahmen umgesetzt werden:

- **Keywording** ist der erste Schritt, wenn mit der SEO-Optimierung einer Webseite begonnen wird. Hier geht es darum, die wichtigsten Schlüsselbegriffe (Keywords) zu ermitteln, welche die Nutzerintentionen widerspiegeln. Anhand der definierten Keywords wird dann die Webseite in Hinblick auf die Struktur, die Inhalte u. v. m. optimiert.

Wenn Sie z.B. ein Anbieter von Schuhen sind, und Sie haben unterschiedliche Seiten für Damen- und Herrenschuhe, für Stiefel, Sandalen und Sneaker, dann finden die Suchmaschinen es gut, wenn sie Keywords finden, die zu Ihrem Inhalt passen. Gibt ein Suchender dann z.B. als Keyword „weiße Stiefel" ein, dann sollte auch die Unterseite Ihrer Webseite bei Google angezeigt werden, auf der Sie weiße Stiefel anbieten und nicht die, auf der rote Sneaker dargestellt werden.

- **Technisches SEO** umfasst die technische Optimierung einer Webseite als Grundvoraussetzung für ein gutes Ranking. Es verfolgt das Ziel, die Inhalte einer Website so darzustellen, dass die verschiedenen Algorithmen, die den Suchmaschinen zu Grunde liegen, diese lesen und verstehen können. Hierbei wird das Augenmerk u.a. auf die URL-Optimierung, die Linkstruktur, vor allem im Hinblick auf fehlerhafte Links, die kein Ziel haben (sog. 404 Errors) und eine Reduzierung der Code-Schnipseln im Quellcode gerichtet. Ein Hauptaugenmerkt liegt dabei auch immer auf der Lösung von Server-Problemen um die Seitenladegeschwindigkeit (Sitespeed) zu optimieren. Das technische SEO ist die Voraussetzung dafür, dass weitere Optimierungsmaßnahmen greifen können.
- **OnPage-Maßnahmen** umfassen alles, was ein Websitebetreiber auf seiner Seite direkt optimieren kann. Dies beinhaltet u.a. die Erstellung von zielgruppengerechtem, relevantem Inhalt, welches das Informationsbedürfnis des Webseiten-Besuchers abbildet. Des Weiteren kann eine klare Struktur der Webseite und die Verwendung und Pflege von Meta-Tags, wie z.B. die Meta Description, welche kurz den Inhalt einer Seite wiedergibt, dazu beitragen, dass die Webseite und die Inhalte besser von den Suchmaschinen gecrawlt und somit als relevant eingestuft werden können.
- **OffPage -Maßnahmen** zielen unter anderem darauf ab, eingehende Links von anderen Seiten, sogenannte Backlinks, zu erhalten. Ein erster Weg solche Backlinks zu erhalten, ist die Registrierung in verschiedenen Branchenverzeichnissen wie z.B. google my business, Gelbe Seiten und Co. Webseiten vernetzen sich untereinander bei thematisch ähnlichen Inhalten als Empfehlung für weiterführende Informationen oder Referenzen. So können Backlinks vor allem durch gutes Content Marketing generiert werden, indem z.B. Blogartikel verfasst, Videos, Grafiken, Studien und Whitepapers veröffentlicht oder in Foren aktiv Inhalte verfasst werden.

In der DSGVO wird der Umgang mit personenbezogenen Daten geregelt. Sobald ein Unternehmen auf irgendeine Art und Weise personenbezogene Daten, die den Nutzern direkt oder indirekt zugeordnet werden können, wie z.B. Name, Anschrift, E-Mail-Adresse, Kontodaten oder Geburtstag sammelt und verarbeitet, findet die DSGVO Anwendung.

Keine SEO-Maßnahme basiert auf personenbezogenen Daten - d.h. für die SEO-Optimierung einer Webseite müssen keinerlei Nutzer-Daten erhoben und verarbeitet werden, weswegen die DSGVO im Bereich SEO keine Anwendung findet. Bei all den Unsicherheiten, welche die DSGVO in anderen Marketingbereichen, wie z.B. E-Mail-Marketing, Suchmaschinenwerbung oder Social Media Werbung hervorgebracht hat, ist SEO das einzige Marketinginstrument, welches von der

DSGVO weitestgehend unberührt bleibt und zudem keine direkten Werbekosten verursacht!

Fazit

Die Suchmaschinenoptimierung (SEO) verfolgt das Ziel eine Webseite, durch die Optimierung von Inhalten und technischen Aspekten, für Suchmaschinen attraktiv zu machen. Hierdurch wird die Webseite als relevant und informativ wahrgenommen und somit in den oberen Ergebnissen gelistet. Durch SEO-Maßnahmen wird somit nicht, wie bei anderen Onlinemarketingmaßnahmen direkt nach der Zielgruppe gesucht und diese angeworben, sondern die eigene Webseite wird so dargestellt, dass die Zielgruppe sie findet. Damit ist SEO die natürlichste Art des Onlinemarketings und zu 100% DSGVO-konform!

Dieser Artikel soll einen allgemeinen Einblick in das Verhältnis zwischen SEO Maßnahmen und aktuellen Regelungen der DSGVO geben, erhebt aber keinen Anspruch auf Vollständigkeit und Aktualität, da sich hier täglich Neuerungen ergeben. Die im Artikel enthaltenden Empfehlungen ersetzen keine Rechtsberatung durch einen Fachanwalt der Creditreform Compliance Services. Bei der technischen Umsetzung der DSGVO auf Ihrer Website oder der Anpassung DSGVO-relevanter Formulierungen, ist Digitalraum GmbH ihr richtiger Ansprechpartner.

(Matthias Sorsoli, Director - Sales & Projects, Digitalraum GmbH)

Impressum

Herausgeber

Creditreform Compliance Services GmbH

Hellersbergstraße 11

41460 Neuss

Tel: +49 2131 109-1089

Fax: +49 2131 109-81089

www.creditreform-compliance.de

info@creditreform-compliance.de

Amtsgericht Neuss HRB 4213

USt-IdNr.: DE120690803

Geschäftsführung

Silvia Rohe

Redaktion, Layout und Satz

Jasmin Falk

Autoren dieser Ausgabe

Alexander Schmidt, Benjamin Spallek, Carina Bühne, Matthias Sorsoli

Bildnachweis

Adobe Stock

Redaktioneller Hinweis